DISEÑO, DESARROLLO E IMPLEMENTACION DEL PLAN DE TRANSICIÓN DEL PROTOCOLO IPV4 A IPV6 DE LA ENTIDAD FENIX

MAURICIO SUAREZ MAYORGA

MANUEL ALFONSO ROVIRA SOLANO

UNIVARSIDAD SANTO TOMAS

FACULTAD DE INGENIERIA

ESPECIALIZACION EN REDES DE DATOS

BOGOTA

2016

DISEÑO, DESARROLLO E IMEMENTACION DEL PLAN DE TRANSICIÓN DEL PROTOCOLO IPV4 A IPV6 DE LA ENTIDAD FENIX

Presentado por:

MAURICIO SUAREZ MAYORGA

MANUEL ALFONSO ROVIRA SOLANO

Proyecto Para Optar El Título De Especialista En Gestión De Redes De Datos

Dirigido por:

MSC. Carlos Enrique Montenegro Narváez

UNIVARSIDAD SANTO TOMAS

FACULTAD DE INGENIERIA

ESPECIALIZACION EN REDES DE DATOS

BOGOTA

2016

RESUMEN

El presente documento expone la migración de la infraestructura de red de la empresa Fénix la cual se desarrolló en tres fases durante el periodo comprendido entre los meses de octubre y diciembre del año 2015. El presente documento se desglosa en tres fases principales de planeación, implementación y pruebas de funcionalidad, en las cuales se migro al protocolo IPv6 toda la infraestructura que era compatible y de esta manera se cumplió con las recomendaciones expuestas por la circular 002 de 2011 donde se promueve la adopción del protocolo IPv6 en Colombia.

Para la fase I se realizó todo el proceso de planeación del proyecto. Para ello se generó el inventario de equipos identificando claramente los equipos que soportan IPv6, cuáles requerían actualizarse y en cuáles definitivamente no se podía implementar IPv6, además se realizó el análisis, diseño y desarrollo del plan de diagnóstico del protocolo IPv4 a IPv6.

Para la segunda fase se desarrolló el plan de implementación. Para esto se realizaron una serie de actividades encaminadas a la habilitación de IPv6 en cada uno de los componentes de hardware y software identificados en la etapa de diagnóstico.

En la tercera fase se realizaron las pruebas y monitoreo de la funcionabilidad de IPv6 en los sistemas de información, sistemas de almacenamiento, sistemas de comunicaciones y servicios de la entidad

Para cada una de las fases se planteó una serie de actividades dentro de un cronograma de trabajo, el cual permitió llevar un avance controlado de cada una de las fases hasta completar el 100% de la migración planteada en la infraestructura compatible con el protocolo IPv6 en este proyecto.

ABSTRACT

This document presents the migration of network infrastructure of the Phoenix Company which was developed in three phases over the period between the months of October and December of 2015. This document is divided into three main phases of planning, implementation and functional tests, in which the IPv6 protocol is migrated in all the infrastructure that was compatible and thus was fulfilled with the recommendations set forth by Circular 002 of 2011 where the adoption of IPv6 in Colombia is promoted.

For Phase I entire project planning process was performed. For this was made the equipment inventory clearly identifying the equipment supporting IPv6, which required update and what definitely could not implement IPv6, plus the analysis, design and development of diagnostic plan IPv4 to IPv6 protocol was performed.

For the second phase implementation plan was developed. For this a series of activities aimed at enabling IPv6 in each of the hardware and software components identified in the diagnostic phase were performed.

In the third phase testing and monitoring of IPv6 functionality were performed in information systems, storage systems, communications systems and services of the entity.

For each of the stages a series of activities was raised in a work schedule, which allowed a controlled advance in each of the phases to complete 100% of migration raised in the infrastructure compatible with the IPv6 protocol in this project.

PALABRAS CLAVES

- IPv6
- DUAL STACK
- MIGRACION

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE GRAFICAS

1 INTRODUCCION

IPv4 no ha cambiado desde su planteamiento inicial para el direccionamiento de las redes, y aunque ha probado ser sólido y trabajar en redes globales, su imposibilidad de adaptarse a los requerimientos actuales genera signos de debilidad por no poder dar respuestas adecuadas, especialmente en lo relativo al agotamiento gradual de direcciones IP públicas disponibles. La llegada de entornos como "Internet de las cosas" está requiriendo una cantidad de direcciones casi que infinitas. En 1992, el Grupo de Trabajo de Ingeniería de Internet (IETF), llamó a la comunidad de investigación para estudiar alternativas para IPv4. El resultado se presentó en 1995 y fue llamado Protocolo de Internet versión 6 (IPv6) (Deering R Hinden S, 1998).

IPv6 es un protocolo aun en etapa evolución, que merece atención y estudio por la academia. Varios avances en la implementación en algunos países de la región han generado un avance aunque según estadísticas de LANIC aún falta mucho por hacer con respecto a la migración de las redes hacia IPv6.

Las tecnologías IP innovan a pasos enormes las comunicaciones mundiales, la convergencia de las tecnologías de la información es clave para dar continuidad a los procesos tanto empresariales como educativos en tiempo real. Para esto la calidad de servicio (QoS) juega un papel importante, debido a que contar con una tecnología (IPv6) que fuera capaz de tener una menor degradación en la calidad y aplicaciones en tiempo real permite una mayor penetración hacia una utilización masiva de las tecnologías de la información de una manera más eficiente.

Las Redes IPv6, se han venido implementando a nivel mundial, garantizando la prestación de servicios duales para evitar no omitir ni denegar servicio a usuarios que aun trabajen sobre el protocolo IPv4. Se logra por esta razón en este documento plantear una solución que permite la convivencia entre las dos.

En el presente documento se desarrolla uno de los pasos más importantes, en la adopción de IPv6, que es la "transición" de IPv4 a IPv6, está implementación fue desarrollada en un ámbito real dentro de una compañía Colombiana por lo cual, y por motivos de confidencialidad se cambió el nombre de la compañía a “FENIX” y se realizó censura a datos sensibles ya que este documento solo tiene fines académicos para guía de futuras migraciones a IPv6. En este aspecto el presente, representa las fases de planeación, implementación y pruebas para lograr una convivencia de los dos protocolos mediante el mecanismo Dual Stack.

La fase I de este documento comprende el proceso de planeación del proyecto, donde se general inventario de equipos identificando claramente los que soportan IPv6 y cuáles requerían actualizarse, además se contempla el análisis, diseño y desarrollo del plan de diagnóstico del protocolo IPv4 a IPv6.

Para la fase II se desarrollara el plan de implementación, el cual contempla actividades encaminadas a la habilitación de IPv6 en cada uno de los componentes de hardware y software identificados en la etapa de diagnóstico.

Finalmente para la fase III se realizaran las pruebas y monitoreo de la funcionabilidad de IPv6 en los sistemas de información, sistemas de almacenamiento, sistemas de comunicaciones y servicios de la entidad para corroborar el correcto funcionamiento de la dualidad del mecanismo implantado

2 PLANTEAMIENTO DEL PROBLEMA

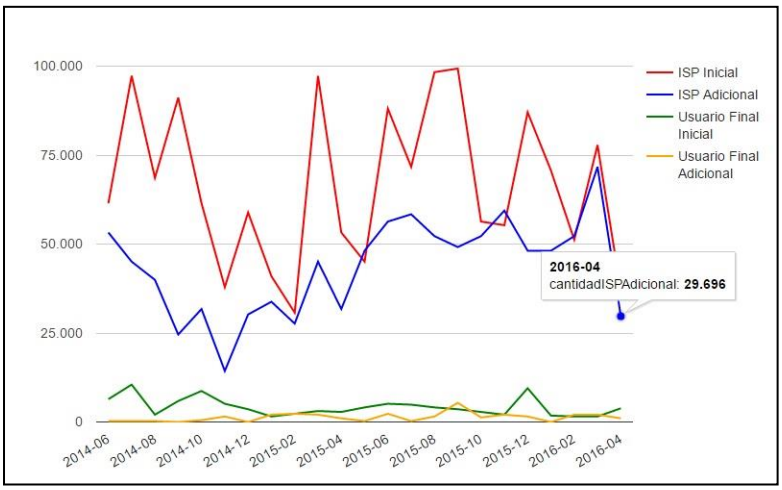
Las redes de comunicación creadas a finales de los años 50's, para la interconexión de ordenadores a nivel mundial, han evolucionado en los últimos 40 años. Por esta razón, se creó un conjunto de normas y reglas para homologar las distintas formas de comunicación de cada uno de los desarrolladores, conocido como protocolos. (Jordy iñigo, 2009)

Un protocolo creado a principios de los 80's es conocido como IPv4, el cual permite conectar los dispositivos que conforman la red por medio de direcciones IP, que son etiquetas numéricas que entregan una identificación a los elementos que componen la red. La estructura de las direcciones en IPv4 está dividida por 4 octetos de 8 bits, es decir 32 bits que dan una cantidad de más de 4.200 millones de direcciones. (Velandia, 2012)

Debido al auge que tuvo la Internet por las nuevas tendencias tecnológicas del mundo en nuevos tipos de productos y servicios y la evolución (Jordy iñigo, 2009) de dispositivos para acceder a la red como teléfonos inteligentes, televisores y consolas (Pulgarin, 2011), las direcciones empezaron a verse limitadas. Por tal motivo, a principios de los 90's se creó un protocolo llamado IPv6, que además de poseer una mejora en la estructura de la cabecera del paquete con respecto a IPv4, tiene capacidad de direccionamiento de 128 bits (8 grupos de 16 bits) es decir $340 * 10^{36} direcciones$(6SOS, 2004)

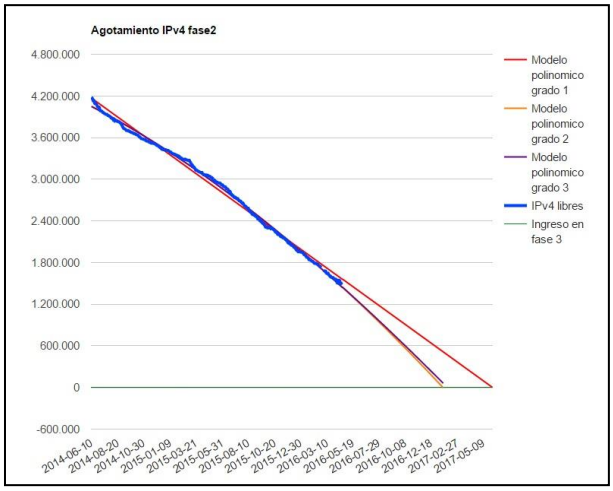
A inicios del año 2011 la IANA (Internet Assigned Numbers Authority) entregó el último grupo de direcciones IPv4 que quedaba disponible (33 millones) a la APNIC que es la entidad encargada de distribuir las direcciones IP en Asia. De acuerdo a esto, Latinoamérica ya está usando sus reservas de direcciones IPv4, lo que conlleva a la inminente transición al protocolo IPv6.

IPv4 ha sido hasta el momento el protocolo más usado en internet pero entró en una fase de agotamiento irreversible. De acuerdo al último informe realizado por LACNIC, los ISP en los últimos meses han utilizado gran parte de sus reservas de direcciones IPv4 y esto se puede evidenciar en la Gráfica 1.



Gráfica 1 Solicitudes IPv4 aprobadas por mes durante la fase 2 de agotamiento.
Fuente: (LACNIC, 2016)

Teniendo en cuenta los datos presentados por LACNIC en la gráfica anterior y tomando en cuenta esta última entrega de direcciones, esta entidad ha hecho una proyección con las posibles fechas de agotamiento de direcciones IPv4. En la gráfica 2 se indica que la fecha aproximada de agotamiento se proyecta para el mes de mayo de 2017.



Gráfica 2 Proyeccion de fechas de agotamiento de direcciones IPv4
(LACNIC, 2016)

Teniendo en cuenta los datos proporcionados por LACNIC, Colombia por medio del Ministerio de Tecnologías de la Información y las Comunicaciones, quiere impulsar la migración hacia el protocolo IPv6, empezando por las entidades del estado. Esto con el fin de alentar a los operadores locales a acelerar la transición en beneficio de los usuarios finales.

En Colombia se muestra la necesidad de implementar IPv6 en la circular 000002 del 6 de julio del 2011 con título "Promoción de la adopción de IPv6 en Colombia". El principal objetivo en este documento, es ampliar el número de usuarios de internet banda ancha de 2.2 a 8.8 millones en un periodo comprendido entre 2010 y 2014. (ACIS, 2011). Adicionalmente RENATA en un informe realizado en el año 2013 advierte que "las instituciones que en 2013 no estén al día en la implementación de IPv6 correrán el riesgo de quedar atrasadas y tener problemas para utilizar determinados recursos en Internet puesto que estos solo serán diseñados para funcionar con este protocolo. Lo anterior podrá representar serias desventajas a la hora de ser competitivos. También es importante recordar que en la medida en que pasa el tiempo y se terminan de agotar las direcciones en IPv4 los costos para implementar IPv6 subirán considerablemente por el incremento de la demanda" (IPv6MX, s.f.)

Además, en las empresas el hecho de desconocer cuál es el procedimiento necesario para adoptar IPv6 sin que se afecten de manera crítica las aplicaciones que actualmente funcionan sobre el protocolo IPv4 y además que se aumenten los costos durante esta implementación, hace que se genere desconfianza e incertidumbre hacía la transición al protocolo IPv6. (Cruz, 2014)

Es importante resaltar que el despliegue IPv6 se posterga en algunos operadores dado que la migración a este protocolo no es una tarea sencilla. Los protocolos IPv4 e IPv6 no son compatibles, y la mayor complejidad radica en que se debe mantener esta compatibilidad con IPv4 mientras se migra a IPv6. Teniendo en cuenta toda la problemática descrita anteriormente con el presente documento se pretende implementar el protocolo IPv6 en una entidad respondiendo a la siguiente pregunta. ¿Cuál es el mecanismo para realizar la migración de IPv4 a IPv6 en la empresa Fenix sin afectar los servicios que actualmente funcionan sobre el primero?

3 JUSTIFICACION

La migración o actualización de una tecnología al inicio genera escepticismo por saber si al adoptar el cambio, se lograrán mejoras con relación al estado anterior del traslado. Según un estudio socio económico realizado en la Universidad Nacional de Colombia, las causas de esta incertidumbre son: el desconocimiento sobre IPv6, asumir que el tema es muy especializado, falta de personal capacitado para implementarlo en los diversos sectores del país; y esto atado al costo que tiene realizar para la compra de equipos, capacitación de personal y tiempo de ejecución a nivel nacional. (Cruz, 2014)

Estas deficiencias hacen que se generen mecanismos a nivel gubernamental, social, económico e investigativo que promuevan la implementación del protocolo IPv6. El gobierno asumirá campañas de capacitación para la actualización e implementación de IPv6 por medio de conferencias, cursos, talleres, convenciones entre otros, con el fin de mitigar los problemas existentes por falta de conocimiento para la adopción del nuevo protocolo. (Cruz, 2014)

El gobierno desde el año 2012, ha realizado alianzas con instituciones como RENATA para iniciar un programa de capacitación y acompañamiento a instituciones; como se expresa en lo publicado en http://www.renata.edu.co, en donde esta entidad informa que "para diciembre de 2013 Colombia contará con 71 instituciones con servicios puestos a punto en la adopción de IPv6. (UNIVERSIDAD DEL QUINDIO, 2016) En 2012 se acompañaron 38 instituciones en la implementación de IPv6 y capacitó a más de 100 ingenieros en la adopción de este protocolo" (IPv6MX, s.f.). Debido a toda esta cantidad de recursos que se han invertido en el acompañamiento y formación para el protocolo IPv6 es importante que instituciones como la entidad Fénix aprovechen estas herramientas que ha dado el gobierno y lleven a cabo esta migración.

La migración es un proceso de despliegue que se extiende en el tiempo, hoy en día existen muchos servicios que solamente se ofrecen en IPv4 y las soluciones a la migración son temporales porque se vive en función de las direcciones Ipv4. Debido a esto, ambos protocolos deben coexistir y uno de los mecanismos para poder realizar una migración de

este tipo es Dual Stack (coexistencia de IPv4 e IPv6 en los mismos dispositivos y redes). Este mecanismo implica la utilización de ambos protocolos en paralelo en los dispositivos. Lo que se pretende en este documento es implementar una migración de IPv4 a Ipv6 mediante el mecanismo de Dual Stack por las razones anteriormente expuestas.

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Implementar el protocolo IPv6 en la infraestructura y aplicaciones compatibles, sin afectar el funcionamiento de los servicios que se ejecutan en IPv4, mediante el mecanismo de Dual Stack, para garantizar la prestación de los servicios en los dos protocolos en la entidad Fenix.

4.2 OBJETIVOS ESPECIFICOS

- Realizar el diseño y desarrollo del plan de diagnóstico del protocolo IPv4 a IPv6 en la red de la entidad Fénix.

- Activar y configurar las funciones del protocolo IPv6 para cada uno de los dispositivos de red de comunicaciones compatibles que componen la infraestructura de la entidad.

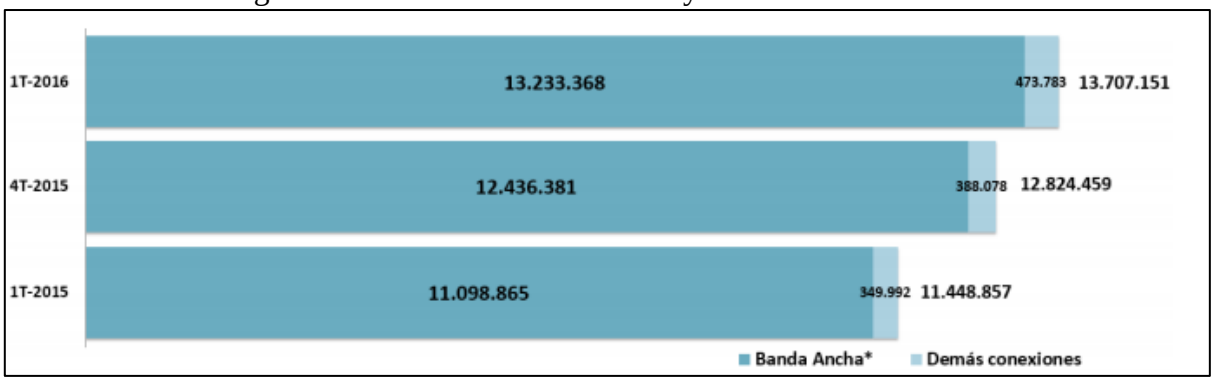
- Realizar pruebas y monitoreo de la funcionalidad de IPv4 e IPv6 en los sistemas de información, sistemas de almacenamiento, Sistemas de Comunicaciones y servicios de la entidad para verificar su correcto funcionamiento.

5 ESTADO DEL ARTE

En términos generales en Colombia y en Latinoamérica se ha venido incrementando la penetración del internet en la población en general lo cual ha venido agotando la cantidad de direcciones IPv4 que se encuentran disponibles, por esta razón el gobierno nacional mediante la Circular 002 del 6 de julio de 2011 promueve la adopción de IPv6 en Colombia, sin embargo muchas de las estadística demuestran que los ISP son reacios a implementar esta infraestructura, por lo cual las entidades estatales han venido migrando sus redes para de esta manera obligar a estos ISP a migrar también sus redes de una manera pronta y oportuna.

Actualmente en Colombia la penetración del internet de banda ancha y móvil se ha venido incrementando de una manera exponencial como se evidencia en cifras presentadas en boletín trimestral de las TIC del primer trimestre de 2016 del Ministerio de las Comunicaciones, donde se ilustra que "*Al finalizar el primer trimestre de 2016, el número total de conexiones a Internet de Banda Ancha* alcanzó los 13.233.368 accesos en el país, mientras las demás conexiones a Internet (conexiones con velocidad efectiva de bajada – Downstream <1.024 Kbps + Móvil 2G) suman 473.783, para un agregado nacional de 13.707.151 conexiones a Internet.*" (MINISTERIO DE LAS TELECOMUNICACIONES, 2016) Figura 1.

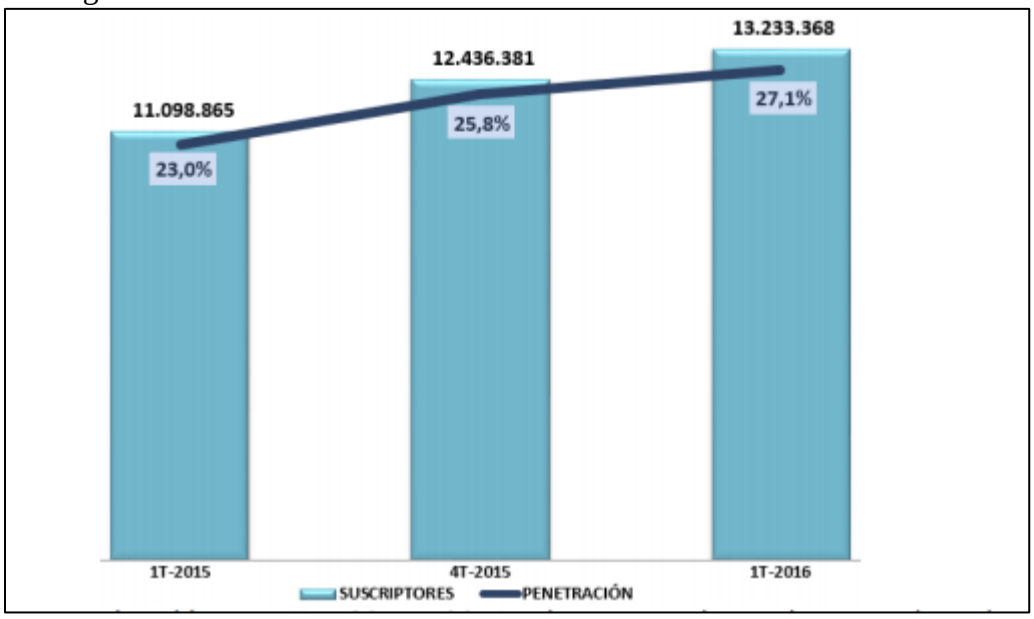
Figura 1 Conexiones Banda Ancha y Demás Conexiones



Fuente: Datos reportados por los proveedores de redes y servicios al SIUST – Colombia TIC. Fecha de Consulta 22 de Junio de 2016.

Teniendo en cuenta estas cifras donde se evidencia que al término del primer trimestre del año 2016 aumentaron los usuarios de banda ancha 4,1 puntos porcentuales con relación al primer trimestre del año 2015, alcanzando un índice de 27,1%. Figura 2.

Figura 2 Conexiones a Internet de Banda Ancha e Índice de Penetración



Fuente: Proyección de población DANE 2015 – 2016 y datos reportados por los proveedores de redes y servicios al SIUST – Colombia TIC. Fecha de Consulta 22 de Junio de 2016.

Teniendo en cuenta estas cifras, se evidencia que el aumento del consumo de internet en los hogares y en general en el país se incrementa año a año y teniendo encuentra que las direcciones IP que se asignaron a Colombia se han venido agotando, se requiere que se adelante un trabajo oportuno de migración de las redes hacia IPv6 para mantener este crecimiento y mantener las redes del país la vanguardia mundial.

Para Colombia la organización encargada de la asignación de direcciones IP es LACNIC, el Registro de Direcciones de Internet para América Latina y Caribe, es una organización no gubernamental internacional establecida en Uruguay en el año 2002. Es responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), esta organización desde años anteriores advirtió a las diferentes naciones que hacen parte de ella

el agotamiento de las direcciones IPv4 y realizo la recomendaciones para que cada país iniciara la implementación del Protocolo IPv6 el cual tiene una capacidad casi que infinita de direcciones y que cumple con requerimientos de calidad de servicio y seguridad mucho mayores que su predecesor, sin embargo en la actualidad y según estudios realizado mediante visitas e informes de cada uno de los países miembros se demuestra cómo esta migración hacia IPv6 se encuentra con bajos índices de implementación.

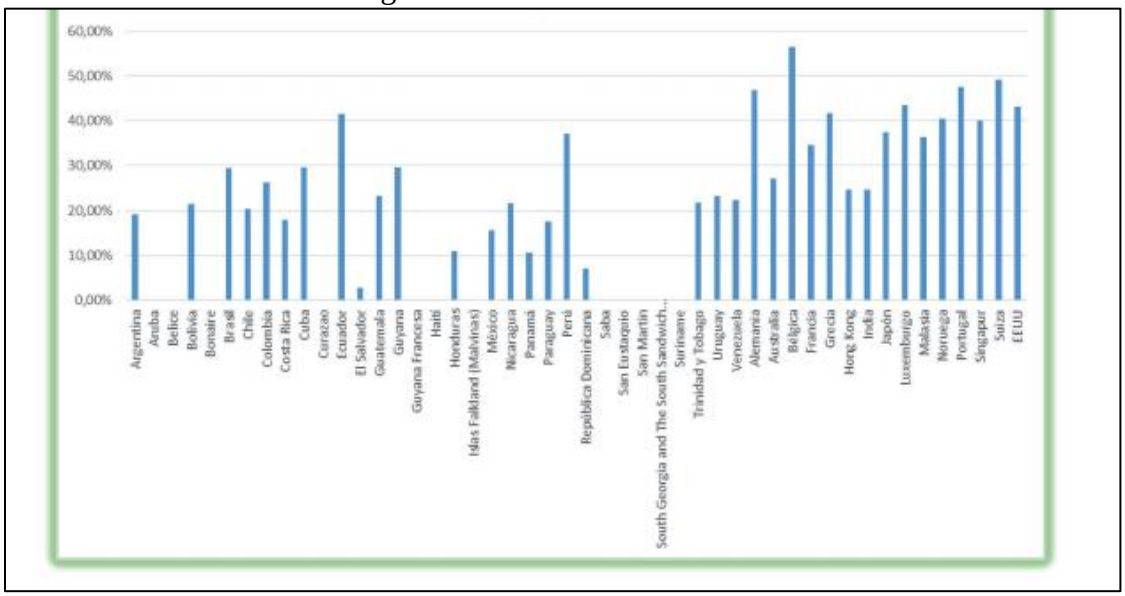
LACNIC en su informe **DESPLIEGUE DE IPv6 PARA EL DESARROLLO SOCIOECONÓMICO EN AMÉRICA LATINA Y EL CARIBE** demuestra el Indicador Clave de Avance para IPv6 de LACNIC (LACNIC/CAF ICAv6) en el cual se evidencia que los siguientes países superan un valor referencial del 20% para este indicador: Bolivia (21,41%), Brasil (29,52%), Chile (20,43%), Colombia (26,24%), Cuba (29,67%), Ecuador (41,57% Guatemala (23,22%), Guyana (29,61%), Nicaragua (21,70%), Perú (37,05%), Trinidad y Tobago (21,81%), Uruguay (23,22%) y Venezuela (22,33%) (LACNIC, portalipv6.lacnic.net, 2015)

Estos datos del indicador LACNIC/CAF ICAv6 utilizan cuatro ópticas principales: uso de prefijos IPv6, Core, Contenido y Usuarios. Teniendo en cuenta que LACNIC informa que "*un valor superior al 20% se puede lograr con una actividad de planificación y despliegue inicial, una cuestión apreciada en la región; o con una combinación de planificación y despliegue inicial, junto con IPv6 en los accesos*". Se evidencia que la mayoría de los países de Latinoamérica se encuentran en esta situación, lo cual indica que hace falta mucha implementación y que mayoría se encuentran aún en una fase de planificación y despliegue inicial y que se aprecia entorno de Colombia en donde actualmente la incertidumbre de la rentabilidad de estas migraciones hace que muchas de estas no pasen a la fase de implementación.

Para LACNIC valores superiores al 30% solo se logran si hay una implementación masiva de IPv6 en los accesos masivos, según este informe (LACNIC, portalipv6.lacnic.net, 2015), Bolivia, Brasil, Ecuador y Perú presentan valores cercanos aunque Colombia y gracias a las

campañas de las entidades públicas por incentivar la migración hacen que se encuentre en un 26 %. Figura 3.

Figura 3 LACNIC /CAF ICAV6



Fuente: Despliegue De IPv6 Para El Desarrollo Socioeconómico En América Latina Y El Caribe. Diciembre 10 de 2015

Estos datos relevantes los cuales indican que el despliegue de la implementación realmente se verá reflejada cuando exista esta implementación a nivel de la redes de acceso y se evidencia que este debe ser objetivo a alcanzar en Colombia si se quiere mejorar este KPI.

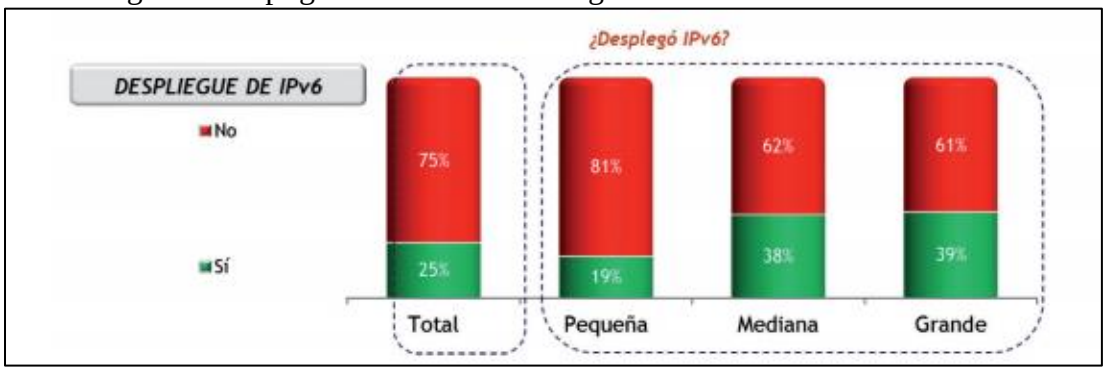
Las medidas que se tendrán que implementar para que se pueda mejorar estos índices de implementación y siguiendo las recomendaciones de LANIC, será mediante el Upgrade de la red de acceso a IPv6 en los ISP o en las grandes instituciones gubernamentales o universitarias.

Despliegue de IPv6 en la región y en los países:

La implementación de IPv6 en la región de Latinoamérica y el caribe aún es muy baja según el estudio realizado en diferentes países por LACNIC, el cual es el encargado de realizar la asignación de estas direcciones a los países miembros de esta organización. Toda vez que se

evidencia que el despliegue está llegando apenas a un 25 %, lo cual demuestra el poco avance que se ha tenido a finales de 2015 fecha en que se presentó este informe.

Figura 4 Despligue De IPv6 En La Region Llatinoamerica Y El Caribe

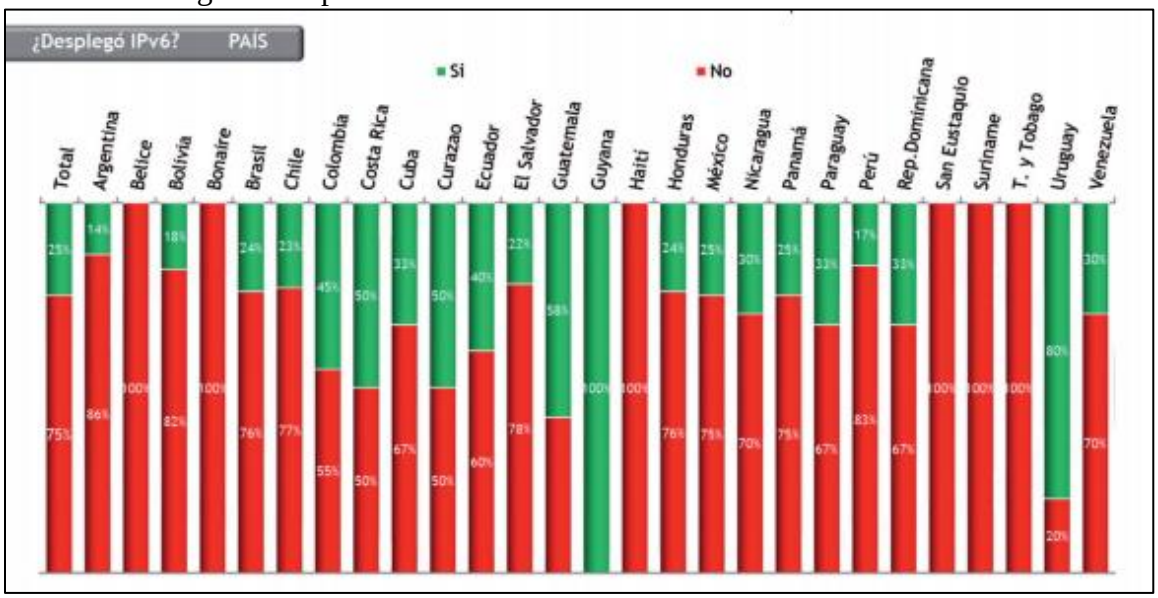


Fuente: Despliegue De Ipv6 Para El Desarrollo Socioeconómico En América Latina Y El Caribe. Diciembre 10 de 2015

Teniendo en cuenta estos dato se ve la importancia de realizar avances en la implementación de esta migración, puesto que es el futuro y es necesario concientizar y realizar labores que permitan que las redes de acceso migren para poder llegar a finales de 2018 a una implementación del por lo menos un 70 % en Latinoamérica y en especial en Colombia ya que con la llegada del internet de las cosas se requiere una evolución del medio para tener competitividad a nivel mundial.

Continuando con el análisis del estado actual de los despliegues IPv6 en la región y teniendo en cuenta que para mejorar los índices KPI de LACNIC frente a esta implementación, la forma es implementar en la red de acceso esta migración ya que los ISP no llegan aún ni al 50 % de ésta en el 80% de los países. Como se evidencia en la siguiente figura 5.

Figura 5 Implementación de los ISP de IPv6 en Clientes Finales



Fuente: Despliegue De Ipv6 Para El Desarrollo Socioeconómico En América Latina Y El Caribe. Diciembre 10 de 2015

Como se evidencia en el consolidado de la figura 5, se puede observar como únicamente en casos puntuales y en países realmente pequeños como Guyana, Uruguay y Guatemala se supera el 50 % de implementación de rede IPv6, lo cual indica el atraso que existe en la región, por lo cual es necesario implementar y llevar a cabo estas migraciones y concientizarse de que esta evolución es necesaria y que traerá beneficios como los ilustrados en este caso de estudio.

En Colombia el despliegue llega al 45 %, el cual pertenece a un nivel corporativo ya que no se ha realizado este despliegue en las redes de acceso residenciales debido a temas como la inversión en los equipos necesarios por lo que muchos de los actualmente instalados en las residencias no son compatibles o requieren de una actualización.

LACNIC en su estudio de campo en Colombia dice que "*Hay avances importantes y sin problemas en el despliegue del acceso corporativo en IPv6 con Dual Stack en casi todos los operadores*". Esto indica que se ha enfocado en lo corporativo y que en la actualidad estos clientes son los que han llevado a los ISP a migrar sus redes debido que son quienes

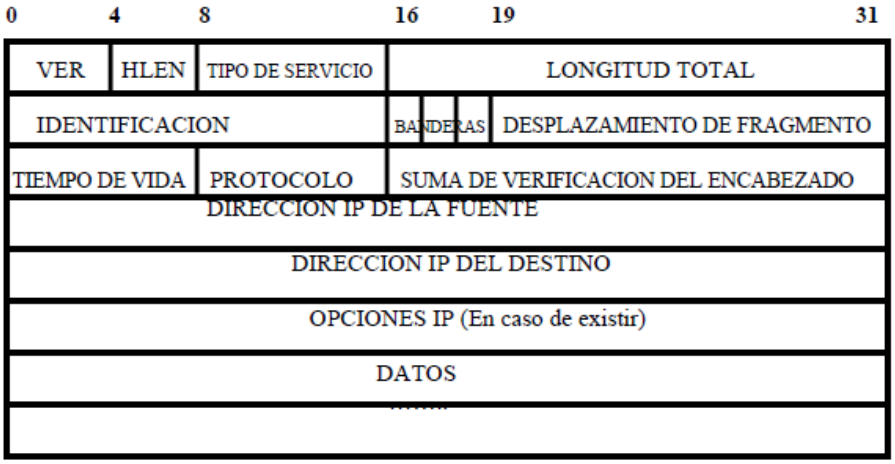
representan gran parte de las ganancias. Por esta razón es importante realizar estas migraciones como la que se presenta en este caso de estudio y adicionalmente generar la presión por parte de los usuarios residenciales para que sus ISP le migren sus redes para que sean más seguras y presten mejores servicios.

6 MARCO TEORICO

6.1 Datagrama

Es la unidad de trasferencia en la cual fluye la información a través de la red. Contiene un encabezado, que tiene los datos sobre la dirección de la fuente y la de destino, y los datos, que son la información neta que se envía. La forma de encaminar los datagramas IP se llama conmutación de paquetes, cada uno de los paquetes se tratan de manera independiente conteniendo la información necesaria para que la red pueda dirigir hacia el ordenador receptor. Son las unidades principales de información de internet destino, y tienen cabida en los servicios de red no orientados a la conexión. (Mathon, 2001)

Figura 6 Cabecera de Datagrama



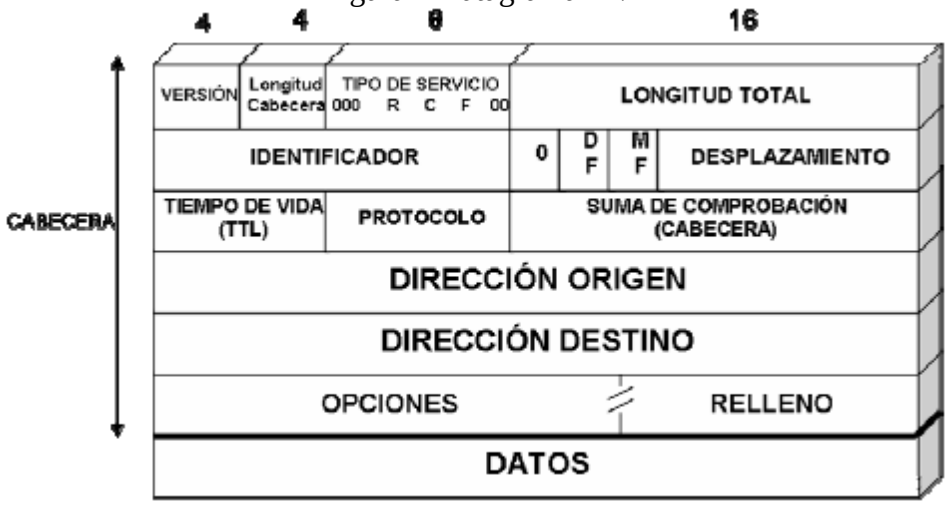
Fuente: Castillo (2005). => también puede ser la fuente completa: nombre y apellido.

6.2 IPv4

Es la cuarta versión del protocolo de internet en uso desde 1981, se utiliza en la capa de red del modelo TCP/IP que permite la conexión a una red, el cual tiene una dirección única para cada dispositivo en la red. Utiliza en la estructura de su direccionamiento 4 octetos de 8 bits por ejemplo 192 168.0.255, esta combinación es capaz de entregar un poco más de 4200

millones de direcciones. La primera dirección de una red se obtiene con una AND lógico y con la máscara de red (Velandia, 2012)

Figura 7 Datagrama IPv4



(Montes Erick Fernando Lujan, 2005)

El datagrama tiene unas divisiones explicadas a continuación:

- Versión

Espacio de 4 bits para indicar la versión de internet.

- Longitud de Cabecera

Indica la longitud del encabezado de 32 bits.

- Tipo de Servicio

Indica la calidad del servicio solicitada por el datagrama, se encuentra descrito en el RFC 791, en un campo de 8 bits.

- Identificador

Es un espacio de 16 bits para la identificación del datagrama IP, identifica de manera única cual paquete pertenece a cual datagrama.

- Banderas

Tienen un espacio de 3 bits, 2 utilizados, el primer identifica la fragmentación del paquete y el segundo bit indica si es el último datagrama del segmento.

- Offset de fragmentación

Indica el Offset del datagrama IP

- Protocolo

Indica el protocolo de trasporte.

- Suma de comprobación

Se utiliza para aprobar la combinación del encabezado.

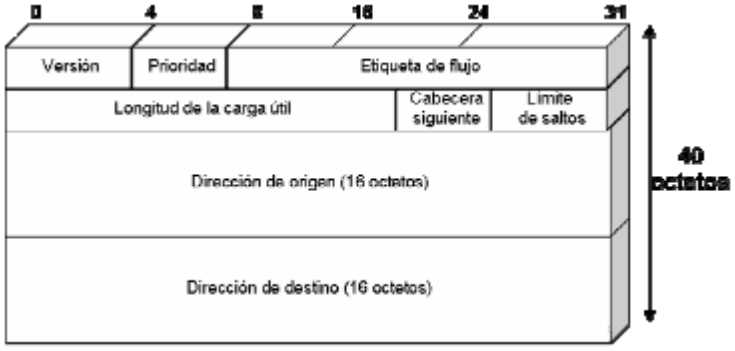
- Dirección origen y dirección destino

Indica las 32 combinaciones para la dirección de la fuente y el destino del paquete respectivamente. (Montes, 2005)

6.3 IPv6

Es una actualización del protocolo de internet IPv4 el cual introduce una serie de mejoras las cuales optimizan la conexión a una red entre los componentes que están conectados. Su característica insignia es su mayor espacio de direcciones. Una dirección IPv6 es de 128 bits de longitud y su representación se da con números hexadecimales separados por dos puntos y ha implantado una mejor jerarquía para el enrutamiento y direccionamiento (Cabellos, 2004)

Figura 8 Datagrama IPv6



(Montes Erick Fernando Lujan, 2005)

- **Versión**

Indica la versión 6 del protocolo de internet IPv6.

- **Prioridad**

Espacio de 8 bits que indican las necesidades del tráfico del paquete.

- **Etiqueta de flujo**

Campo de 20 bits experimental.

- **Longitudes de carga útil**

Espacio de 16 bits que indica la longitud de la carga sin utilizar el encabezado.

- **Cabecera siguiente**

Espacio de 8 bits para las cabeceras de extensión.

- **Límite de saltos**

Campo de 8 bits similar a TTL de IPv4

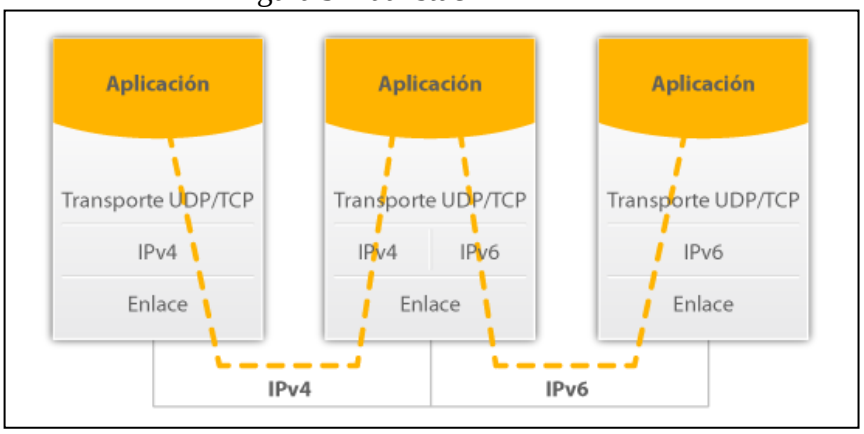
- **Dirección origen destino**

Campo de 128 bits para las direcciones fuente y destino del paquete. (Montes, 2005)

6.4 Mecanismos de transición

- Dual Stack: Es el método propuesto originalmente para tener una transición suave hacia IPv6. En este caso se necesita contar con suficiente cantidad de direcciones IPv4 para poder desplegar las dos versiones del protocolo en simultáneo en toda la red. (LACNIC, Ipv6 portal)

Figura 9 Dual stack



6.5 Aplicaciones

Las aplicaciones son los programas de software que se utilizan para comunicarse a través de la red. Algunas aplicaciones requieren implementar los protocolos de la capa de aplicación y pueden comunicarse directamente con las capas inferiores del stack de protocolos. Los clientes de correo electrónico y los exploradores Web son ejemplos de este tipo de aplicaciones. (Wikispace, 2016)

Cliente-Servidor: Es la tecnología que proporciona al usuario final el acceso transparente a las aplicaciones, datos, servicios de cómputo o cualquier otro recurso del grupo de trabajo y/o, a través de la organización, en múltiples plataformas. El modelo soporta un medio ambiente distribuido en el cual los requerimientos de servicio hechos por estaciones de

trabajo inteligentes o "clientes", resultan en un trabajo realizado por otros computadores llamados servidores (Universidad UCOL, 2016)

7 METODOLOGIA

La metodología que se utilizó en este proyecto fue la de caso de estudio, en donde se analizara el estado actual de la compatibilidad de la infraestructura y aplicaciones de la entidad Fénix, con el fin de realizar la migración al protocolo IPv6. Para realizar esta implementación, se dividirá el desarrollo del proyecto en las siguientes fases:

- **Fase I Planeación**: en esta fase se realiza todo el proceso de planeación del proyecto, para ello se debe generar el inventario de equipos identificando claramente cuales equipos soportan IPv6, cuales requieren actualizarse y en cuales definitivamente no se puede implementar IPv6, además se realiza el análisis, diseño y desarrollo del plan de diagnóstico del protocolo IPv4 a IPv6 en la red de la entidad Fénix y se define el modelo de transición a implementar. Esta información será proporcionada por la entidad Fénix.

- **Fase II Implementación**: En esta fase se desarrolla el plan de implementación, para esto se ejecutara una serie de actividades encaminadas a la habilitación de IPv6 en cada uno de los componentes de hardware y software identificados en la etapa de diagnóstico y teniendo en cuenta el inventario de los activos de información de la entidad Fénix.

- **Fase III Pruebas de Funcionabilidad**: En esta fase se realizan las pruebas y monitoreo de la funcionabilidad de IPv6 en los sistemas de información, sistemas de almacenamiento, Sistemas de Comunicaciones y servicios de la entidad para validar su correcto funcionamiento.

8 SOLUCION

8.1 Fases del Proyecto

8.1.1 Fase I Planeación

En esta fase se realizó todo el proceso de planeación del proyecto, para ello se generó el inventario de equipos identificando claramente los equipos que soportan IPv6 y cuáles requerían actualizarse y en cuáles definitivamente no se podía implementar IPv6, además se realizó el análisis, diseño y desarrollo del plan de diagnóstico del protocolo IPv4 a IPv6 en la red de la empresa Fenix y se definió el modelo de transición a implementar.

Fase I, Planeación	Actividades Generales	Tiempo de Actividad	Personal Involucrado
Diagnóstico de la Solución	Construcción del Plan de Diagnóstico	Del 28 de septiembre al 2 de octubre de 2015	Todo el equipo de Trabajo
	Inventario de TI	Del 3 de octubre al 9 de octubre de 2015	Ingeniero de Comunicaciones, Gerente de Proyecto
	Análisis de nueva topología de la infraestructura actual y su funcionamiento	Del 13 de octubre al 14 de octubre de 2015	Ingeniero Networking
	Protocolo de pruebas de validación de aplicativos, comunicaciones, plan de seguridad y coexistencia de los protocolos.	Del 15 de octubre al 20 de octubre de 2015	Ingenieros de: Aplicaciones, Comunicaciones y Seguridad
	Planeación de migración de los servicios tecnológicos de la entidad.	Del 21 de octubre al 23 de octubre de 2015	Ingeniero Networking

	Validación del estado actual de los sistemas de información y comunicaciones y la interfaz entre ellos.	Del 26 de octubre al 28 de octubre de 2015	Ingeniero de Comunicaciones
	Identificación de esquemas de seguridad de la red de comunicaciones y sistemas de información	El 29 de octubre de 2015	Ingeniero de Seguridad

Tabla 1 Detalle de la Fase I Planeación

8.1.2 Fase II Implementación

En esta fase se desarrolló el plan de implementación. Para esto se realizaron una serie de actividades encaminadas a la habilitación de IPv6 en cada uno de los componentes de hardware y software identificados en la etapa de diagnóstico y teniendo en cuenta el inventario de los activos de información de la empresa FENIX

Fase II, Implementación	Actividades Generales	Tiempo de Actividad	Personal Involucrado
Desarrollo del Plan de implementación	Habilitación direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo al plan de diagnóstico de la Primera Fase.	Del 30 de octubre al 9 de noviembre de 2015	Ingeniero de Networking
	Configuración de servicios de DNS, DHCP, Seguridad, VPN y otros	Del 30 de octubre al 6 de noviembre de 2015	Ingeniero de Datacenter
	Configuración del protocolo IPv6 en Aplicativos y Sistemas de Comunicaciones	Del 9 de noviembre al 13 de noviembre de 2015	Ingeniero de Aplicaciones y Comunicaciones

	Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones de acuerdo con los RFC de seguridad en IPv6.	Del 17 de noviembre al 27 de noviembre de 2015	Ingeniero de Seguridad
	Coordinación con el (los) proveedor (es) de servicios de Internet para lograr la conectividad integral en IPv6.	Del 24 de noviembre al 27 de noviembre de 2015 se realizarán reuniones y se compartirá toda la información para las mejores prácticas de implementación. Del 27 de noviembre al 2 de diciembre de 2015 se realizarán las acciones para lograr conectividad de IPv6 por las redes WAN.	Gerente de Proyecto

Tabla 2 Detalle de la Fase II Implementación

8.1.3 Fase III Pruebas de Funcionabilidad

En esta fase se realizaron las pruebas y monitoreo de la funcionabilidad de IPv6 en los sistemas de información, sistemas de almacenamiento, sistemas de comunicaciones y servicios de la entidad.

Fase III, Pruebas de Funcionalidad	Actividades Generales	Tiempo de Actividad	Personal Involucrado
Pruebas de funcionalidad de IPv6	Pruebas y monitoreo de la funcionalidad de IPv6	Del 3 de diciembre al 11 de diciembre de 2015	Ingeniero de Seguridad

	Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI.	Del 14 de diciembre al 18 de diciembre de 2015	Ingeniero de Seguridad
	Afinamiento de las configuraciones de hardware, software, y servicios de la empresa FENIX.	Del 21 de diciembre al 23 de diciembre de 2015 y del 28 de diciembre al 30 de diciembre de 2015	Ingeniero de Comunicaciones

Tabla 3 Detalle de la Fase III Pruebas de Funcionabilidad

8.2 Fase I Planeación

La fase de planeación representa una etapa crítica e importante del proceso de transición, ya que como se detallará más adelante se identificaron claramente cuáles equipos soportan IPv6, cuales requieren actualizarse y cuáles no soportan el nuevo protocolo, dejando la respectiva documentación en constancia al momento de optar hacia IPv6. Comenzando con el plan de diagnóstico de la infraestructura de TI de la empresa FENIX. Las siguientes son las actividades a tener en cuenta en esta fase:

8.2.1 Diagnóstico de la Situación Actual

Para la construcción del plan de diagnóstico, que es el pilar fundamental de esta fase I, se requiere la realización de una evaluación previa de la infraestructura tecnológica que permita medir el grado de avance en la adopción del protocolo IPv6. Dentro de dicha validación es necesario revisar el grado de compatibilidad del protocolo IPv6 con la infraestructura de las entidades de tal manera que la información recogida de esta tarea sea insumo para la acometida de la segunda fase que es la implementación de IPv6.

- Elaborar y validar el inventario de activos de información de servicios tecnológicos de la empresa FENIX y su interrelación entre ellos. Para esta actividad se requiere desarrollar y mantener el inventario de hardware y software, identificando claramente cuáles equipos soportan IPv6, cuáles requieren actualizarse y cuáles no soportan el nuevo protocolo, dejando la respectiva documentación en constancia al momento de optar hacia IPv6.

- Identificar la topología actual de la red y su funcionamiento dentro de la organización.

- Evaluar el grado de compatibilidad del protocolo IPv6 a nivel de hardware y software con miras a preparar la nueva infraestructura de red de la entidad.

8.2.2 Evaluación de Requerimientos de Hardware y Software de Cumplimiento IPv6

Realizando una descripción general de la red de datos de la empresa FENIX y haciendo énfasis en los aspectos clave que involucran la futura transición hacia IPv6, es necesario conocer qué fortalezas y debilidades posee frente a IPv6 con el fin de evaluar el impacto que tendría la transición sobre los equipos de red (routers, switch, firewall), equipos de usuarios final, la topología y los enlaces.

Además de los requerimientos físicos, se debe tener en cuenta el soporte IPv6 que tienen los diferentes sistemas operativos en los servidores que prestan servicios de aplicaciones que funcionan sobre la red, estas deben ser sometidas a un análisis por parte de los administradores y proveedores con el fin de evaluar qué modificaciones son requeridas para el correcto funcionamiento de las mismas sobre IPV6.

La red de datos la empresa FENIX está definida como un sistema de Backbone en alta disponibilidad con topología en estrella. Esta posee un nodo central (Switches Cisco

referencia 6500), los cuales sirven como switches de core y desde ellos se proveerá la conectividad a los switches de piso (Switches Cisco referencia 2960S) que se encuentran configurados en stack. Cabe aclarar que la infraestructura física en donde se encuentra instalada esta red es un edificio de 7 pisos y cada piso cuenta con switches de acceso.

Adicionalmente las conexiones principales hacia el exterior (WAN, Internet, MPLS) se conectan a través de un firewall Cisco ASA 5520, un switch WAN y un router provisto por el proveedor de servicio.

Los dispositivos centrales o switches de core están configurados en modo VSS (Virtual Switching System) logrando de esta forma tener alta disponibilidad tanto de hadrware como software. Estos equipos cuentan con tarjetas WS-X6716-10GE que permiten conexiones a 10Gb con cada uno de los switch de acceso de los pisos de la empresa FENIX.

Analizando cómo ha sido el comportamiento de estos dispositivos se pudo observar que en horarios productivos presenta un consumo de memoria promedio de 14% y en cuanto al procesamiento tiene un consumo promedio de 20% con algunos picos del 100% durante las últimas 72 horas como se puede apreciar en la Figura 10.

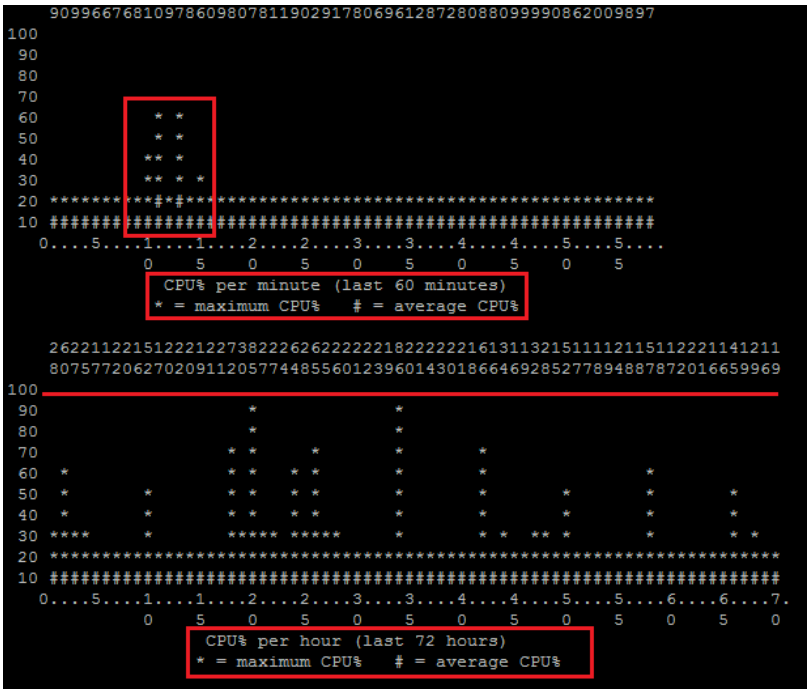
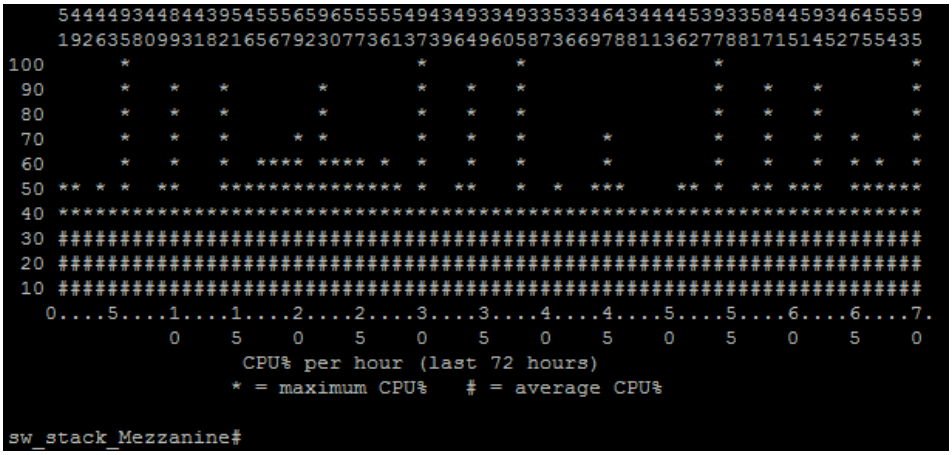


Figura 10 Consumo CPU Cisco Switch 6500

Fuente: Propia

Para el acceso a usuarios finales se utilizan los switch Cisco 2960S en modo stack en cada piso. Analizando el comportamiento del consumo de memoria y CPU de estos equipos en horario hábil, se encontró que tienen un promedio de utilización de 40% con algunos picos donde se hace uso del 100%. Lo anteriormente mencionado se puede observar en la figura 11.



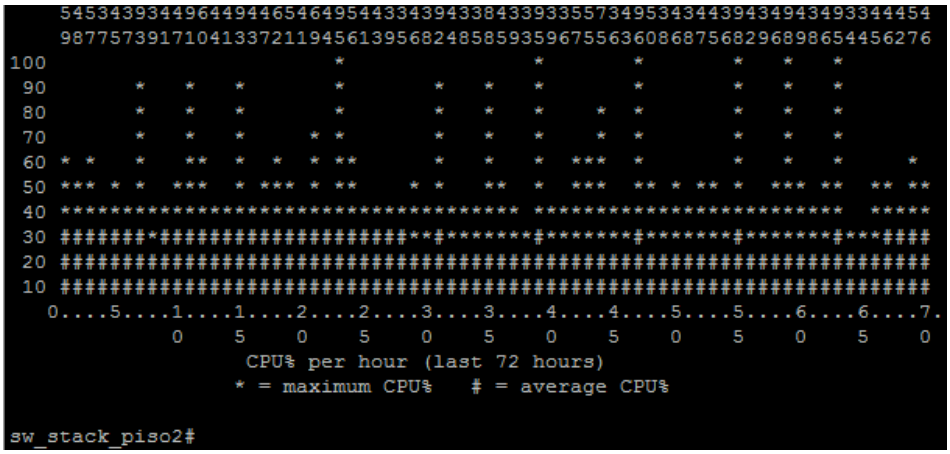


Figura 11 Consumo de CPU Cisco Switch 2960 Stack Piso 2 y Mezannine

Fuente: Propia

Otro dispositivo importante sobre la red de comunicaciones de la empresa FENIX es el Firewall ASA 5520, su trabajo es tener permitir o denegar las conexiones entrantes y salientes hacia Internet, hacia la nube MPLS y establecer conexiones terminales de VPN sitio a sitio y de acceso remoto para usuario desde la internet.

El firewall Cisco ASA 5520 está configurado en alta disponibilidad en modo Activo-Stanby y permite responder ante cualquier falla de hardware y software que se presente. Como información adicional, sus interfaces configuradas con velocidades de 1GB.

Evaluando las capacidades de este equipo y la utilización de sus recursos de Memoria y CPU; se puede observar que durante las horas valle, su consumo es de 59% promedio para CPU y de memoria de 416MB, pero para las horas pico, se tiene un 84% promedio de procesamiento y memoria de 427MB. Lo mencionado anteriormente puede ser observado en las figuras 12 y 13.

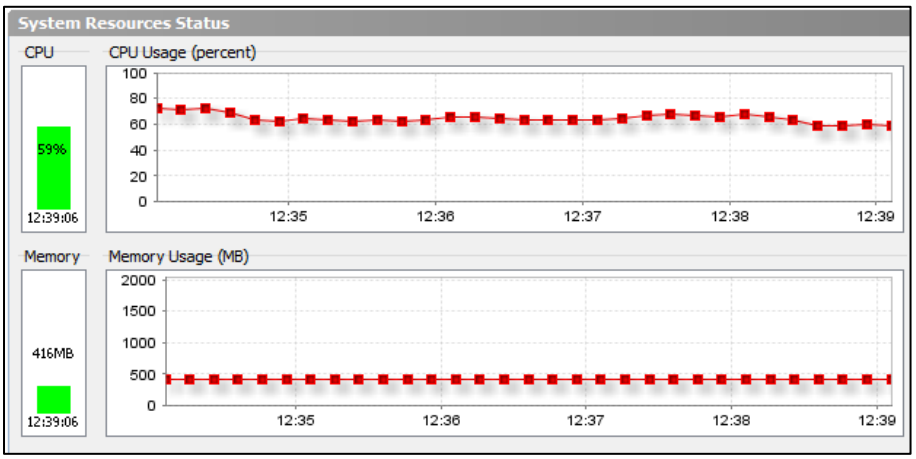


Figura 12 Consumo CPU Cisco ASA 5520 Horas Bajo Nivel de Tráfico

Fuente: Propia

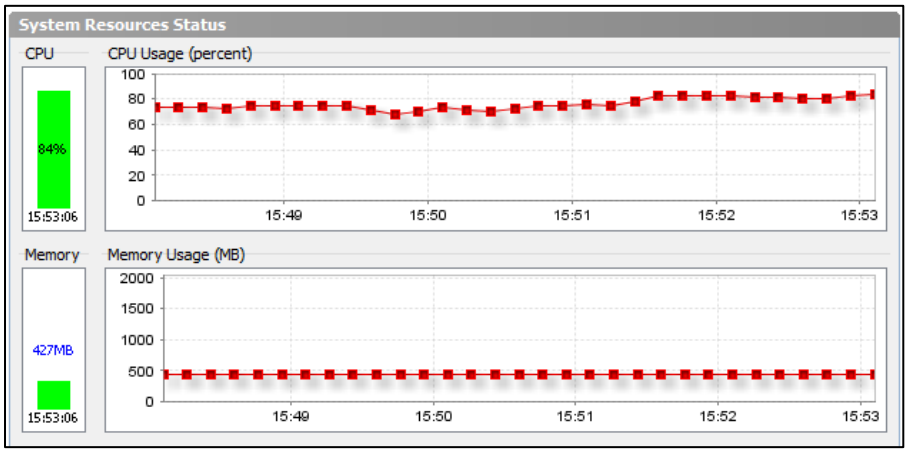


Figura 13 Consumo CPU Cisco ASA 5520 Horas de Alto Nivel de Tráfico

Fuente: Propia

Por último, cabe anotar que este dispositivo es de suma importancia para el buen funcionamiento de la red ya que es el encargado de la seguridad perimetral de la red controlando el flujo de conexiones internas y externas y por ende por este dispositivo debe circular todo el tráfico LAN y WAN. Por tal motivo debe poseer un Throughput adecuado para soportar todo el tráfico que pase a través de él. En la figura 14 se puede observar el máximo Throughput que puede manejar el firewall de la entidad.

Feature	Description
Firewall Throughput	Up to 450 Mbps
Maximum Firewall and IPS Throughput	• Up to 225 Mbps with AIP SSM-10 • Up to 375 Mbps with AIP SSM-20 • Up to 450 Mbps with AIP SSM-40
VPN Throughput	Up to 225 Mbps
Concurrent Sessions	280,000
IPsec VPN Peers	750
Premium AnyConnect VPN Peer License Levels*	2,10, 25, 50, 100, 250, 500, or 750
Security Contexts*	Up to 20
Interfaces	4 Gigabit Ethernet ports and 1 Fast Ethernet port
Virtual Interfaces (VLANs)	150
Scalability	VPN clustering and load balancing
High Availability	Active/Active**, Active/Standby

Figura 14 Especificaciones Cisco ASA 5520

Fuente: Propia

8.2.3 Plan de Integración

Para el plan de transición del protocolo IPv6 se debe evaluar el grado de afinamiento a nivel de hardware y software sobre la infraestructura actual de comunicación, como también un análisis del estado actual de los servicios de IT.

Con este diagnóstico se procederá a elaborar un plan de implementación de transición a protocolo IPv6, tal vez con recomendaciones pertinentes a que haya lugar respecto acciones a seguir, dependiendo de las capacidades de cada dispositivo de red, servidor, aplicaciones, servicios con su soporte para trabajar con IPv6

El alto grado de homogeneidad en la distribución y configuración de la red de comunicaciones, al pertenecer sus dispositivos a la misma marca Cisco, permite que la transición hacia IPv6 se realice en un entorno estandarizado, y recomendado por el fabricante, igualmente la segmentación y topología se prestan para realizar pruebas de IPv6 validando antes de la transición total de todas las áreas o VLAN,

La mayoría de los dispositivos que conforman la red cuentan con el soporte en su software, por lo cual no habría que realizar cambios físicos o de hardware sobre la infraestructura. Por ahora se contempla en actualizar sistemas operativos y activar los componentes que requiere IPv6.

Debido que a nivel mundial aún no se ha definido el día concreto para la implantación definitiva de IPv6 y la desaparición total de IPv4, se hace necesario seguir manteniendo la infraestructura y aplicaciones IPv4 mientras se avanza en la consolidación de IPv6 como el protocolo encargado del direccionamiento en Internet.

8.2.4 Requerimientos para la Integración de IPv6

Ahora que se ha analizado de manera general la situación actual de la red de datos, se deben plantear los requerimientos necesarios para el correcto funcionamiento de IPv6.

8.2.4.1 Hardware y Software

Muchos fabricantes de hardware, siendo conscientes del cambio que se avecina, han decido implementar IPv6 en sus equipos, sistemas operativos en routers, switch y firewall. Estos se encuentran almacenados en la memoria flash en caso de presentarse una necesidad de actualización del sistema operativo por una versión compatible con IPv6.

Analizando los componentes de red que son involucrados para la transición a IPv6 son del fabricante CISCO, este fabricante es compatible con este protocolo a partir de los siguientes sistemas operativos:

IOS 12.2(2)T, Switch y Routers,
IOS 7.2.101.0 Wireless LAN Controller

ASA Versión 7.0(1)

Los sistemas operativos descritos anteriormente cuentan con soporte y operatividad para el protocolo IPv6. Tanto los switch de acceso, switch de core, firewall y controladora de Wireless tienen su sistema operativo listo para activar sus características y funcionar con el protocolo IPv6.

Una recomendación importante es tener un monitoreo constante de los dispositivos involucrados en la transición, analizar y observar su comportamiento en la utilización de sus recursos de memoria, CPU y throughput, tanto antes, durante y después de la fase de pruebas, como también durante plan de transición y finalización del mismo.

Para el dispositivo de seguridad Cisco ASA 5520 se debe tener bastante cuidado, debido al alto grado de importancia en la red, a su desempeño y a la carga de trabajo (throughput) que actualmente presenta, como analizamos anteriormente.

Para la transición a IPv6 se adoptó el mecanismo recomendado por la IETF, como también el sugerido por los estudios previos a la implementación y establecidos en la licitación, el cual fue un DOUBLE STACK.

Doble Pila (DOUBLE STACK) es la forma más directa y sencilla de conseguir que un nodo sea IPv6/IPv4 pueden inter-operar directamente con nodos IPv4 e IPv6, poder ser equipado para soportar ambos protocolos y tener tres modos de operación:

- Con su pila IPv4 habilitada y su pila IPv6 no habilitada
- Con su pila IPv6 habilitada y su pila IPv4 no habilitada
- Con ambas pilas habilitadas

8.2.4.2 DNS y DHCP

Este mecanismo permite también ser activado sobre los servidores de DHCP para configuración de direcciones o utilizar los sistemas de autoconfiguración IPv6, en servidores DNS, sistema de nombres de dominio utilizando IPv4 e IPv6 para hallar coincidencias entre nombres de host y su dirección IP, el DNS también deber ser dotado de librerías que le permitan manejar registros IPv4(A) e IPv6 (A6/AAAA).

8.2.4.3 Servicios y Aplicaciones

Dependiendo de la complejidad del montaje de cada servicio por parte de cada proveedor de infraestructura y aplicaciones, los responsables deben plantear cuáles serían las recomendaciones y la mejor ejecución que se acomode a sus necesidades para no impactar el servicio y lograr la transición al protocolo IPv6, cuáles serían los escenarios de fases de pruebas, cronograma y finalización.

8.2.5 Protocolo de Pruebas

Existe una gran madurez a nivel de los productos y servicios de comunicaciones respecto a su cumplimiento de los estándares que definen IPv6. IPv6 es un protocolo maduro, de amplio desarrollo y soporte, pero, de todas formas, su adopción no alcanza de forma significativa a los usuarios finales.

El protocolo de pruebas, una metodología genérica propone para los sistemas de software con foco en IPv6 y gran parte de los componentes de infraestructura (switches, routers, tarjetas de red, sistemas operativos, drivers, etc.) soportan IPv6, y se pretende que las

aplicaciones maduren en el uso del protocolo. En la presente metodología se define el proceso de adecuación de sus sistemas informáticos para soportar el estándar. Se trata de una orientación para buscar y certificar que ciertos sistemas operan adecuadamente sobre IPv6.

8.2.5.1 Planificación de Pruebas

El primer paso en el protocolo de pruebas es definir qué se va a probar y qué no se va a probar. Estas pruebas pueden tener diferentes alcances: se pueden probar todas las funcionalidades de una de las interfaces (GUI, Web, Servicios Web, Bibliotecas, etc.), y se puede probar todas las funcionalidades de partes de la aplicación claramente definidas (módulos, subsistemas).

A partir de las interfaces a probar se registran todas las funcionalidades que se proveen. Luego se evalúa su prioridad para las pruebas según el riesgo que implican cambiar del protocolo IPv4 al IPv6. Las interfaces y funcionalidades a probar determinan el cubrimiento en extensión de las pruebas, mientras que su prioridad, determina su cubrimiento en profundidad, o sea la intensidad de las pruebas.

8.2.5.2 Diseño de las Pruebas

En esta etapa se define la estrategia de prueba para cada ítem del inventario de componentes e interfaces, Aplicaciones y servicios, se diseñan los casos de prueba y las misiones de testing exploratorio. Dado que las pruebas tienen el objetivo de detectar problemas con el manejo de las direcciones IP, se presentan una serie de ideas de prueba relacionadas a los datos que nos darán herramientas para diseñar casos adaptados al contexto. Es importante identificar también las funcionalidades asociadas a la comunicación de las aplicaciones y servicios, porque pueden ser otra fuente de problemas. Por último, es importante diseñar pruebas asociadas al ambiente en el cual se ejecuta la aplicación.

8.2.5.2.1 Configuración de las Aplicaciones en un Ambiente de Pruebas

Para la ejecución de todas las pruebas es necesario armar ambientes de pruebas. En primer lugar, si la aplicación se encontrase trabajando actualmente en IPv6, se creará un ambiente para ser probada. Si, en cambio, la aplicación se encuentra ejecutando en IPv4 se armará un ambiente IPv4 para su prueba.

Una vez probada, se deberá configurar la aplicación y el ambiente para su funcionamiento bajo IPv6. La idea fundamental de la configuración es filtrar las interfaces de interés, rechazando todos los paquetes IPv4. Toda configuración debe ser documentada por los administradores de la aplicación ya que es un insumo fundamental para conformar los ambientes de producción.

Eventualmente, en la prueba sobre IPv6 se podrán encontrar errores en el código fuente, en la configuración de la aplicación, en los componentes del ambiente o en su configuración. Para ejecutar las pruebas de regresión, se deberá corregir esos errores y documentarlos.

8.2.5.2.2 Ejecución de Pruebas

En primera instancia, si existe la posibilidad, se prueba la aplicación ejecutándose en su ambiente IPv4 (si se trata de una migración a IPv6). De esta manera, se tendrá información sobre el estado de la aplicación antes de los cambios (migración o ajustes en el código fuente). Los errores encontrados no serán atribuidos luego al cambio a IPv6. Estas pruebas son además una oportunidad para capturar tráfico en las interfaces de interés, a los efectos de validar experimentalmente cuáles son los servicios que hacen uso de las redes.

Luego, se comienza con la prueba exhaustiva de los ítems del inventario en un ambiente IPv6. Si el ambiente no logra ser IPv6 puro se monitorizan las interfaces donde pueden viajar paquetes IPv4. De existir problemas que no estaban en la versión IPv4 o que pueden ser

atribuibles a este protocolo, se detienen las pruebas hasta su corrección. Con la nueva versión se ejecutan pruebas de regresión sobre las funcionalidades donde se encontraron problemas y donde pueden impactar los cambios.

8.2.6 Análisis y Evaluación de Aplicativos

En esta etapa se revisa el material recogido en todo el proceso de trabajo y se analiza para determinar el nivel alcanzado. Este material será la evidencia de la realización de las pruebas y que cubre tanto los ítems del inventario de aplicaciones como las interfaces que no son IPv6. Mediante la organización de pruebas se consolida la información y experiencia recogida en el proyecto, para integrarla a la base de datos del conocimiento.

La mayoría de equipos de usuarios finales ubicados en todas las dependencias de la empresa FENIX utilizan el sistema Operativo Microsoft Windows Siete, esta versión del sistema operativo Windows se caracteriza por dar un soporte óptimo a una gran cantidad de aplicaciones, desarrollo, administrativas, lúdicas entre otras mientras que para los servidores que contienen las aplicaciones Corporativas predomina el sistema Operativo Windows Server 2008 ,2010 y LINUX Red Hat.

8.2.7 Plan de Seguridad para la Coexistencia de los dos Protocolos

Se revisó los RFC de seguridad, en especial el RFC 4942 que hace referencia a las consideraciones de seguridad para el proceso de coexistencia y transición a IPv6.

Se revisó el RFC 6177, cuya especificación técnica se refiere a las recomendaciones que deben seguir los clientes para solicitar asignación de segmentos de IPv6 en el rango de /48 a /56.

La fase de implementación del protocolo IPv6, se estructuró con base en los esquemas de seguridad de información, sobre los cuales se tenían contempladas las políticas de confidencialidad, integridad y disponibilidad de la empresa FENIX.

Se requirió definir un plan de marcha atrás (Plan de Contingencias), para enfrentar inconvenientes de indisponibilidad de los servicios que pudieran atentar contra la seguridad de la información y de las comunicaciones de la Entidad al momento de implementar el protocolo IPv6.

En el proceso de transición hacia el nuevo protocolo, se revisó la seguridad de información de las infraestructuras de TI, la seguridad de IPv6 y el nivel de impacto de servicios como el Directorio Activo, Sistemas de Nombres de Dominio - DNS, Correo Electrónico, Servicio de Protocolo de Configuración Dinámica de Host – DHCP (Definido en el RFC3315 para DHCPv6), Sistemas Proxy, Servicios de aplicaciones, Servicios Web y Sistemas de Gestión y Monitoreo.

Se generó la documentación necesaria que contempló aspectos de seguridad del entorno en los sistemas de comunicaciones, sistemas de información y sistemas de almacenamiento, que surgieron del desarrollo de la implementación de IPv6.

La implementación de IPv6 podría generar riesgos de seguridad de información, que impactarán en los servicios de la empresa FENIX y que podrían acarrear problemas; con el objeto de poder detectar estos riesgos se planeó hacer un análisis detallado que permitiera encontrar posibles vulnerabilidades y que en IPv6 es necesario hacer esta labor debido a que el protocolo se apoya en otros protocolos como IPSec, HTTP, TCP, UDP o SIP.

La verificación y el entendimiento de los componentes de seguridad diseñados para el protocolo IPv6 fueron claves para evaluar, monitorear y mejorar el desempeño de los servicios y aplicaciones bajo IPv6. En este sentido fue tenido en cuenta el documento sobre

"Política para la adopción de IPv6 en Colombia, estructuración y definición de Cintel y Mintic del año 2012", dice:

> *"Se debe dar paso a la transición de IPv4 a IPv6 como una herramienta para mejorar las condiciones de seguridad nacional y la seguridad de la información. Siempre que la adopción de IPv6 facilita las tareas de monitoreo y refuerza los protocolos de seguridad nacional, dado que con IPv6 cada usuario, cada equipo, cada terminal móvil puede recibir, de forma estática, una dirección IP que lo identifica, lo cual hace posible establecer con certeza la ubicación y el origen de la comunicación y permite adoptar medidas de seguridad que redundarán en beneficios para todos."*

Con respecto a lo anteriormente expuesto y teniendo en cuenta que el protocolo IPv6, debido a su gran cantidad de direcciones disponibles, no tiene como política manejar direcciones IP públicas o privadas, por lo que elimina toda clase de elementos que permite "esconder" direcciones IP públicas en la comunicación (como uso de NATs – Traducciones de red)), lo cual minimiza los riesgos de intrusión en la red; sin embargo lo anterior no quiere decir que el protocolo IPv6 sea más seguro que IPv4, pero el IPv6 si obliga a incorporar dentro del paquete IP al protocolo IPsec (eliminando la variedad de protocolos de seguridad existentes en IPv4), y al no requerir NATs, se puede utilizar IPsec, extremo-a-extremo, incrementando los niveles de seguridad en la red.

Para la implementación de un aspecto esencial de control de acceso en la capa IP se utilizó IPsec, el cual incluye una especificación mínima para una funcionalidad de firewall.

IPsec contiene las siguientes características:

- Integración a nivel de red, brindando seguridad de IP a los protocolos de capas superiores.

- IPsec es un componente embebido dentro de IPv6 que suministra control de acceso, autenticación de origen de datos, confidencialidad, integridad; es un esquema no orientado a la conexión, con independencia en los algoritmos de cifrado y negociación de compresión IP.

8.2.7.1 Redes Virtuales Privadas (VPN)

Como parte del diseño se contempló el caso que la Entidad tuviera como parte de su diseño una o varias conexiones privadas virtuales extremo a extremo que intercomunican dos o más redes locales (LAN). En este orden de ideas, el tráfico IPv6 puede pasar por muchos recursos compartidos en una red de amplia cobertura, razón por la cual, es necesario garantizar la seguridad del tráfico de las comunicaciones entre estas redes privadas virtuales con la utilización del protocolo IPSec.

8.2.7.2 Monitoreo de IPv6

El grado de control permite establecer el nivel de criticidad del monitoreo de redes IPv6, por lo que es necesario tener en cuenta: La detección y prevención de problemas, diagnóstico de fallas, determinación de acciones para la solución de problemas de seguridad y tener un plan de contingencias.

Las siguientes son las variables a tener en cuenta a la hora de realizar monitoreo de los servicios de red en IPv6:

- Medición de tráfico sobre interfaces y dispositivos de red.
- Estado de servicios
- Estado de aplicaciones y
- Actividad de los hosts.

8.2.7.3 Seguridad de IPv6 en los Centros de Datos

Al momento de implementar IPv6 en la entidad, los centros de datos fueron los elementos más importantes a revisar por ser los ejes centrales de todas las operaciones tecnológicas de

la entidad, de esta manera y atendiendo las recomendaciones que con respecto a esto da la empresa FENIX“Existen varias formas de introducir y operar IPv6 en Centros de Datos. Una forma es continuar con una operación IPv4 dentro del centro de datos y hacer algún tipo de translación en el borde, una segunda forma es usar la pila doble y una tercera es usar únicamente IPv6.

8.2.8 Inventario IT

Para la implementación de transición de IPv6 se realizó un levantamiento de información o inventario de la infraestructura actual de comunicaciones de la empresa FENIX de las telecomunicaciones, este inventario permitió desarrollar las labores de transición a IPv6 de una forma controlada ya que se enfocó en validar todos sus componentes desde su topología de red, funcionamiento, segmentación, hardware y software.

En la información recolectada se concentró con mayor vigor sobre los equipos de red que albergan las comunicaciones de la empresa FENIX (Switch de Acceso, CORE, Routers), como grupo principal, seguido del grupo de Servidores físicos y virtuales que prestan los servicios de aplicaciones y por ultimo un grupo de periféricos (PCs, Computador portátil, Impresoras, Teléfonos IP, etc).

Con este análisis y evaluación de capacidad de compatibilidad para soportar IPv6, se pudo habilitar el direccionamiento IPv6 en cada de los componentes o dispositivos de red que lo soportan.

8.2.9 Implementación de IPv6

Los bloques de direccionamiento en IPv6 cumplen con las políticas de seguridad y privacidad de la información, permitiendo que el funcionamiento de las mismas sea transparente para los usuarios finales dela empresa FENIX.

Los planes de direccionamiento en IPv6 se realizaron con base en los criterios de confidencialidad, integridad y disponibilidad de los sistemas de información y comunicaciones.

Se recomendó crear VLANs (Redes de Área Local Virtuales) por separado dentro de las redes locales de la entidad para propósitos de pruebas de direccionamiento, tráfico, monitoreo y seguridad.

8.2.9.1 Diseño de Direccionamiento IPv6

Se evidencio que el diseño de segmentación de la red de datos estaba enfocado por ciertas áreas y mayormente por piso a las cuales se les asigno una vlan para ser identificadas, como se púede observar en la gráfica No. Grafica No.1 Segmentación Lógica Red LAN de la empresa FENIX.

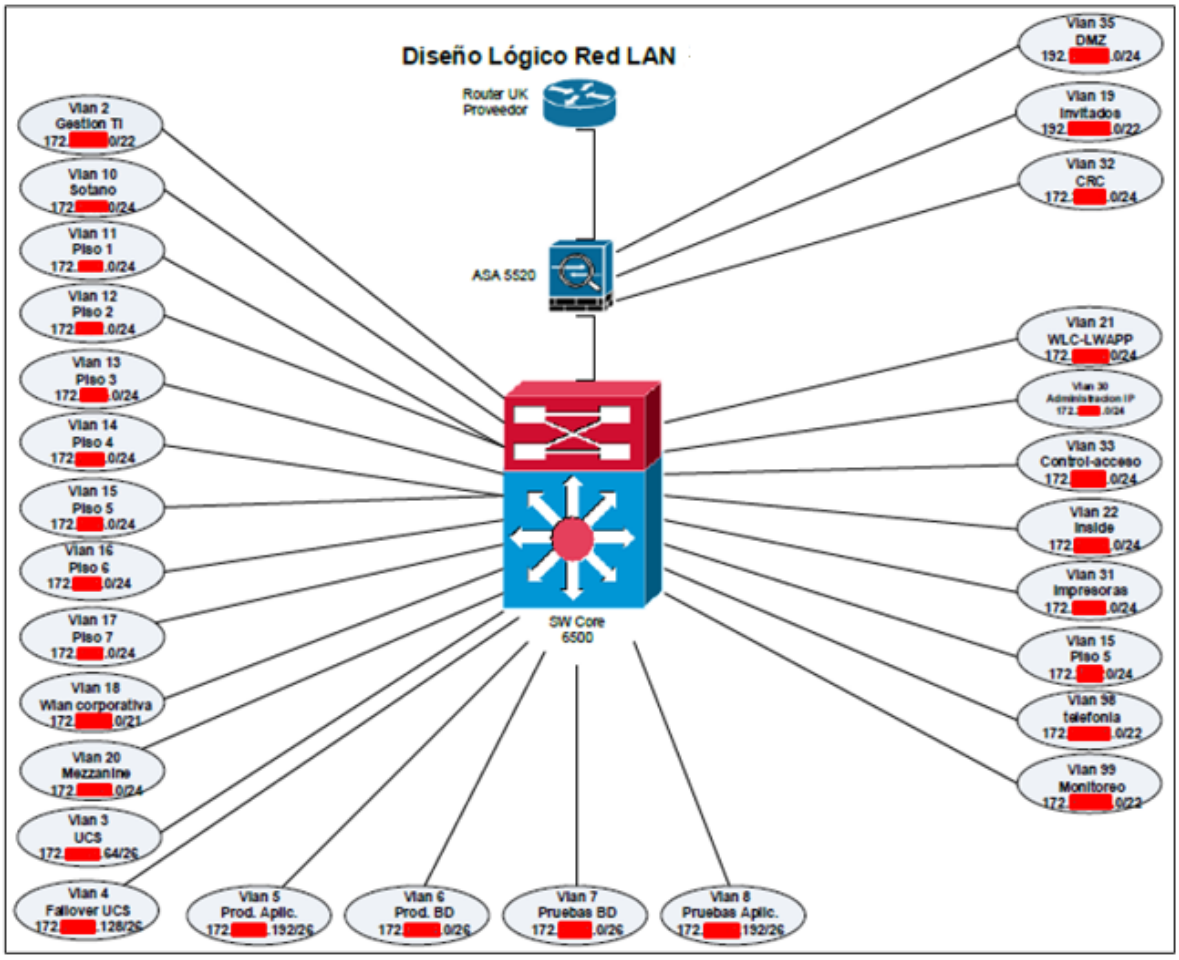


Figura 15 Segmentación Lógica Red LAN FENIX

Fuente: Propia

Una vez entregado el rango o pool de dirección IPv6 2801:11:400::/48, se procedió a realizar un diseño lógico de segmentación, siguiendo las recomendaciones sugeridas por el grupo RENATA, se toma cuatro (4) bits para dividir en 16 subredes de las cuales la segunda subred 2801:11:4000:1000::/52 se asignó a la sede Principal de la empresa FENIX.

Para mantener un mapeo con las vlan actuales y facilitar un análisis de falla para hacer familiar el nuevo rango de direcciones IPv6 se tomó el ID de vlan y se le asigno la subred correspondiente para su identificación como se muestra en la siguiente tabla No. Tabla No. 18 Direccionamiento IPv6.

IPV6	Asignación	VLAN	IPv4
2801:11:[redacted]:/52	Sito Sede Principal		
2801:11:[redacted]:/64	WAN		
2801:11:[redacted]:/64		Vlan1	192.[redacted]1
2801:11:[redacted]:/64	Servidores	Vlan2	172.[redacted].1
2801:11:[redacted]:/64	Gateway CIMC UCS	Vlan3	172.[redacted].65
2801:11:[redacted]:/64		Vlan4	172.[redacted].129
2801:11:[redacted]:/64	Gateway Capa Aplicacion	Vlan5	172.[redacted].193
2801:11:[redacted]:/64	Gateway Capa BD	Vlan6	172.[redacted].1
2801:11:[redacted]:/64	Ambiente BD Pruebas	Vlan7	172.[redacted].1
2801:11:[redacted]:/64	Ambiente Aplicacion Pruebas	Vlan8	172.[redacted].193
2801:11:[redacted]:/64	Data_Sotano	Vlan10	172.[redacted].1
2801:11:[redacted]:/64	Data_Piso1	Vlan11	172.[redacted].1
2801:11:[redacted]:/64	Data_piso2	Vlan12	172.[redacted].1
2801:11:[redacted]:/64	Data_piso3	Vlan13	172.[redacted].1
2801:11:[redacted]:/64	Data_piso4	Vlan14	172[redacted].1
2801:11:[redacted]:/64	Data_piso5	Vlan15	172.[redacted].1
2801:11:[redacted]:/64	descData_piso6	Vlan16	172.[redacted].1
2801:11:[redacted]:/64	Data_piso7	Vlan17	172.[redacted].1
2801:11:[redacted]:/64	--wireless--	Vlan18	172.[redacted].1
2801:11:[redacted]:/64	Data_Mezzanine	Vlan20	172.[redacted].1
2801:11:[redacted]:/64		Vlan21	172.[redacted].1
2801:11:[redacted]:/64	INSIDE	Vlan22	172.[redacted].1
2801:11:[redacted]:/64	Administracion_IP	Vlan30	172.[redacted].1
2801:11:[redacted]:/64	Impresoras	Vlan31	172.[redacted].1
2801:11:[redacted]:/64		Vlan33	172.[redacted].1
2801:11:[redacted]:/64	Gestión	Vlan40	172.[redacted].1
2801:11:[redacted]:/64	Control_Acceso_RFID	Vlan41	172.[redacted].1
2801:11:[redacted]:/64	Actualizaciones Configuration Manager	Vlan43	172.[redacted].1
2801:11:[redacted]:/64	Vlan Autenticacion ISE	Vlan44	172.[redacted].1
2801:11:[redacted]:/64	[redacted]_WIFI_VIP	Vlan51	172.[redacted].1
2801:11[redacted]:/64	Voz_IP	Vlan98	172.[redacted].1
2801:11:[redacted]:/64	Vlan_Monitoreo&SIUP_Simona	Vlan99	172[redacted]1

Tabla 4 Direccionamiento IPv6

Fuente: Propia

IPV6	Asignación	VLAN	IPv4
2801:11:[redacted]/64	Despacho [redacted]	Vlan100	172.[redacted].1
2801:11:[redacted]/64	Of_Asesora_Planeacion_y_Estudios	Vlan101	172.[redacted].1
2801:11:[redacted]/64	Oficina de TI	Vlan102	172.[redacted].1
2801:11:[redacted]/64	Oficina_Asesora_Juridica	Vlan103	172.[redacted].1
2801:11:[redacted]/64	Oficina_de_Control_Interno	Vlan104	172.[redacted].1
2801:11:[redacted]/64	Oficina_Internacional	Vlan105	172.[redacted].1
2801:11:[redacted]/64	Oficina_Asesora_de_Prensa	Vlan106	172.[redacted].1
2801:11:[redacted]/64	Asesor_[redacted]	Vlan107	172.[redacted].1
2801:11:[redacted]/64		Vlan108	172.[redacted].1
2801:11:[redacted]/64	Direccion_de_Vigilancia_y_Control	Vlan109	172.[redacted].1
2801:11:[redacted]/64	Direccion_de_Industria_[redacted]	Vlan110	172.[redacted].1
2801:11:[redacted]/64	Direccion_de_Conectividad	Vlan111	172.[redacted].1
2801:11:[redacted]/64	Direccion_de_Promocion_[redacted]	Vlan112	172.[redacted].1
2801:11:[redacted]/64	Direccion_de_Apropiacion_[redacted]	Vlan113	172.[redacted].1
2801:11:[redacted]/64	Gr_Recursos_y_Actuaciones_Admin	Vlan114	172.[redacted].1
2801:11:[redacted]/64	Despacho_[redacted]	Vlan115	172.[redacted].1
2801:11:[redacted]/64	Dir_de_Politicas_y_Desarrollo_[redacted]	Vlan116	172.[redacted].1
2801:11:[redacted]/64	Dir_de_Gobiemo_en_Linea	Vlan117	172.[redacted].1
2801:11:[redacted]/64	Dir_de_Estandares_y_Arq_[redacted]	Vlan118	172.[redacted].1
2801:11:[redacted]/64	Secretaria_General	Vlan119	172.[redacted].1
2801:11:[redacted]/64	Subdirec_Admin_y_Gestion_Humana	Vlan120	172.[redacted].1
2801:11:[redacted]/64	Subdireccion_Financiera	Vlan121	172.[redacted].1
2801:11:[redacted]/64	Grupo_de_Contratacion	Vlan122	172.[redacted].1
2801:11:[redacted]/64	Gr_Control_Interno_Disciplinario	Vlan123	172.[redacted].1
2801:11:[redacted]/64	Of_Gestion_Ingresos_[redacted]	Vlan124	172.[redacted].1
2801:11:[redacted]/64	[redacted]	Vlan125	172.[redacted].1
2801:11:[redacted]/64	Proveedores	Vlan126	172.[redacted].1
2801:11:[redacted]/64	Dispositivos_Moviles_[redacted]	Vlan127	172.[redacted].1
2801:11:[redacted]/64		Vlan200	172.[redacted].1
2801:11:[redacted]/64		Vlan201	172.[redacted].33
2801:11:[redacted]/64		Vlan202	172.[redacted]65
2801:11:[redacted]/64		Vlan203	172.[redacted]97
2801:11:[redacted]/64		Vlan204	172.[redacted].129

Tabla 5 Continuación Direccionamiento IPv6

Fuente: Propia

8.3 Fase II Implementación

8.3.1 Desarrollo del Plan de Implementación

Inicialmente se realizó la ejecución y configuración del piloto de pruebas de IPv6, analizando el comportamiento de cada dispositivo de la red de comunicaciones, agregando carga, servicios y usuarios finales, pruebas realizadas utilizando las mejores prácticas y metodologías de transición a IPv6, como la técnica de doble pila o Dual stack.

Obteniendo los resultados del piloto de pruebas, las actividades principales desarrolladas en esta segunda fase, fue básicamente la activación y configuración de las funciones del protocolo IPv6 para cada uno de los dispositivos de red de comunicaciones que componente la infraestructura de comunicaciones de la empresa FENIX, esto de acuerdo al plan de diagnóstico de la primera Fase del proceso de transición a IPv6 y teniendo en cuenta la topología e inventario de los activos de información de la empresa FENIX.

8.3.2 Ejecución de Configuraciones Piloto de Pruebas de IPv6

La transición a IPv6 es una labor que implicó ir paso por paso, un proceso evolutivo que empezó con la implantación del nuevo protocolo en la infraestructura de servicios de red, para continuar luego con la modificación y adaptación de aplicaciones, servicios y sistemas, acabando con la extensión de IPv6 a la mayor parte de dispositivos interconectados a la red.

Para facilitar y estandarizar el proceso de transición se realizaron pruebas en los segmentos de red y se tuvo un segmento de pruebas con pocos equipos y usuarios, en donde se aprovechó la homogeneidad de la red. Esto permitió afianzar y trasladar la implantación a segmentos de red cada vez más extensos con servicios de filtrados críticos y evitar traumatismos en el normal funcionamiento de la red de la empresa FENIX.

La transición a IPv6 fue de la mano con la generación o adaptación de aplicaciones que utilizaron este protocolo, ya que no tiene mucho sentido dotar la red con IPv6 si no se cuenta con aplicaciones que puedan aprovechar las ventajas este.

El objetivo principal de las pruebas fue visualizar el comportamiento general de tráfico de IPv4 e IPv6 (Doble Pila), y así garantizar la compatibilidad entre ambas versiones dependiendo de los servicios, mientras IPv6 es consolidado en la red.

8.3.2.1 Configuraciones Iniciales del Piloto de Pruebas de IPv6

Para tener una zona controlada en donde se realicen las pruebas de funcionalidad del nuevo protocolo de comunicaciones IPv6, se requirió aislar un segmento de red. Para esto se creó un nuevo segmento de red, el cual permitió hacer los cambios y activaciones necesarias para confirmar las funciones de IPv6 sin afectar a usuarios o segmentos en producción, esto también con el fin de seguir las recomendaciones y mejores prácticas sugeridas en todos los manuales de implementación de transición de IPv6, como también las líneas de guía por parte de LACNIC.

8.3.2.2 Equipos Configurados para el Piloto de Pruebas

Habiendo ya realizado la fase de planeación, donde se analizaron los principales dispositivos de infraestructura de red, de donde se obtiene un diagrama topológico y se enumeran los equipos de red a intervenir y configurar para lograr el objetivo de tener una zona controlada de pruebas en IPv6 a los cuales se les activará los componentes del nuevo protocolo.

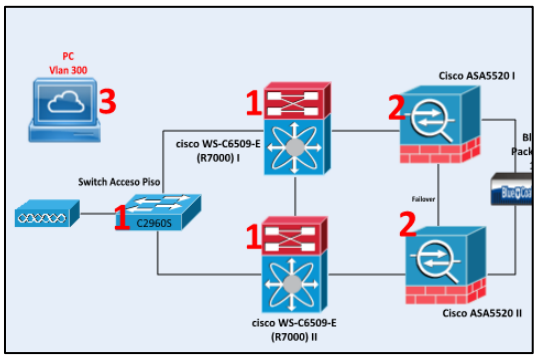


Figura 16 Diagrama Equipos Configurados para Pruebas IPv6

Fuente: Propia

8.3.2.3 Creación VLAN 300 para Pruebas IPv6

Inicialmente se creó una Vlan con ID 300 y con la descripción Prueba IPv6 sobre el dispositivo de red uno (1) Switch CORE Cisco WS-C6509, Ver *Figura 16. E*sta Vlan 300 fue configurada en modo "Dual Stack" con lo cual se cumple con las recomendaciones por parte del Ministerio y LACNIC para la convivencia de ambos protocolos, IPv4 e IPv6. En la Figura 17 se puede observar la configuración de una IP de 32 bits 172.27.250.0/24 para protocolo IPv4 y otra de 128bits 2801:11:4000:1001::0/64 para protocolo IPv6. Utilizando un DHCP IPv6 sin estado a los usuarios en esta Vlan 300 se les asignó una IP dinámica:

```
SWCOREMinTic#show run inter vlan 300
Building configuration...

Current configuration : 214 bytes
!
interface Vlan300
 ip address 172.[redacted].1 255.255.255.0
 ip helper-address 172.[redacted].144
 ipv6 address 2801:11:[redacted]::1/64
 ipv6 enable
 ipv6 dhcp relay destination 2801:11:[redacted]::144 Port-channel5
end
```

Figura 17 Configuración VLAN 300 Switch CORE

Fuente: Propia

El segundo (2) equipo que se intervino y configuró para activar el protocolo IPv6 fue el dispositivo de seguridad Firewall ASA, Ver Figura 16, donde se activó IPv6 sobre las

interfaces actuales en operación INSIDE y OUTSIDE, la interface INSIDE permite recibir el tráfico de la VLAN 300 con protocolo IPv6 e IPv4 (Dual Stack) y la interface OUTSIDE permite conectar la vlan 300 a la salida de internet con ambos protocolos IPv6 e IPv4, como se muestra en las líneas de configuración del Cisco ASA 5520 figura 18:

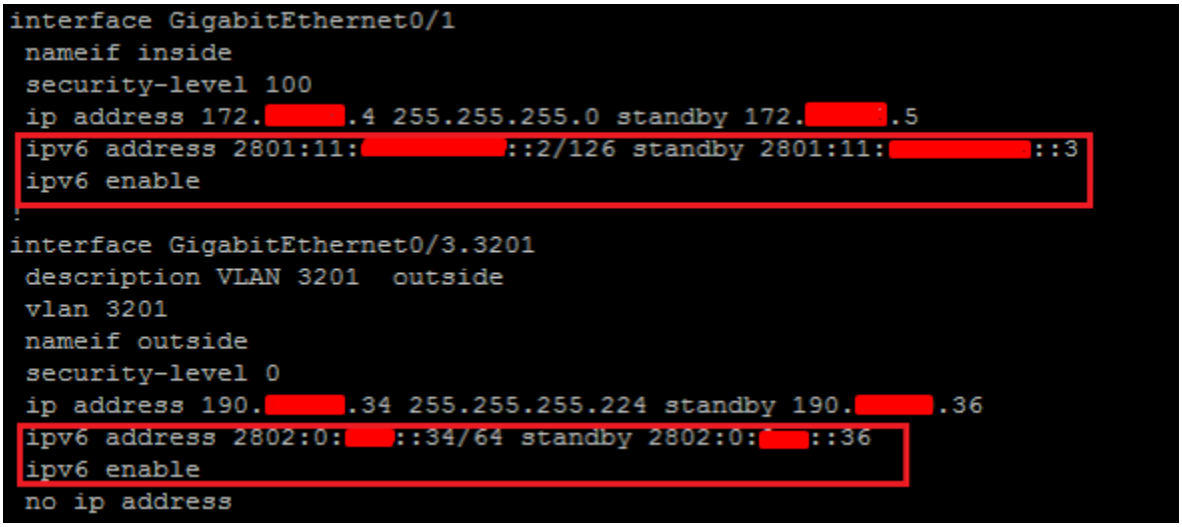


Figura 18 Configuración Cisco Firewall ASA 5520

Fuente: Propia

Adicionalmente se configuraron rutas estáticas para encaminar el tráfico de salida y retorno de respuestas de la vlan 300 usando el protocolo IPv6, como también una ruta por defecto apuntando hacia la salida del proveedor de Internet IFX, figura 19:

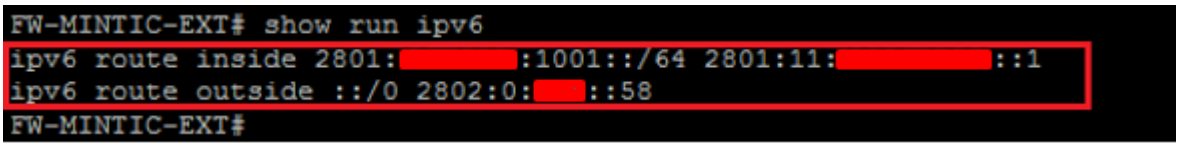


Figura 19 Rutas Estáticas IPv6 Firewall

Fuente: Propia

Por último, se trabajó en conjunto con el ISP, para realizar publicación del pool IPv6 (2801:11:4000:/48) de la empresa FENIX a nivel público y su respectivo enrutamiento interno y externo de la infraestructura de red del ISP.

8.3.2.4 Pruebas de Tráfico Realizadas Sobre la VLAN 300

Para la realización de estas pruebas, el objetivo principal fue tener un PC en la Vlan 300 con funcionalidad en Dual Stack, a éste se le verificaron sus conexiones, servicios y aplicaciones tanto en IPv4, como en IPv6. Luego de confirmar la estabilidad de la Vlan 300, se agregaron más usuarios para que realizaran sus labores cotidianas en servicios y aplicaciones de la empresa FENIX.

Posteriormente se procedió a conectar un PC en la red de la empresa FENIX a través de un switch de acceso de Piso, para verificar la asignación de una dirección IP en versión 4 y en versión 6. Esta asignación se da de forma dinámica por los servidores DHCP IPv4 e IPv6, con sus respectivas IP de puerta de enlace y servidores DNS para resolución de nombres. Esto confirmó la correcta función del servidor DHCP. Como se puede observar en la Figura 20, al PC conectado a la red se le asignaron las siguientes direcciones IPv4, v6, Puerta de enlace y DNS:

Dirección IPv4: 172.27.250.36
Dirección IPv6: 2801:11:4000:1001::15
Puerta de Enlace IPv4: 172.27.250.1
Puerta de enlace IPv6: 2801:11:4000:1001:1
Servidores DNS IPv4: 172.23.24.144
Servidores DNS IPv62801:11:4000:1002::144

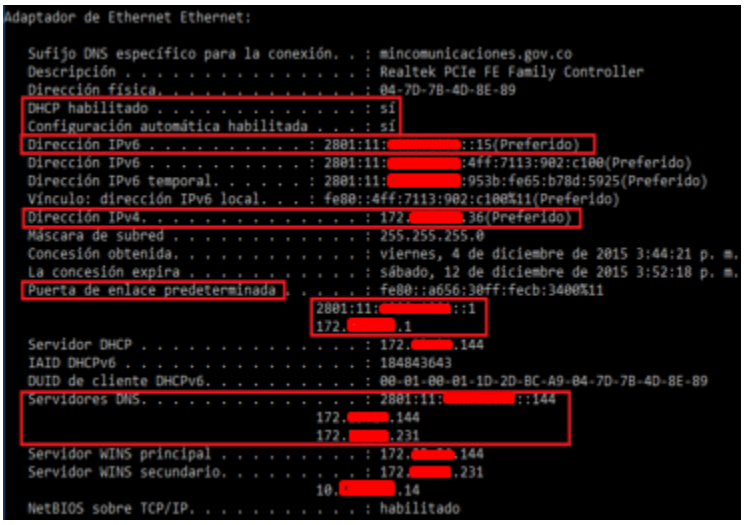


Figura 20 Direcciones IP Asignadas Para el PC en la VLAN 300

Fuente: Propia

Al revisar la respuesta de la puerta de enlace para la vlan 300 tanto para IPv4 como para IPv6, se realizó una prueba de ping donde se verificó que no existe perdida de paquetes y los tiempos de respuesta son óptimos y normales para una red LAN. Figura 21.

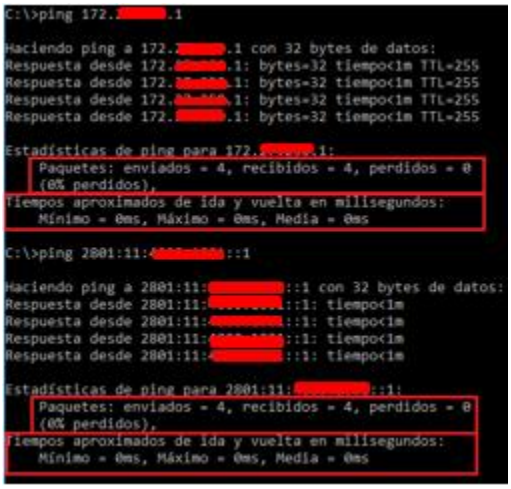


Figura 21 Respuestas Puerta de Enlace Vlan 300

Fuente: Propia

Continuando con el set de pruebas, para la verificación del correcto funcionamiento del servidor DNS en IPv6. Se realizaron pruebas de nslookup para los destinos www.google.com y www.youtube.com. El servidor DNS 2801:11:1002::144 entregó las direcciones IPv6 e IPv4 de los sitios solicitados, como se puede observar en la figura 22:

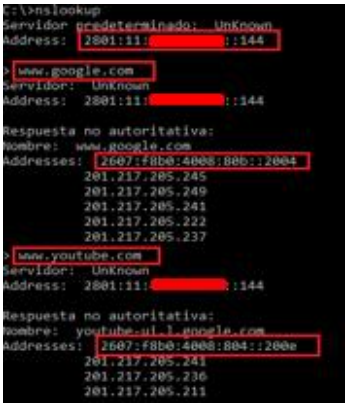


Figura 22 DNS IPv6 Para VLAN 300

Fuente: Propia

Al realizar una traza hacia destinos que están configurados en protocolo IPv6, se puede observar que el PC prefiere por defecto realizar esta conexión con el protocolo IPv6 y esto se puede ver en la figura 23:

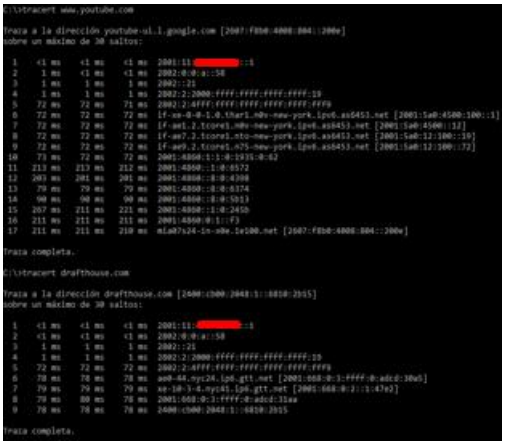


Figura 23 Trazas hacia páginas que Operan en IPv6

Fuente: Propia

Algo que puede llegar a suceder es que un destino web no tenga disponibilidad para el protocolo IPv6 o solo esté funcionando en IPv4, cuando esto pase, este destino web será resuelto por el protocolo IPv4, como se puede observar en la figura 24:

Figura 24 Tráfico en IPv4 (Dual Stack)

Fuente: Propia

Con los resultados de las pruebas anteriores se comprueba que ya se puede tener navegación hacia páginas en internet tanto en IPv6 como en IPv4. Una página de ejemplo de navegación de un usuario con protocolo IPv6 fue hacia www.drafthouse.com desde un PC en la Vlan ID 300 como se puede observar en la figura 25:

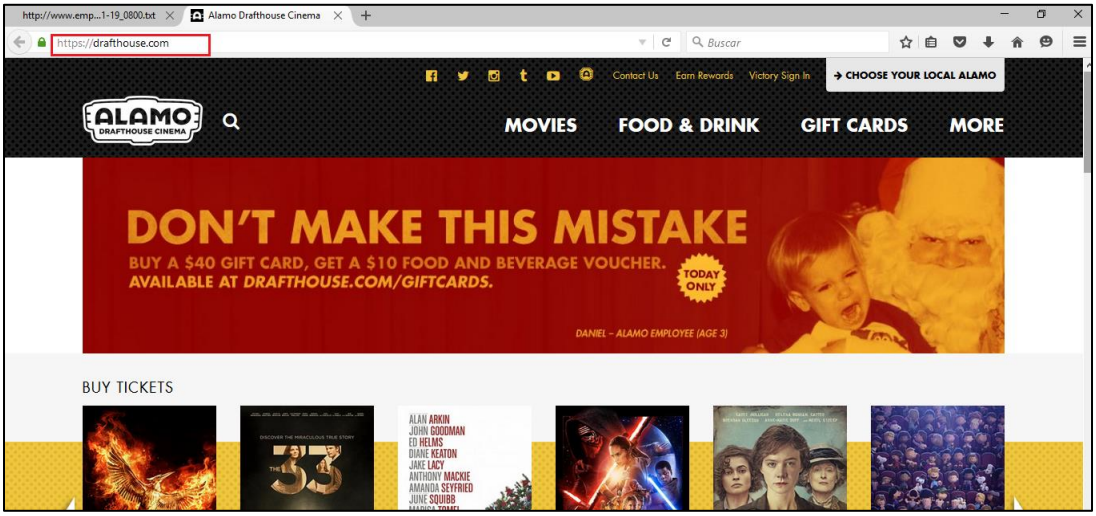


Figura 25 Ejemplo de Navegación Paginas en IPv6

Fuente: Propia

Una forma de hacer una comprobación de los servicios y funciones de IPv6 para la vlan 300, es por medio de páginas de test de IPv6, por ejemplo www.test-ipv6.com, la cual indica que se está usando una configuración correcta. Esto se puede observar en la figura 26:

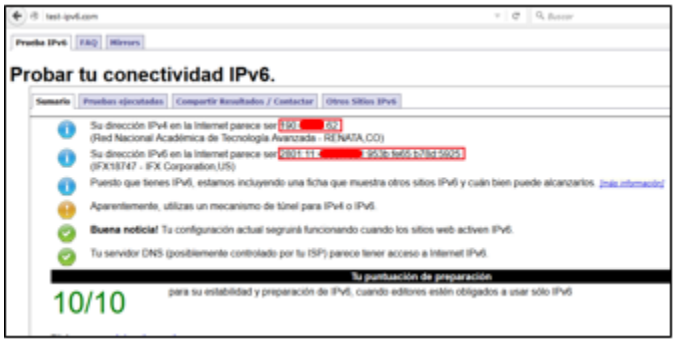


Figura 26 Test IPv6

Fuente: Propia

Durante las pruebas de carga y tráfico para la Vlan 300, se creó una lista de máximo 10 usuarios finales a los cuales se agregaron a esta Vlan para que realizaran sus labores diarias de trabajo y monitorear si ocurre algún inconveniente de algún servicio o aplicación.

Al revisar sobre el switch de core de la empresa FENIX se observaron usuarios sobre la Vlan 300, como también las vlan de Servidores 2 y 3 donde están alojados los servicios de DNS y controladores de dominio. En la figura 27 se pueden observar los usuarios de la vlan 300 con sus respectivas direcciones IPv6:

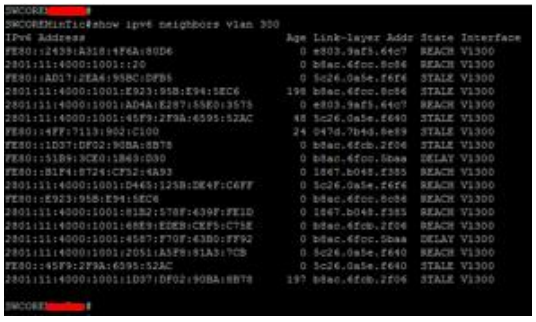


Figura 27 Usuarios VLAN 300

Fuente: Propia

Sobre el dispositivo de seguridad Firewall ASA5520 se puede observar el tráfico de la Vlan 300 circulando hacia internet por puerto 80 http, también solicitudes en puerto 443 https, todas estas conexiones se observan en IPv6 en la figura 28:

Figura 28 Usuarios VLAN 300

Fuente: Propia

Analizando el tráfico desde internet hacia los PC de usuarios internos o servidores, se puede observar que las políticas de seguridad aplicadas para IPv6 están funcionando de manera óptima para filtrar las conexiones y dejar pasar solo las necesarias. En la interface OUTSIDE se permite únicamente protocolo Icmpv6, y para transacciones de salida se permite el puerto 53 Domain para resolución de nombres como se puede ver en la figura 29:

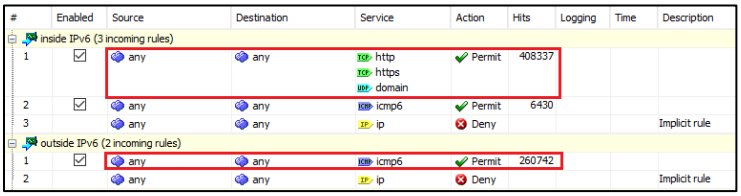


Figura 29 Políticas de Seguridad IPv6

Fuente: Propia

Al realizar pruebas de conexión desde un servidor externo con configuración en IPv6, se observa de forma satisfactoria que las respuestas hacia servidores internos de la empresa FENIX por protocolo Icmpv6 son satisfactorias como se puede observar en la figura 30:

Figura 30 Políticas de Seguridad IPv6

Fuente: Propia

En este momento se concluye que los usuarios sobre la Vlan 300 no han reportado inconvenientes de alguna conexión, servicio o aplicación y se tiene en monitoreo el tráfico de esta Vlan 300, como también el procesamiento del firewall ASA 5520.

8.3.3 Dispositivos Intervenidos en la Activación y Configuración del protocolo IPv6 en el Hardware y Software de la empresa FENIX

Con el análisis de topología realizado previamente de los equipos de comunicaciones principales de la infraestructura de red de la empresa FENIX, se procedió a la activación sus componentes de IPv6 para iniciar pruebas de funcionalidad y compatibilidad para el nuevo protocolo y así empezar a brindar el servicio a todos los usuarios de la empresa FENIX.

A continuación se ilustra el diagrama de red de la empresa FENIX y los equipos principales a intervenir para otorgar IPv6, en esta figura 31 se enumera el orden de configuración para cada dispositivo, el cual fue analizado previamente con el fin de evitar alguna falla de comunicación o alteración de los servicios prestados por cada dispositivo, según su rol en la topología de red e importancia.

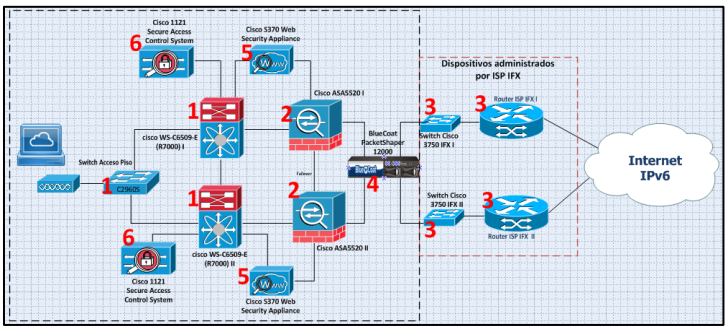


Figura 31 Diagrama de Dispositivos de Red Implementados en IPv6

Fuente: Propia

Tenido en cuenta lo anteriormente expuesto se empezó por el dispositivo marcado 1 Switch CORE Cisco WS-C6509, ya que este administra el direccionamiento IPv4 de todas las interfaces Vlan de la empresa FENIX, en este dispositivo se activa el soporte de IPv6 mediante el comando “IPv6 Enable”, en cada una de las 64 interfaces Vlan que tiene en operación y se asigna una IPv6 según direccionamiento interno de la entidad.

A continuación, en la Figura 32 se muestra las líneas de configuración realizada en el dispositivo **Switch CORE Cisco WS-C6509** de la empresa FENIX, ingresado los comandos correspondientes de activación IPv6 en la Interface vlan 2 Servidores, Interface Vlan 5 Gateway Capa Aplicación, y por ultimo interface vlan 22 INSIDE la cual está conectada para la salida toda hacia internet de la empresa FENIX

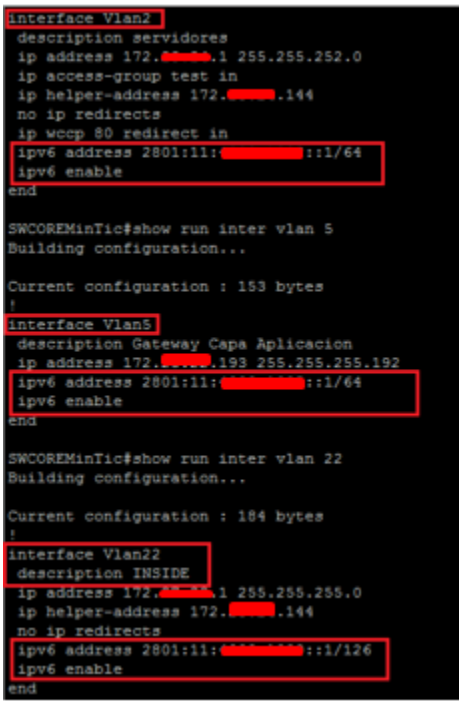


Figura 32 Configuración Switch de Core Cisco WS-C6509

Fuente: Propia

Para el dispositivo número 2 el cual es el Firewall “Cisco ASA5520 ver en la *Figura 22*” utilizado por la entidad y que es altamente importante en su rol en seguridad, se activaron sus funciones de IPv6 igualmente con el comando “IPv6 Enable” y se asigna una IPv6 según plan de direccionamiento sobre las interfaces que actualmente tiene en operación como lo es su Interface GigabitEthernet0/3.3201 Outside y en la interface GigabitEthernet0/1 Inside.

Como se observa en la *Figura 32* para la interface Inside se asignó la dirección IPv6 2801:11:4000:1000::2/126 la cual pertenece al rango de direccionamiento WAN IPv6 según direccionamiento interno de la entidad.

Para configurar la interface Outside Vlan 3201, se debido interactuar y trabajar conjuntamente con el ISP durante una semana buscando la mejor solución para la activación del protocolo IPv6, analizando la topología actual sin causar intermitencias o fallas de

comunicación. Para establecer el canal de comunicación en IPv6, se configuro una dirección 2802:0:0:a::34/64 en el extremo del firewall asignada por parte del proveedor ISP, y una IPv6 de puerta de enlace 2802:0:0:a::58/64 con el fin de integrar las comunicaciones con los equipos de enrutamiento del ISP.

Por último, el ISP realizo publicación del pool IPV6 de la empresa FENIX a nivel mundial y su respectivo enrutamiento interno y externo.

En la figura 33, se observa la configuración resultante en modo grafico después de ingresar los comandos correspondientes. Ver Figura 34.

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	VLAN
GigabitEthernet0/0		Yes				native
GigabitEthernet0/0.700		Yes				vlan700
GigabitEthernet0/0.701		Yes				vlan701
GigabitEthernet0/1	inside	Yes	100	172.[redacted].4 2801:11:[redacted]::2	255.255.255.0 126	native
GigabitEthernet0/2	dmz	Yes	30	192.[redacted].1	255.255.255.0	native
GigabitEthernet0/3		Yes				native
GigabitEthernet0/3.3201	outside	Yes	0	190.[redacted].34 2802:0:[redacted]:34	255.255.255.224 64	vlan3201
GigabitEthernet0/3.3202	MPLS_JPX	Yes	10	10.[redacted].1	255.255.255.248	vlan3202
Management0/0		Yes				native
Management0/0.32	ravec	Yes	40	172.[redacted].3	255.255.255.0	vlan32
Management0/0.36	RTIC	Yes	45	10.[redacted]97	255.255.255.248	vlan36
Management0/0.50	invitados	Yes	41	192.[redacted].1	255.255.252.0	vlan50
Management0/0.70	RENATA	No	46	190.[redacted]194	255.255.255.192	vlan70

Figura 33 Configuración Interfaces Firewall ASA 5520 en IPv6

Fuente: Propia

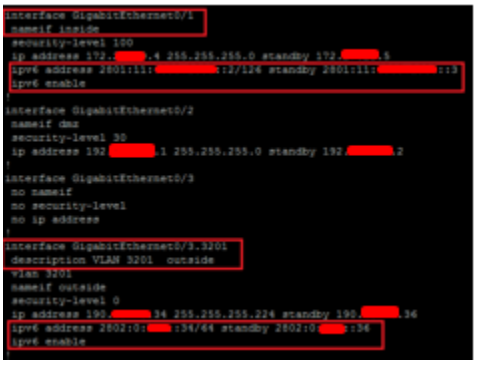


Figura 34 Configuración Firewall ASA 5520

Fuente: Propia

Una parte vital del dispositivo número 2 “Cisco ASA5520” ver Figura 31, son las funciones de seguridad que debe desarrollar para mantener segura la red interna. Ahora con el protocolo de internet versión 6 y para fines de realizar pruebas en IPv6, se configuran reglas básicas para tener tráfico permitido con los protocolos IP (TCP Http, https, Icmpv6) y (UDP Domain), para la interface Inside.

El trafico permitido para la interface Outside se configura mediante listas de acceso que únicamente da ingreso o respuesta del protocolo icmpv6 con el fin de validar conectividad desde internet, ver figura 35.

```
FW-[redacted]-EXT#
FW-[redacted]-EXT# show run ipv6
ipv6 route outside ::/0 2802:0:0:a::58
ipv6 access-list inside_access_ipv6_in permit object-group DM_INLINE_SERVICE_17 any any
ipv6 access-list inside_access_ipv6_in permit icmp6 any any
ipv6 access-list outside_access_ipv6_in permit icmp6 any any
FW-[redacted]-EXT#
```

Figura 35 Comandos Políticas de Seguridad de IPv6

Fuente: Propia

Una vez implementadas las políticas de seguridad, se muestra el resultado de la configuración y activación de IPv6, en modo grafico de administración del Cisco ASA5520, donde se puede observar la columna de Hits que nos indica la existencia de tráfico circulando por la interface en IPv6, siendo verificado, revisado y asegurado por el dispositivo.

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
MPLS_IPX IPv6 (2 implicit incoming rules)									
RENATA IPv6 (2 implicit incoming rules)									
RTIC IPv6 (2 implicit incoming rules)									
dmz IPv6 (2 implicit incoming rules)									
inside IPv6 (3 incoming rules)									
1	☑	any	any	http https domain	Permit	160844			
2	☑	any	any	icmp6	Permit	1637			
3		any	any	ip	Deny				Implicit rule
invitados IPv6 (2 implicit incoming rules)									
outside IPv6 (2 incoming rules)									
1	☑	any	any	icmp6	Permit	67375			
2		any	any	ip	Deny				Implicit rule
ravec IPv6 (2 implicit incoming rules)									

Figura 36 Políticas de Seguridad Modo Gráfico IPv6

Fuente: Propia

Dando continuidad se configuro los dispositivos numero 3 (tres) ver Figura 31, administrados y soportados por el proveedor ISP, las cuales no son posible mostrar por políticas de seguridad por parte de este proveedor.

El BlueCoat PacketShaper marcado con numero 4 (Cuatro) ver Figura 31, el cual permite aplicar políticas de calidad de servicio o balanceo sobre los canales de internet para las Vlan de la empresa FENIX. De primera instancia se creó la regla general de tráfico sobre IPv6, para identificar usuarios y servicios, los cuales ya están utilizando este nuevo protocolo de conexión versión 6, como se puede observar en la Figura 37:

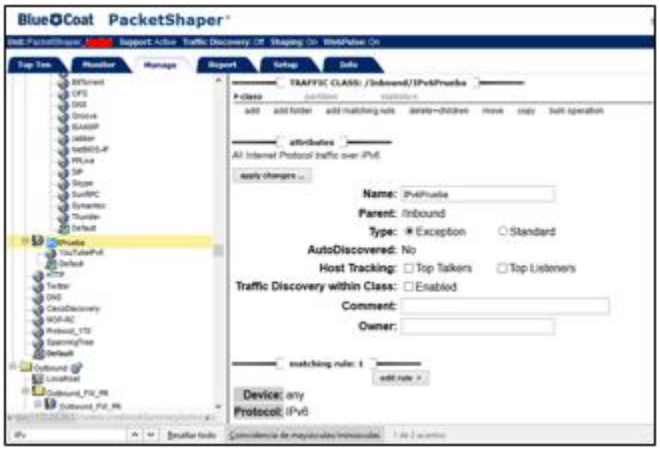


Figura 37 Creación de Política General de IPv6

Fuente: Propia

Ya identificado cierto tipo de tráfico circulando y para verificar que este establecido el IPv6, se creó una regla para filtrar tráfico de youtube.com en IPv6 o tipo de tráfico que contenga videos, para efectos de la prueba se creó la regla “YouTubeIPv6” como se observa en la figura 38:

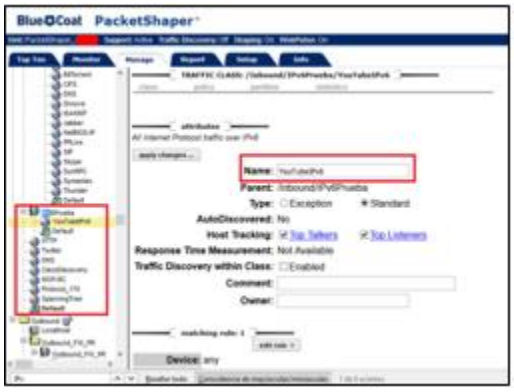


Figura 38 Regla de You Tube IPv6

Fuente: Propia

Por ultimo verificando el tráfico identificado, se pudo obtener la gráfica de consumo de ancho de banda para el protocolo o servicio audio/Videoclips de la regla “YouTubeIPv6”. Figura 39.

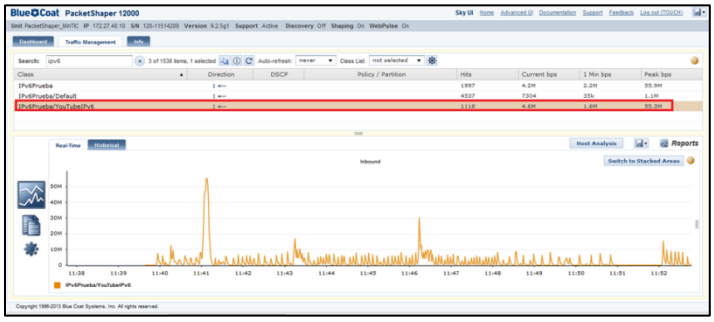


Figura 39 Regla Gráfica para YouTube IPv6

Fuente: Propia

Se realizaron las configuraciones necesarias sobre los dispositivos Cisco Web Security Appliance, para lograr tener servicios de seguridad en páginas web (5) ver Figura 31, se agregaron listas de acceso en IPv6 para filtrar el tráfico y ser analizado, también se especificó a donde dirigir el tráfico por medio del sistema Web Cache Control Protocol. Figura 40:

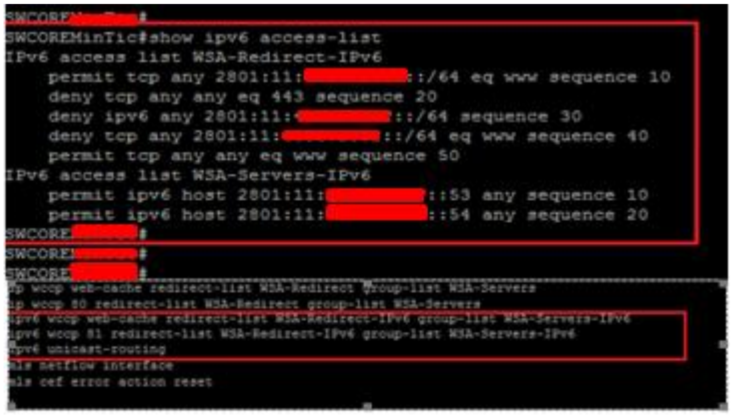


Figura 40 Configuración WCCP IPv6 y WSA

Fuente: Propia

Para lograr esto de debió hacer una actualización de Sistema Operativo del Switch 6500 CORE, la cual se realizó de forma controlada por medio de una solicitud de RFC, siendo ejecutada con éxito.

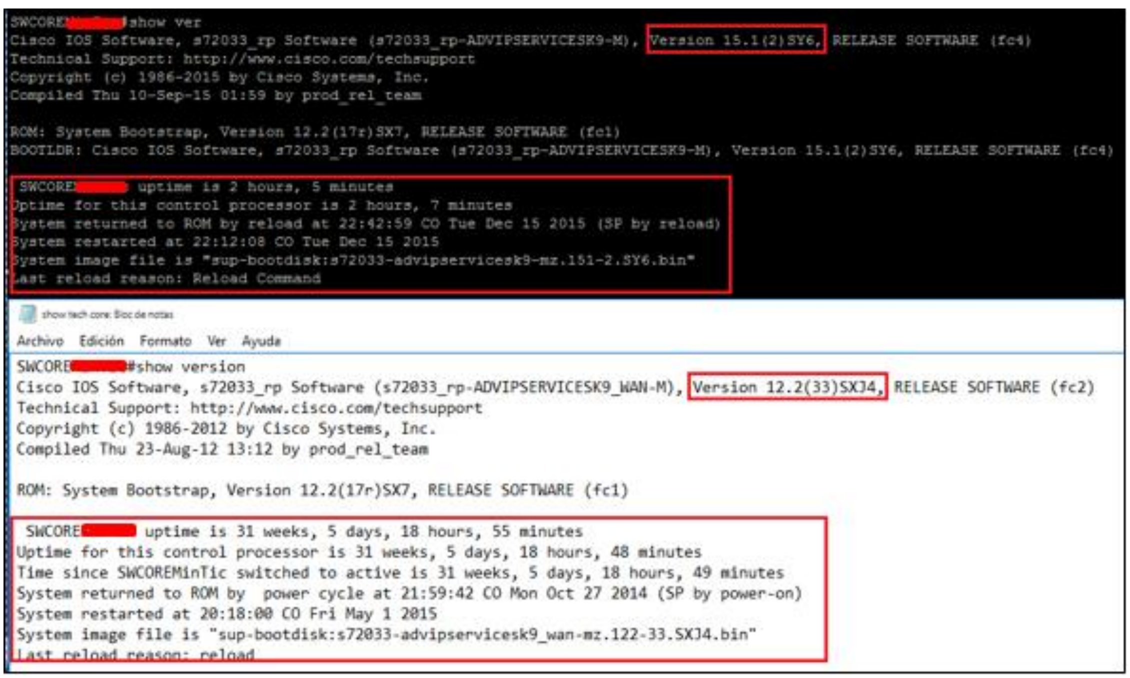


Figura 41 Actualización de IOS Switch 6500 Core

Fuente: Propia

Al finalizar la actividad se ejecutó la siguiente lista de chequeo:

- Validación de comunicación y servicios de red desde los switch de acceso de cada piso de la empresa FENIX
- Autenticación de usuarios al directorio activo
- Validación de servicio del ACS contra el directorio activo
- VPN Site to site y Site to client
- Autenticación de usuarios via WiFi (VIP, invitados, WiFi)
- Tráfico hacia internet y Firewall
- IPv6 sobre el switch 6500 CORE y Vlan 300

Se validó también la respuesta de los servidores importantes del Datacenter, como fue servicios de DNS, DHCP, Controladores de dominio, y aplicaciones web. Figura 42:

Figura 42 Chequeo de Servicios y Aplicaciones

Fuente: Propia

Por último se presenta la relación de porcentaje de configuración en cada uno de los dispositivos de comunicaciones de la empresa FENIX, los cuales ya tiene configurado y trabajando sus componentes de IPv6 como se puede ver en la tabla 6:

CANTIDAD	MODELO	TIPO	FIRMWARE	%IPv6 Implementado
37	Cisco WS-C2960S-48FPD-L	Switch	C2960S Software (C2960S-UNIVERSALK9-M), Version 12.2(55)SE3, RELEASE SOFTWARE (fc1)	100%
78	AIR-LAP1262N-A-K9	Access Point	7.4.140.0	100%
2	cisco WS-C6509-E (R7000)	Switch	s72033_rp Software (s72033_rp-ADVIPSERVICESK9_WAN-M), Version 12.2(33)SXJ4, RELEASE SOFTWARE (fc2)	100%
2	AIR-CT5508-K9	Controlador Wireless	7.4.140.0	100%
2	Cisco ASA5520	Firewall	Software Version 8.2(5) Device Manager Version 6.4(5)	100%
2	N5K-C5548UP	Switch Datacenter	Cisco NX-OS Software Release 6.0(2)	100%
3	N2K-C2232PP-10GE	Switch Datacenter	Cisco NX-OS Software Release 6.0(2)	100%
4	Cisco NAC 3315	Cisco NAC	ISE 1.2	100%
2	Cisco NAC 3355	Cisco NAC	ISE 1.2	100%
2	Cisco S370 Web Security Appliance	Ironport	8.0.7-142	100%
1	Cisco 1121 Secure Access Control System	Cisco ACS	5.4	100%
1	Switch Cisco 3750 ETB	Switch		Desconectado
1	BlueCoat	PacketShaper	Packet Shaper 12000	100%
2	SONICWALL SRA 4600	VPN	SonicOS SSL-VPN 6.0.0.6-24sv	100%
1	Router Cisco 1800 IFX G-NAP	Router		100%
2	Router Cisco 2900 IFX internet	Router		100%
2	Switch Cisco 3750 IFX	Switch		100%

Tabla 6 Porcentaje de Configuración Dispositivos en IPv6 Comunicaciones

8.4 Fase III Pruebas de Implementación IPv6

8.4.1 Configuraciones del Nuevo Protocolo Realizadas en las Plataformas o Componentes de Hardware y Software

A continuación se presentara una descripción de configuraciones en los distintos equipos que son necesarios para implementar IPv6 en una red empresarial y algunas recomendaciones a tener en cuenta para cada tipo de dispositivo que conforma la infraestructura de red.

8.4.1.1 Routers

Los equipos de encaminado deben tener configurados los prefijos IPv6 que correspondan en la empresa en las interfaces que van a tener IPv6 habilitado. Es conveniente permitir que los prefijos de red sean anunciados en cada LAN o Vlan, para permitir la autoconfiguración de dispositivos en dado caso que se desee.

8.4.1.2 Servidores

Los sistemas operativos que se utilizan para brindar servicios en este tipo de redes generalmente son sistemas Linux, Windows Server o sistemas virtuales. Estos sistemas tienen soporte de IPv6 desde hace muchos años, con versiones muy estables.

No se recomienda hacer autoconfiguración IPv6 en los servidores, sino especificar direcciones estáticas o manualmente.

8.4.1.3 Estaciones de trabajo (PC, Portátiles, otros dispositivos)

Tanto las PC de escritorio como los portátiles deben tener sistemas operativos que soportan IPv6, ya sea Linux o Windows. Este tipo de dispositivos pueden tener activa la autoconfiguración, preferiblemente con un servidor DHCPv6 que permite tener un control mayor sobre la asignación de direcciones y suministrar otra información como por ejemplo cuales son los servidores DNS, también facilitara la actualización automática de los registros en el DNS de la empresa FENIX si se utiliza esta facilidad.

En general, las aplicaciones de uso diario, no tendrán problemas en lo que a la nueva versión del protocolo IP se refiere. Entre esas aplicaciones se pueden citar los clientes de correo, navegadores de internet, sistemas de colaboración, etc.

Dentro de los equipos conectados a la red se pueden encontrar diversos tipos de dispositivos para la adquisición de datos y que proveen una interfaz de red, tales como analizadores, controles de acceso o registro, sensores, cámaras de seguridad o DVR. En esos casos, es muy probable que estén preparados para soportar IPv6. También se pueden encontrar limitaciones en impresoras de red y escáneres, por lo que habrá que contemplar la necesidad de mantener la compatibilidad con IPv4. Por esa razón, la recomendación es que los equipos de usuario mantengan el sistema de Doble Pila o Dual Stack.

8.4.1.4 Equipos de Videoconferencia

Más allá de los sistemas por software es común encontrar equipos especializados para realizar videoconferencias. Estos pueden ser de sala o de escritorio, entre los equipos más conocidos que existen en el mercado se tienen, por ejemplo, Polycom, Tandberg, Aethra, Sony, LifeSize con una gran variedad de modelos dentro de estas marcas.

El nivel de soporte de IPv6 varía en función del modelo y marca que se esté utilizando, vale la pena mencionar que al momento de evaluar la adquisición de un equipo de videoconferencia se debe evaluar el grado de adopción del protocolo IPv6 posee. En algunos casos es posible utilizar solo el protocolo SIP en IPv6, no están soportadas las comunicaciones en H323, También es posible que el equipo tenga una configuración manual limitada y solo permita mecanismo de autoconfiguración.

8.4.1.5 Switch, Cableados e inalámbricos

Desde el punto de vista de IPv6, los dispositivos de capa 2 no deberán representar un inconveniente ya que no necesitan interpretar el tráfico de las capas superiores. En cuanto a los puntos de acceso inalámbricos, solo en casos en que estos equipos actúen como routers, será necesario tener en cuenta el soporte de IPv6 y de las opciones de configuración que permite.

8.4.1.6 Firewall, Filtros WEB, Control Autenticación

Los firewalls son un punto crítico en la infraestructura de red disponible, se debe verificar el soporte de IPv6 y que permita configurar reglas de filtrado en forma similar que con IPv4, es importante tener en cuenta que deben reproducir las mismas reglas en IPv6 que en IPv4, porque de lo contrario se estarían teniendo políticas diferentes para una versión del protocolo que para otra. La utilización de recursos de hardware es alta para estos dispositivos ya que tendrán que desarrollan dos ambientes de trabajo en IPv6 e IPv4.

Para sistemas de filtrado WEB o sistemas autenticación se recomienda verificar sus funcionalidades en protocolo IPv6 y aplica la misma recomendación en políticas de seguridad con reglas y consumo de sus recursos de hardware y software para trabajar en IPv6 e IPv4.

8.4.2 Dispositivos a Intervenir en su Configuración para IPV6

Con el análisis de topología realizado previamente de los equipos de comunicaciones principales de la infraestructura de red de la empresa FENIX, se procedió a activar sus componentes de IPv6 para iniciar pruebas de funcionalidad y compatibilidad para el nuevo protocolo y así activar el servicio a todos los usuarios de la empresa FENIX.

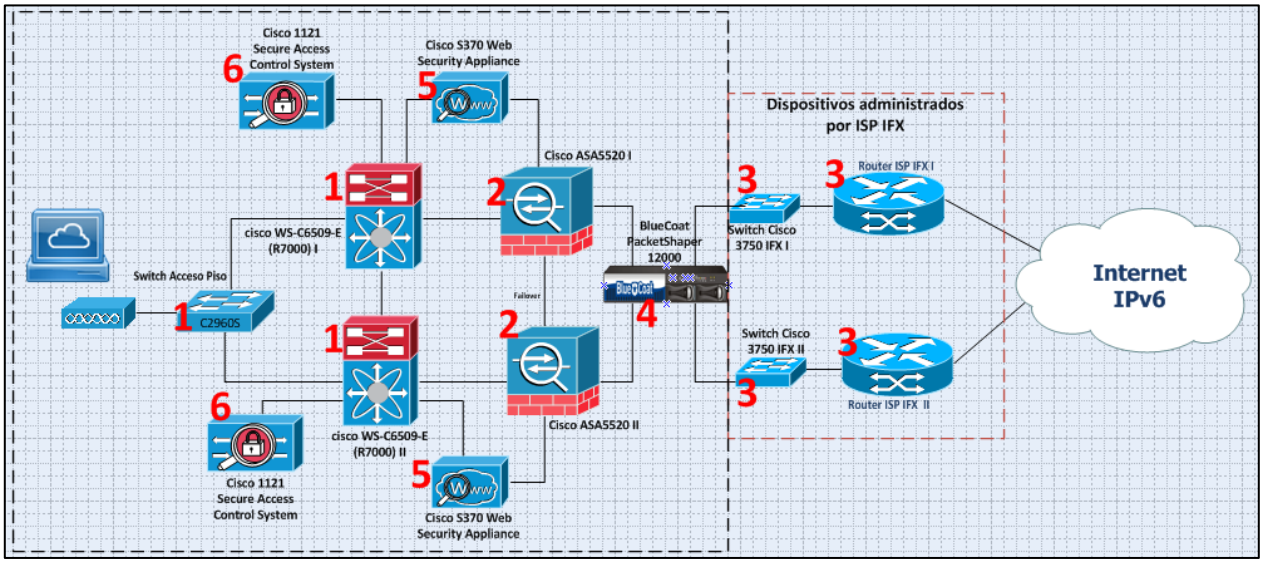


Figura 43 Diagrama de Red Dispositivos Principales para IPv6

Fuente: Propia

Como se puede observar en la figura 43 el diagrama de red de la empresa FENIX y los equipos principales a intervenir para otorgar IPv6 a la empresa FENIX. Como se enumera será el orden de configuración para cada dispositivo, esto ya analizado previamente con el

fin de evitar alguna falla de comunicación o alteración de los servicios prestados por cada dispositivo según su rol en la topología de red e importancia.

8.4.2.1 Switch Core Cisco WS-C6509

Se inició la configuración con el dispositivo marcado con el número 1 Switch Core Cisco WS-C6509 de la figura 43, ya que este dispositivo administra el direccionamiento IPv4 de todas las interfaces Vlan de la empresa FENIX. Básicamente a este dispositivo se le activó su soporte de IPv6 mediante el comando IPv6 enable en cada una de las 64 interfaces Vlans que actualmente tiene en operación y se asignó una IPv6 como fue descrito anteriormente.

A continuación, en la Figura 44 se muestran las líneas de configuración realizadas para el dispositivo Switch Core Cisco WS-C6509 de la empresa FENIX, ingresado los comandos correspondientes de activación IPv6 en la Interface vlan 2 Servidores, Interface Vlan 5 Gateway Capa Aplicación, y por ultimo interface Vlan 22 Inside, la cual está conectada para la salida toda hacia internet de la empresa FENIX:

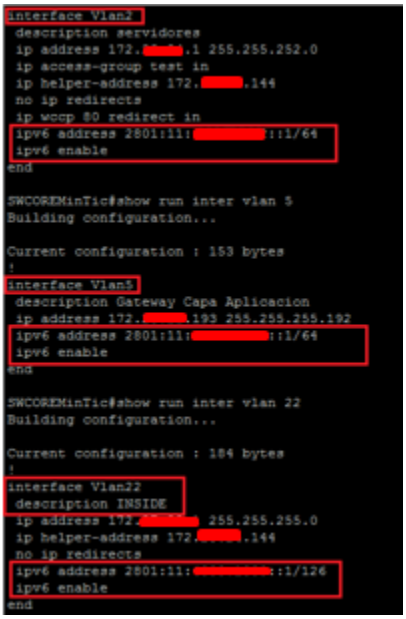


Figura 44 Configuración Switch Core

Fuente: Propia

8.4.2.2 Cisco ASA 5520

Se continuó con el dispositivo marcado con el número 2 Cisco ASA5520 de la Figura 43. Este Firewall utilizado es por la empresa FENIXy es altamente importante su rol en seguridad. Se activaron sus funciones de IPv6 igualmente con el comando IPv6 enable y se asignó una IPv6 según el plan de direccionamiento sobre las interfaces que actualmente tiene en operación como lo es la Interface Outside y la interface Inside.

Para configurar la interface Outside en vlan 3201, se debido interactuar y trabajar conjuntamente con el ISP durante una semana buscando la mejor solución para la activación del protocolo IPv6, analizando la topología actual sin causar intermitencias o fallas de comunicación. Para establecer canal de comunicación en IPv6 se configuró una dirección 2802:0:0:a::34/64 en el extremo del firewall asignada por parte del proveedor ISP, y una IPv6 de puerta e enlace 2802:0:0:a::58/64 con el fin de integrar las comunicaciones con los equipos de enrutamiento del ISP y también como parte de solución debido a que la empresa FENIX no cuenta con equipos Router de Borde con sistema autónomo AS para anunciar su pool IPv6.

Por último, el ISP realizó la publicación del pool IPV6 de la empresa FENIX a nivel mundial y su respectivo enrutamiento interno y externo.

A continuación, se puede ver en la Figura 45 la configuración resultante en modo grafico después de ingresar los comandos correspondientes que se ven en la Figura 46:

Interface	Name	Enabled	Security Level	IP Address	Subnet Mask Prefix Length	VLAN
GigabitEthernet0/0		Yes				native
GigabitEthernet0/0.700		Yes				vlan700
GigabitEthernet0/0.701		Yes				vlan701
GigabitEthernet0/1	inside	Yes	100	172.[redacted].4 2801:11:[redacted]::2	255.255.255.0 126	native
GigabitEthernet0/2	dmz	Yes	30	192.[redacted].1	255.255.255.0	native
GigabitEthernet0/3		Yes				native
GigabitEthernet0/3.3201	outside	Yes	0	190.[redacted].34 2802:0:[redacted]::34	255.255.255.224 64	vlan3201
GigabitEthernet0/3.3202	MPLS_IFX	Yes	10	10.[redacted].1	255.255.255.248	vlan3202
Management0/0		Yes				native
Management0/0.32	ravec	Yes	40	172.[redacted].3	255.255.255.0	vlan32
Management0/0.36	RTIC	Yes	45	10.[redacted].97	255.255.255.248	vlan36
Management0/0.50	invitados	Yes	41	192.[redacted].1	255.255.252.0	vlan50
Management0/0.70	RENATA	No	46	190.[redacted].194	255.255.255.192	vlan70

Figurara 45 Configuración Interfaces Firewall ASA 5520 en IPv6

Fuente: Propia

```
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.[redacted].4 255.255.255.0 standby 172.[redacted].5
 ipv6 address 2801:11:[redacted]::2/126 standby 2801:11:[redacted]::3
 ipv6 enable
!
interface GigabitEthernet0/2
 nameif dmz
 security-level 30
 ip address 192.[redacted].1 255.255.255.0 standby 192.[redacted].2
!
interface GigabitEthernet0/3
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3.3201
 description VLAN 3201  outside
 vlan 3201
 nameif outside
 security-level 0
 ip address 190.[redacted].34 255.255.255.224 standby 190.[redacted].36
 ipv6 address 2802:0:[redacted]::34/64 standby 2802:0:[redacted]::36
 ipv6 enable
!
```

Figura 46 Configuración Firewall ASA 5520

Fuente: Propia

Una parte vital del dispositivo marcado número 2 Cisco ASA5520 ver Figura 43, son sus funciones de seguridad que debe desarrollar para mantener segura la red interna. Ahora con el protocolo IPv6, para continuar activando la red sobre este nuevo servicio y para realizar pruebas en IPv6 posteriormente, se configuraron reglas básicas para tener tráfico permitido con los protocolos IP (TCP Http, https, Icmpv6) y (UDP Domain), para la interface Inside.

El trafico permitido para la interface Outside, por el momento permite únicamente ingreso o respuesta del protocolo icmpv6 con el fin de validar conectividad desde la internet. A continuación se puede observar en la Figura 47 los comandos ingresados en el Cisco ASA5520.

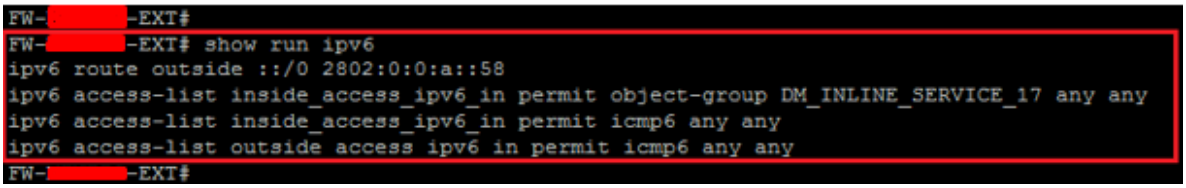


Figura 47 Comando Políticas de Seguridad IPv6

Fuente: Propia

En la Figura 48 se puede observar el resultado de la configuración y activación de IPv6 visualizado en modo grafico de administración del Cisco ASA5520 y se puede ver la columna de Hits que indica la existencia de tráfico circulando por la interface en IPv6, siendo verificado, revisado y asegurado por el dispositivo.

Figura 48 Políticas de Seguridad Modo Grafico IPv6

Fuente: Propia

8.4.2.3 Dispositivos Administrados y Soportados por el ISP

Las configuraciones para los dispositivos marcados con número 3, ver Figura 43, son administrados y soportados por el proveedor ISP, las cuales no es posible mostrar por políticas de seguridad por parte de este proveedor.

Hasta este punto de ejecución de configuración sobre los dispositivos de red de comunicaciones de la empresa FENIX, en las pruebas realizadas se logra tener tráfico en IPv6 y salida a internet, esto sobre una Vlan de pruebas sin ningún tipo de restricción o seguridad, pero la empresa FENIX tiene servicio de seguridad y contención de servicios controlados y tuvieron transición a IPv6, para lograr esto se configuro el dispositivo Cisco Web Security Appliance el cual dentro del diagrama topológico marcado con número 5. Ver Figura 43.

8.4.2.4 Dispositivos WSA y ACS

Para continuar con la activación de los componentes marcados como 5.WSA y 6.ACS, se requirio una actualización de versión VSS v3.0 sobre los switch Cisco 6500 CORE de la

empresa FENIX, el cual se ejecutó el día miércoles 9 de diciembre. Al ser aprobado y ejecutado se pudo continuar con la activación de componentes IPv6 para los equipos restantes.

8.4.2.5 Dispositivo PacketShaper

Otro de los dispositivos al cual se le configuró el protocolo IPv6 fue el BlueCoat PacketShaper marcado con numero 4(Cuatro) ver Figura 43, el cual permite aplicar políticas de calidad de servicio o balanceo sobre los canales de internet para las Vlan de la empresa FENIX.

En primera instancia se crea la regla general de tráfico sobre IPv6, para identificar usuarios y servicios los cuales ya están utilizando este nuevo protocolo de conexión versión 6, como se puede observar en la Figura 49 ” Política General IPv6”:

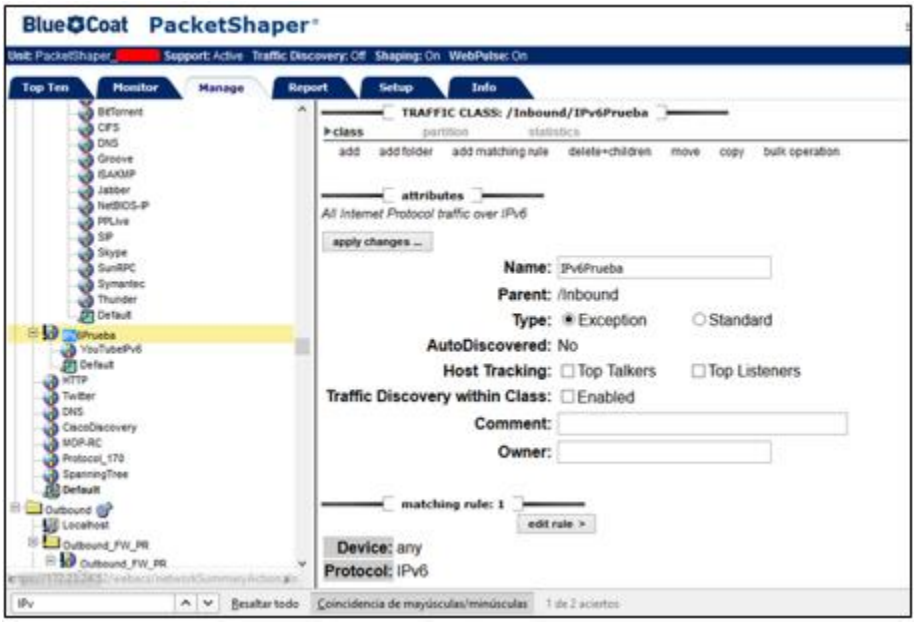


Figura 49 Creación de Política General de IPv6

Fuente: Propia

Ya identificado cierto tipo de trafico circulando y para verificar que este sobre IPv6, se creó una regla para filtrar tráfico de youtube.com en IPv6 o tipo de tráfico que contenga videos, con ello se creó la regla “YouTubeIPv6” como se observa en la Figura 50.

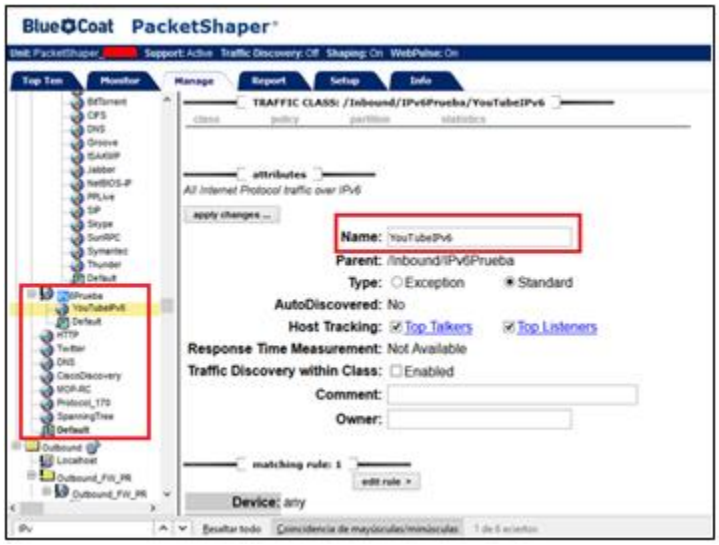


Figura 50 Regla “YouTube IPV6”

Fuente: Propia

Por ultimo verificando el tráfico identificado podemos obtener grafica de consumo de ancho de banda para el protocolo o servicio audio/Videoclips de la regla “YouTubeIPv6” como podemos ver en la Figura 51.

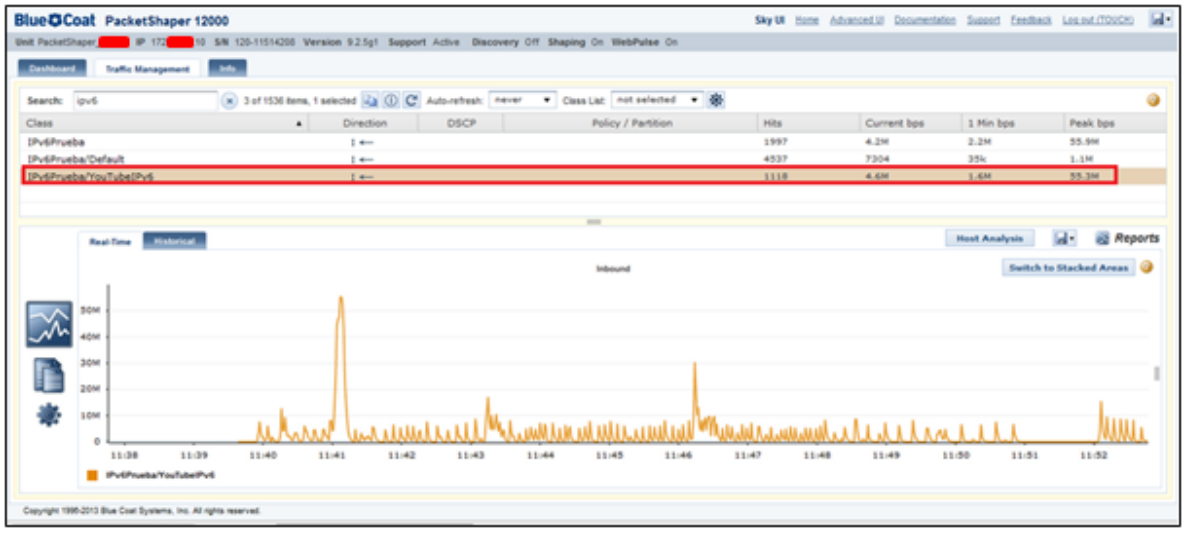


Figura 51 Grafica para Regla YouTubeIPv6

Fuente: Propia

Continuando se realizaron las configuraciones necesarias sobre los dispositivos Cisco Web Security Appliance, para lograr tener servicios de seguridad en páginas web (5) ver Figura 43, básicamente se agregaron listas de acceso en IPv6 para filtrar el tráfico y ser analizado, también se especifica a donde dirigir el tráfico por medio del sistema Web Cache Control Protocol:

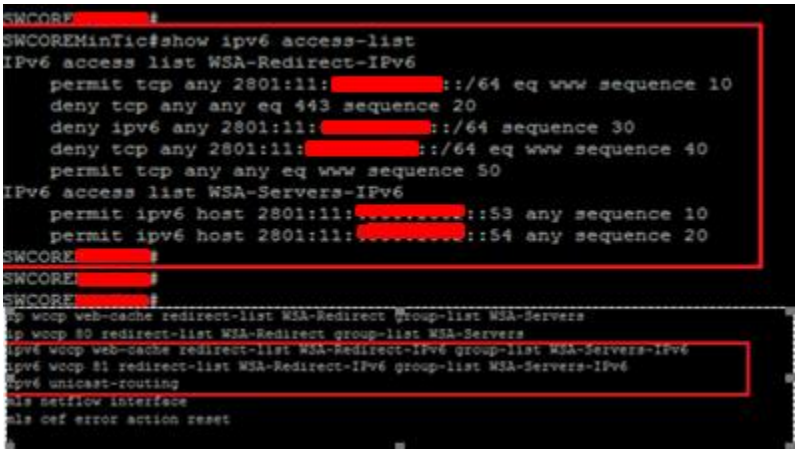


Figura 52 Configuración WCCP IPv6 y WSA

Fuente: Propia

Para lograr esto fue necesario realizar una actualización de Sistema Operativo del Switch 6500 CORE, la cual se realizó de forma controlada exitosamente. Se realizó la actividad de actualización de los switch de Core Cisco 6500 de la versión 12.2(33) a la versión 15.1(2) satisfactoriamente como se puede observaren la Figura 53.

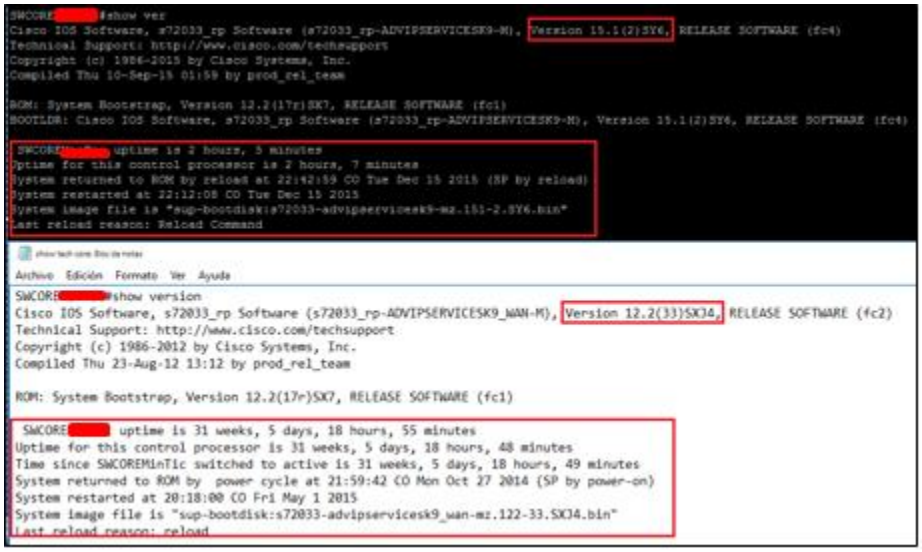


Figura 53 Actualización de IOS Switch 6500 Core

Fuente: Propia

Al finalizar la actividad se ejecutó la siguiente lista de chequeo:

- Validación de comunicación y servicios de red desde los switch de acceso de cada piso de la empresa FENIX
- Autenticación de usuarios al directorio activo
- Validación de servicio del ACS contra el directorio activo
- VPN Site to site y Site to client
- Autenticación de usuarios via WiFi (VIP, invitados, WiFi)
- Tráfico hacia internet y Firewall
- IPv6 sobre el switch 6500 CORE y vlan 300

Se validó también la respuesta de los servidores importantes del DataCenter, como fue servicios de DNS, DHCP, Controladores de dominio, y aplicaciones web:

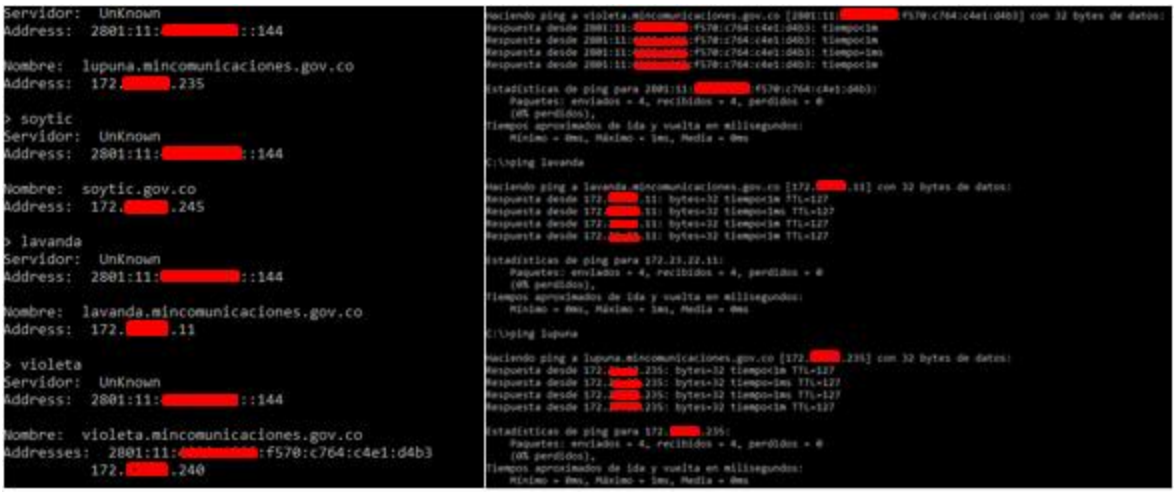


Figura 54 Chequeo de Servicios y Aplicaciones

Fuente: Propia

9 RESULTADOS

Los resultados y el avance del proyecto de dio de acuerdo al cronograma que se implementó para cada una de las fases y de esta forma poder evidenciar el avance del proyecto en las diferentes etapas y cumpliendo con los requerimientos del cliente final.

9.1 Fase I de Diagnóstico

Comprende las Siguientes Actividades

Nombre de tarea	Duración	Comienzo	Fin	% completado
FASE I Diagnóstico de la solución	**18 días**	**mié 07/10/15**	**vie 30/10/15**	**0%**
Construcción del Plan de Diagnóstico	11 días	mié 07/10/15	mié 21/10/15	0%
Inventario de TI	11 días	mié 07/10/15	mié 21/10/15	0%
Análisis infraestructura actual y funcionamiento	18 días	mié 07/10/15	vie 30/10/15	0%
Protocolo de pruebas	18 días	mié 07/10/15	vie 30/10/15	0%
Validación de las aplicaciones actuales	18 días	mié 07/10/15	vie 30/10/15	0%
Planeación de migración	18 días	mié 07/10/15	vie 30/10/15	0%
Identificación de esquemas de seguridad	18 días	mié 07/10/15	vie 30/10/15	0%
Elaboración de informe de implementación IPv6	18 días	mié 07/10/15	vie 30/10/15	0%
Revisión del informe y entrega	18 días	mié 07/10/15	vie 30/10/15	0%

9.2 Fase II de Desarrollo del Plan de Implementación

Comprende las Siguientes Actividades

Nombre de tarea	Duración	Comienzo	Fin	% completado
FASE II Desarrollo del plan de implementación	**20 días**	**lun 02/11/15**	**vie 27/11/15**	**0%**
Habilitación IPv6 componentes HW y SW	20 días	lun 02/11/15	vie 27/11/15	0%
Configuración de servicios de DNS, DHCP, Seguridad, VPN y otros	20 días	lun 02/11/15	vie 27/11/15	0%
Configuración IPv6 en Aplicativos y Red	20 días	lun 02/11/15	vie 27/11/15	0%
Activación políticas seguridad IPv6 en HW seguridad y red	20 días	lun 02/11/15	vie 27/11/15	0%
Generación tráfico con ISP sobre IPv6	20 días	lun 02/11/15	vie 27/11/15	0%

9.3 Fase III de Pruebas de Funcionabilidad

Comprende las Siguientes Actividades

Nombre de tarea	Duración	Comienzo	Fin	% completado
FASE III Pruebas de funcionalidad IPv6	**20 días**	**jue 03/12/15**	**mié 30/12/15**	**0%**
Pruebas y monitoreo de la funcionalidad de IPv6	20 días	jue 03/12/15	mié 30/12/15	0%
Análisis de información y pruebas de funcionalidad- seguridad perimetral	20 días	jue 03/12/15	mié 30/12/15	0%

Afinamiento parte 1	20 días	jue 03/12/15	mié 30/12/15	0%
Afinamiento parte 2	20 días	jue 03/12/15	mié 30/12/15	0%
Facturación 3	0 días	mié 30/12/15	mié 30/12/15	0%

Para la verificación de cada uno de los avances se programó reuniones en donde se presentaron los avances del proyecto, de tal manera que se evidenciara el progreso de la implementación y el cumplimiento del cronograma de trabajo planteado cumplir con las metas corporativas para este proyecto.

Para la fase I se realzaron las siguientes entregas:

9.4 Informe de Avance 1

Reunión 21-10-2015

Nombre de tarea	% Complete
FASE I Diagnóstico de la solución	**71%**
Construcción del Plan de Diagnóstico	100%
Inventario de TI	100%
Análisis infraestructura actual y funcionamiento	100%
Protocolo de pruebas	100%
Validación de las aplicaciones actuales	100%
Planeación de migración	100%
Identificación de esquemas de seguridad	50%
Elaboración de informe de implementación IPv6	20%

Revisión del informe y entrega	0%

Según las actividades propuestas se pondero un Porcentaje Completado de la Fase 1 del 71 % y un porcentaje pendiente de 29 %, Fases 2 y Fase 3 no había avance en el porcentaje de actividades.

	% Completado	% Pendiente
FASE 1	71%	29%
FASE 2	0%	100%
FASE 3	0%	100%

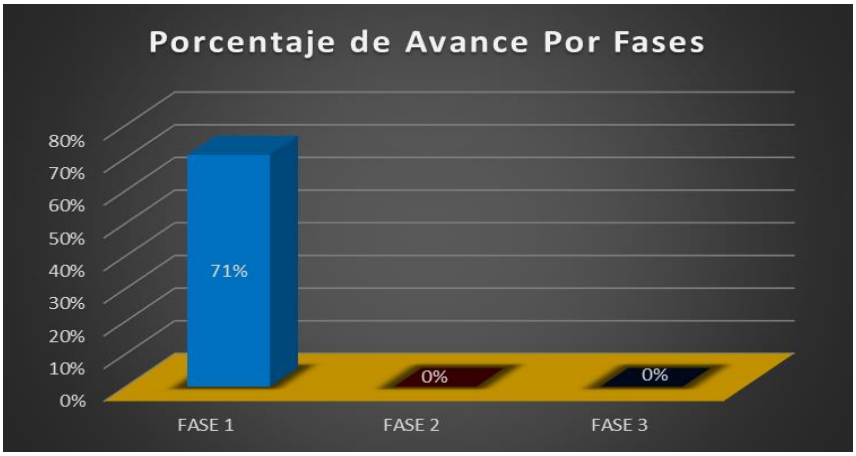


Figura 55 Porcentaje de Avance de la Fase I 21-10-2015

La figura 56 muestra el Informe del trabajo completado del total del proyecto a corte a 21 de octubre de 2015.

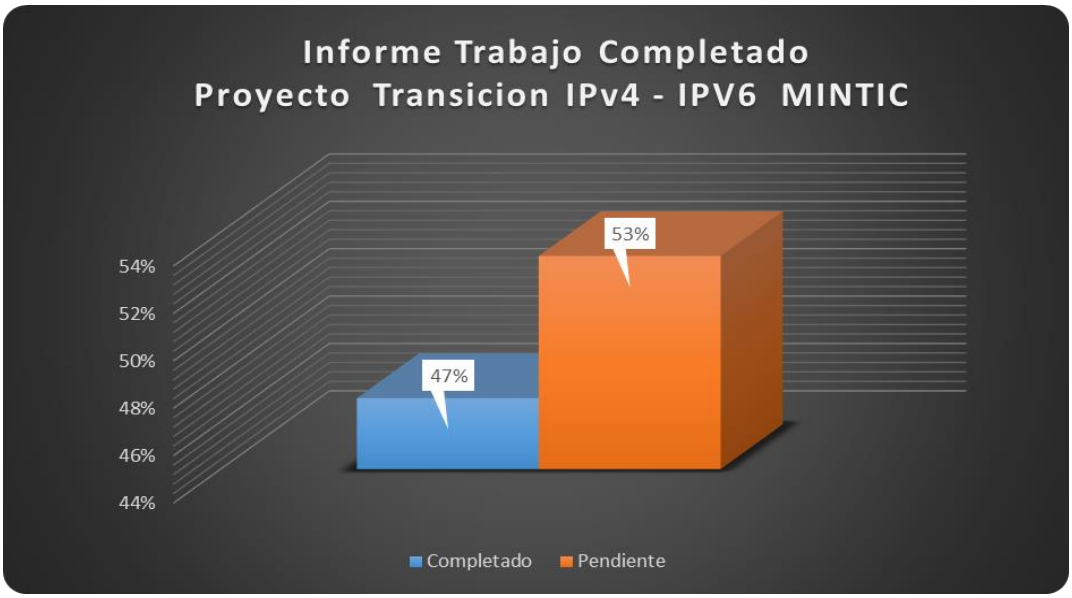


Figura 56 Avance Proyecto 21-10-2015

9.5 Informe de Avance 2

Reunión 28-10-2015

Para 28 de octubre de 2015, se completó la totalidad de las actividades pendientes en el cronograma de trabajo para la fase I, llegando a un 100% de todas las actividades planeadas para esta fase y de esta manera poder dar inicio a las actividades de la fase II según el cronograma plateado para este proyecto.

	% Completado	% Pendiente
FASE 1	100%	0%
FASE 2	0%	100%
FASE 3	0%	100%

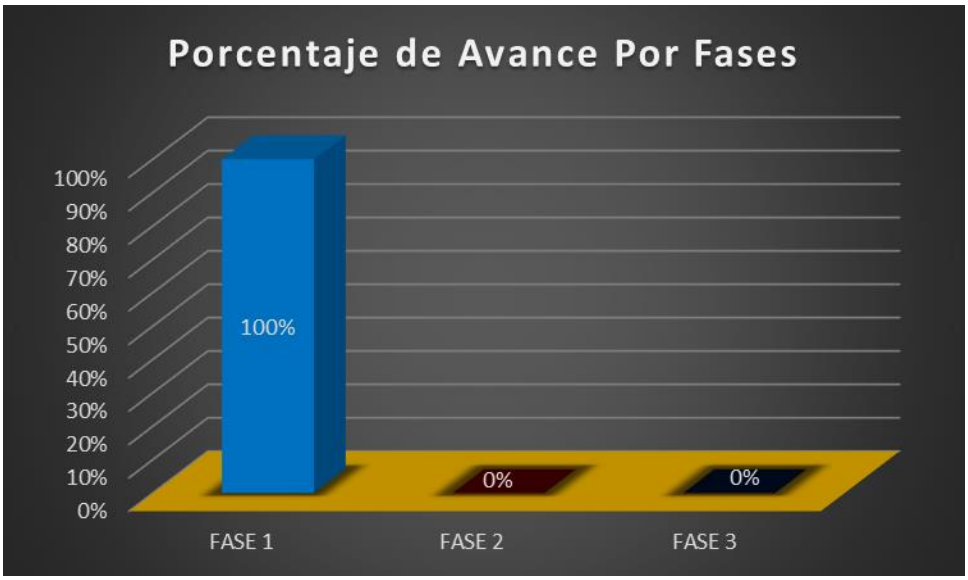


Figura 57 Avance Fase 1 Reunión 28-10-2015

La figura 58 muestra el Informe del trabajo Total del Proyecto a corte a 28 de octubre de 2015 que corresponde a un 53 % del total del Proyecto y con pendientes de un 47 %.

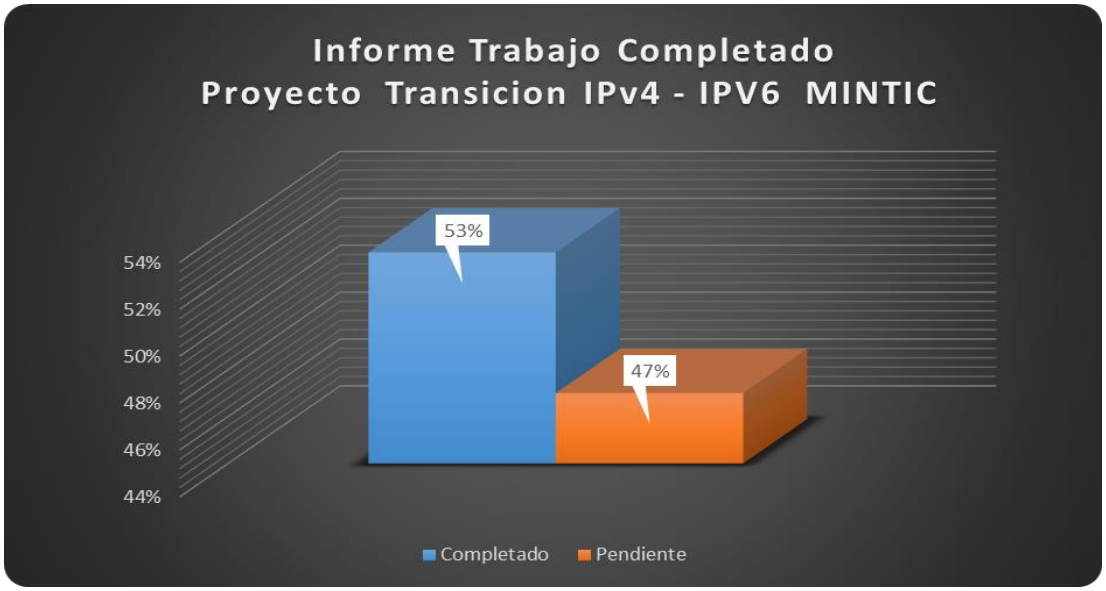


Figura 58 Avance Proyecto 28-10-2015

9.6 Informe de Avance 3

Reunión 11-11-2015

Nombre de tarea	% Complete
FASE II Desarrollo del plan de implementación	**48%**
Habilitación IPv6 componentes HW y SW	95%
Configuración de servicios de DNS, DHCP, Seguridad, VPN y otros	90%
Configuración IPv6 en Aplicativos y Red	0%
Activación políticas seguridad IPv6 en HW seguridad y red	0%
Reunión proveedores	0%
Generación tráfico con ISP sobre IPv6	30%

El Porcentaje Completado en fases, Fase I completado al 100 % y un 48% de avance de la Fase 2.

	% Completado	**% Pendiente**
FASE 1	100%	0%
FASE 2	48%	52%
FASE 3	0%	0%

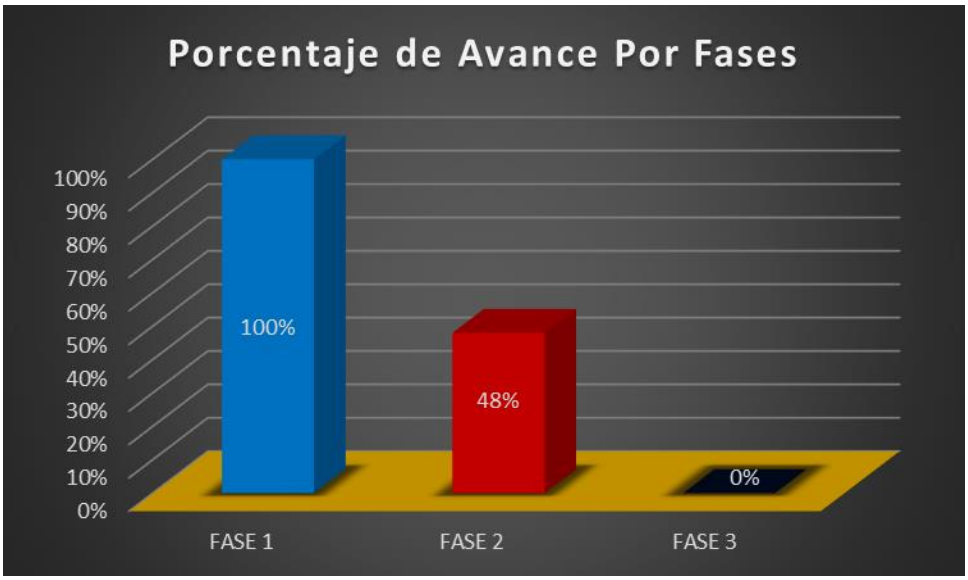


Figura 59 Avance Fase 2 Reunion 11-11-2015

La figura 60 muestra el Informe del trabajo completado Total del Proyecto a corte a 11 de noviembre de 2015 que corresponde a un 69 % del total del Proyecto y con pendientes de un 31 % correspondientes a las actividades relacionadas por terminar en la Fase II y III respectivamente.

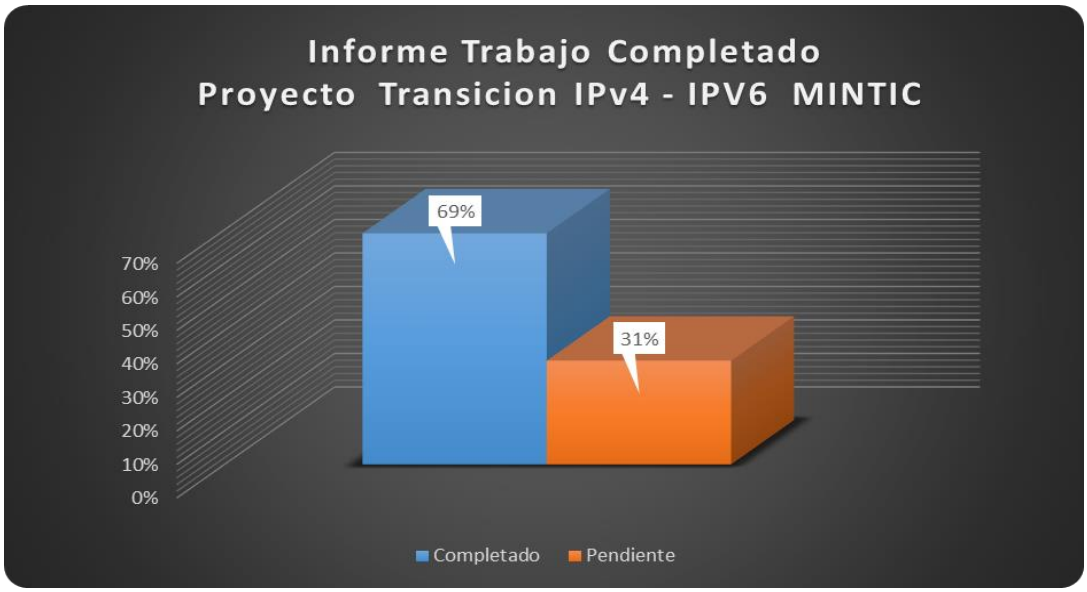


Figura 60 Avance del Proyecto 11-11-2015

9.7 Informe de Avance 4

Reunión 02-12-2015

Nombre de tarea	% Complete
FASE II Desarrollo del plan de implementación	**100%**
Habilitación IPv6 componentes HW y SW	100%
Configuración de servicios de DNS, DHCP, Seguridad, VPN y otros	100%
Configuración IPv6 en Aplicativos y Red	100%
Activación políticas seguridad IPv6 en HW seguridad y red	100%
Reunión proveedores	100%
Generación tráfico con ISP sobre IPv6	100%

Porcentaje Completado en fases, Fase I completado al 100 % y con un avance del 100 % de la Fase 2 y pendiente por ejecutarse la Fase 3 de proyecto.

	% Completado	**% Pendiente**
FASE 1	100%	0%
FASE 2	100%	0%
FASE 3	0%	0%

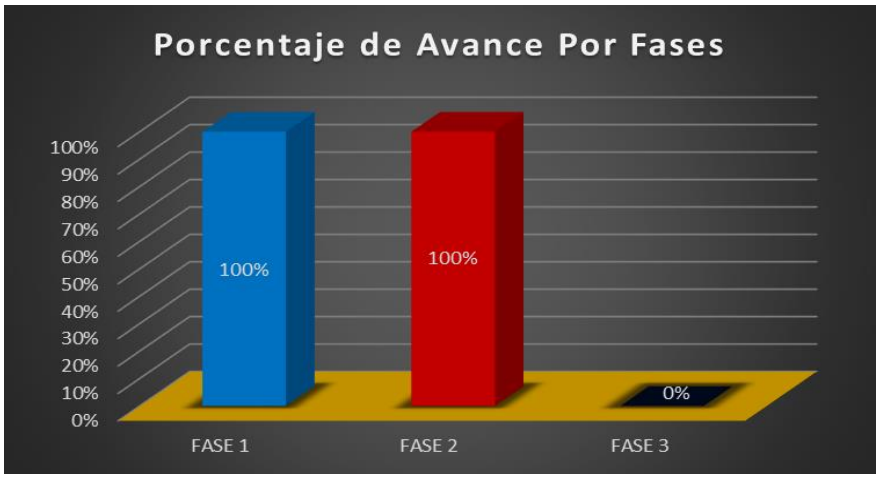


Figura 61 Avance Fase 2 Reunión 02-12-2015

La figura 62 muestra el Informe de trabajo completado para un Total del Proyecto a corte a 02 de diciembre de 2015 que corresponde a un avance del 76 % del total y pendiente por ejecutar un 24% correspondientes a las actividades relacionadas en la Fase III.

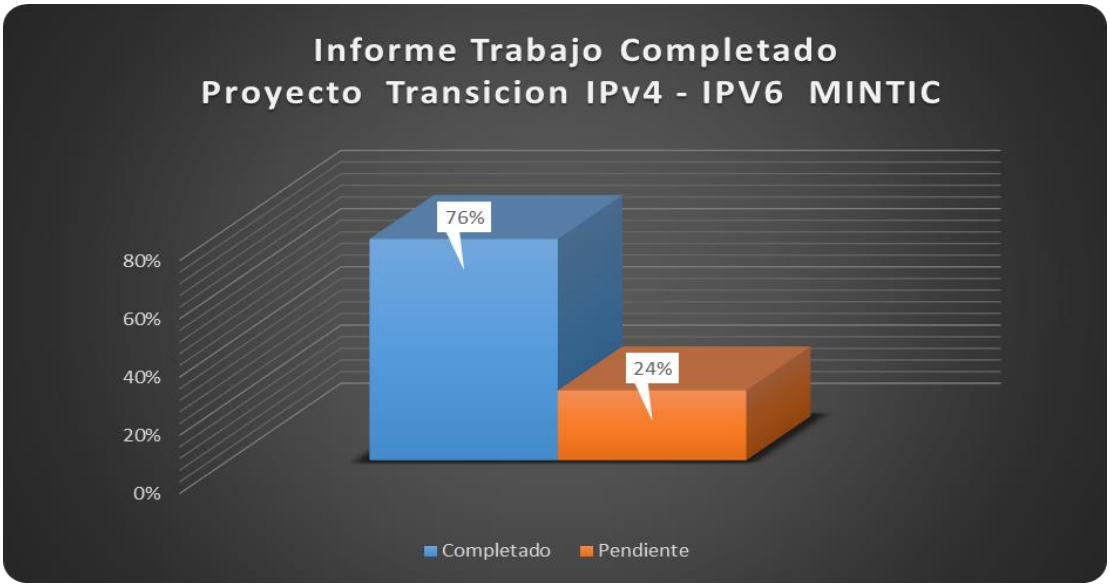


Figura 62 Avance del Proyecto 02-12-2015

9.8 Informe de Avance 5

Reunión 09-12-2015

Nombre de tarea	% Complete
FASE III Pruebas de funcionalidad IPv6	**33%**
Pruebas y monitoreo de la funcionalidad de IPv6	65%
Análisis de información y pruebas de funcionalidad- seguridad perimetral	65%
Afinamiento parte 1	0%
Afinamiento parte 2	0%

El Porcentaje Completado en fases, Fase I y Fase II completadas al 100 % y con un avance del 33 % de la Fase 3 y a esta fecha solo se encontraba pendiente por ejecutar 67 % de la fase.

	% Completado	**% Pendiente**
FASE 1	100%	0%
FASE 2	100%	0%
FASE 3	33%	67%

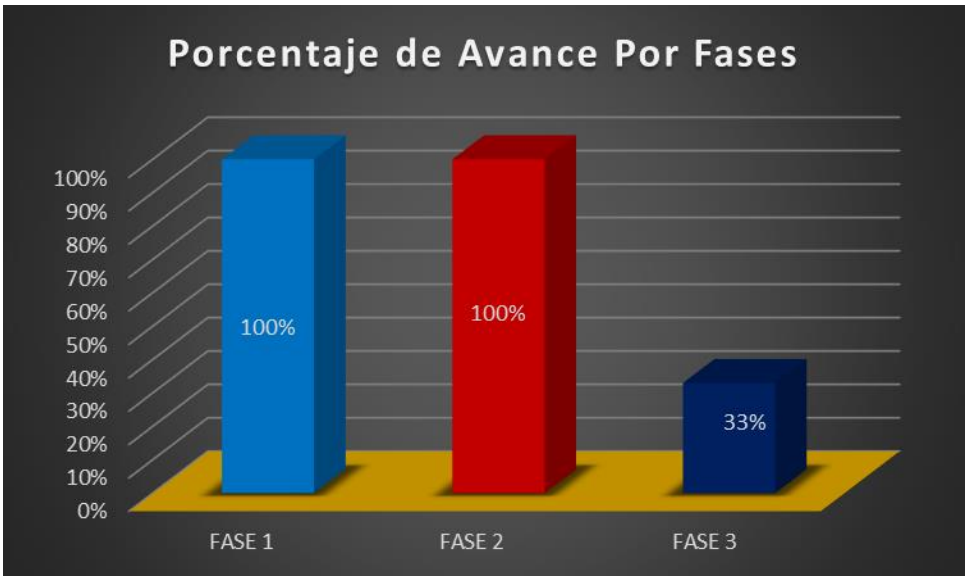


Figura 63 Avance Fase 3 Reunión 09-12-2015

La figura 64 muestra el Informe del trabajo completado Total del Proyecto a corte a 09 de diciembre de 2015 que corresponde a un avance del 83 % del total del Proyecto y con pendiente por ejecutar un 17 % correspondientes a las actividades relacionadas por terminar en la Fase III.

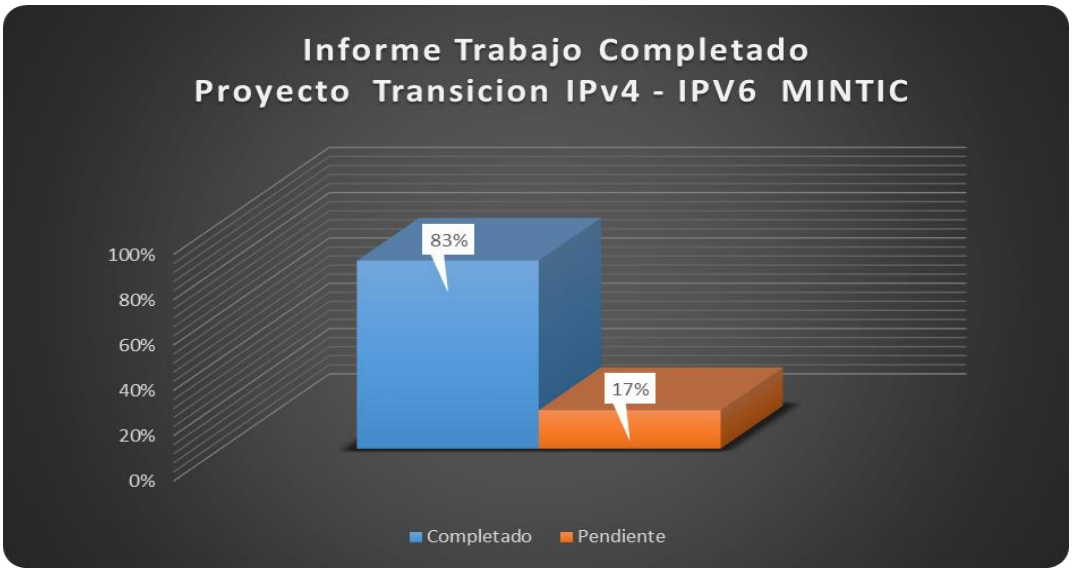


Figura 64 Avance del Proyecto 09-12-2015

9.9 Informe de Avance 6

Reunión 23-12-2015

Nombre de tarea	% Complete
FASE III Pruebas de funcionalidad IPv6	**80%**
Pruebas y monitoreo de la funcionalidad de IPv6	80%
Análisis de información y pruebas de funcionalidad- seguridad perimetral	80%
Afinamiento parte 1	80%
Afinamiento parte 2	80%

El Porcentaje Completado en fases, Fase I y Fase II completadas al 100 % y con un avance del 80 % correspondiente a la Fase 3 y a esta fecha solo estaba pendiente de la Fase II el 20 %.

	% Completado	**% Pendiente**
FASE 1	100%	0%
FASE 2	100%	0%
FASE 3	80%	20%

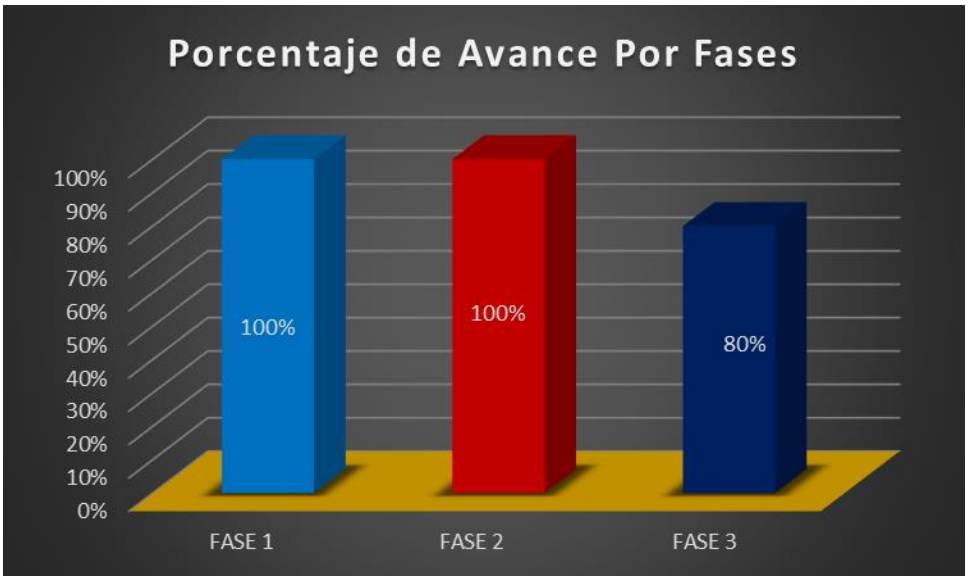


Figura 65 Avance Fase 3 Reunión 23-12-2015

La figura 66 muestra el Informe del trabajo completado Total del Proyecto a corte a 23 de diciembre de 2015 que correspondía a un avance del 95 % del total del Proyecto y con pendiente por ejecutar un 15 % de las actividades relacionadas por terminar en la Fase III.

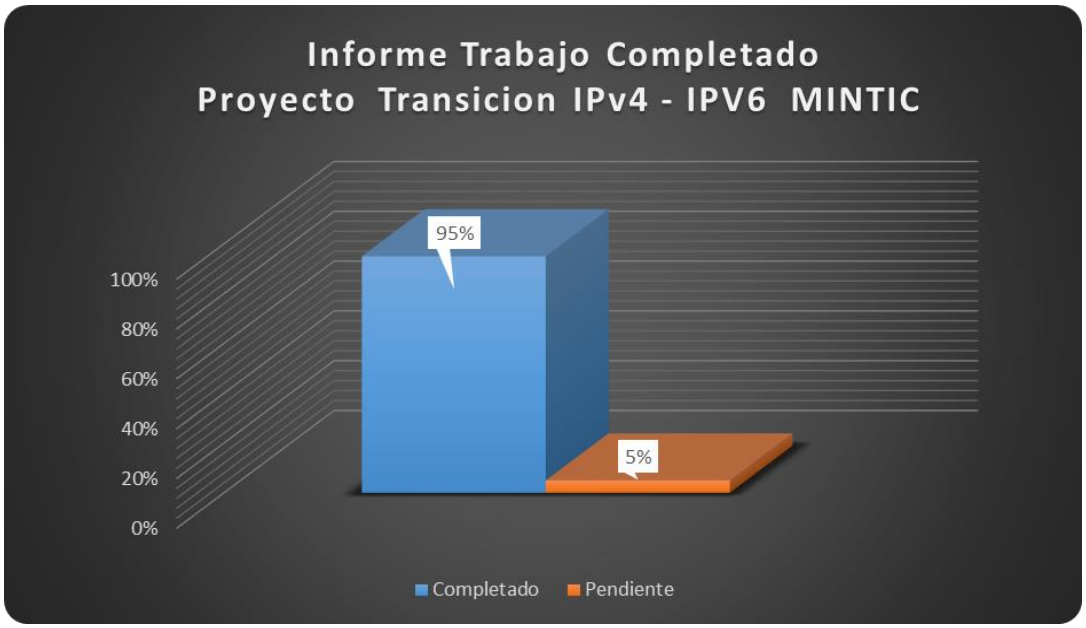


Figura 66 Avance del Proyecto 23-12-2015

9.10 Informe de Avance 7

Reunión 31-12-2015

Nombre de tarea	% Complete
FASE III Pruebas de funcionalidad IPv6	**100%**
Pruebas y monitoreo de la funcionalidad de IPv6	100%
Análisis de información y pruebas de funcionalidad- seguridad perimetral	100%
Afinamiento parte 1	100%
Afinamiento parte 2	100%

Finalmente se completa la totalidad del proyecto de las fases I, II, III, cumpliendo con el cronograma de trabajo estipulado para el cliente final y garantizando la compatibilidad del sistema de doble pila en IPv6.

	% Completado	**% Pendiente**
FASE 1	100%	0%
FASE 2	100%	0%
FASE 3	100%	0%

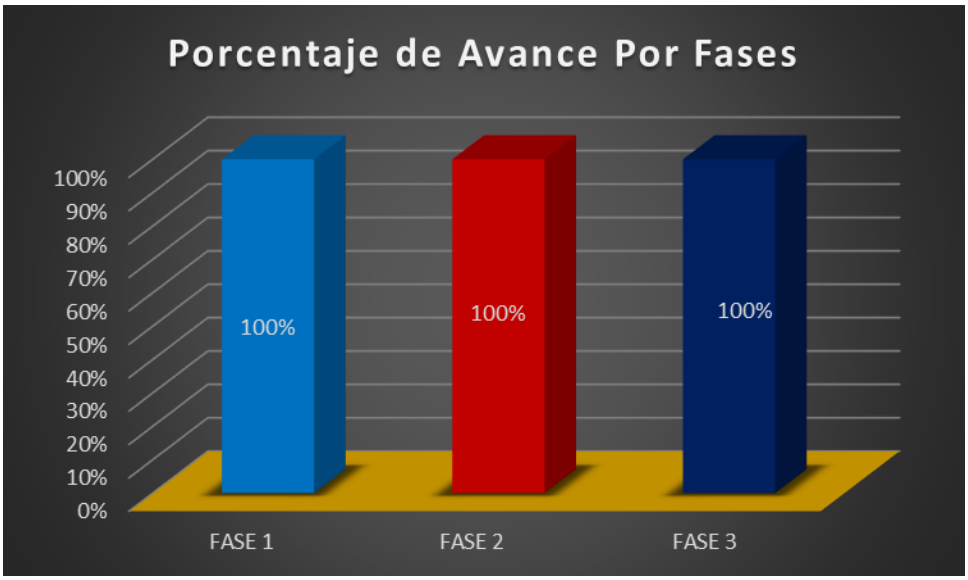


Figura 67 Avance Por Fases 31-12-2015

Finalmente la gráfica anterior representa el estado de las fases a 31 de diciembre, cumpliendo con el cronograma de trabajo estipulado para cada una de las fases y obteniendo como resultado final la implementación del protocolo IPv6 en la entidad. Garantizando la compatibilidad mediante el método de Dual Stack, el cual fue el escogido para esta implementación y de esta manera el cliente cumple con las recomendaciones dadas por la circular 002 del Ministerio de las Telecomunicaciones.

Una vez completado el 100 % es recibido por el cliente a satisfacción y se obtiene como resultado la aplicación del método de Dual Stack y la implementación de la totalidad de los equipos compatibles con el protocolo IPv6 y cumpliendo con las metas y el presupuesto estimado para el proyecto.

10 PRESUPUESTO

Para la elaboración de este proyecto se tuvieron encuentra factores de dedicación de mano de obra especializada, la cual estaba comprendida por un equipo de trabajo con una dedicación de tiempo completo y un salario fijo mensual durante la ejecución de las diferentes fases del proyecto.

No se tienen encuentra suministro de equipos y materias puesto que son los existentes en la entidad al momento de realizar la migración y solo se realizó una prestación de servicios profesionales a esta entidad.

10.1 EQUIPO DE TRABAJO

- Gerente De Proyecto (1):
  - Administrar la estructura organizacional del proyecto.
  - Establecer objetivos y pautas de desarrollo del proyecto.
  - Manejar las técnicas operativas para el análisis y toma de decisiones necesarias en el cumplimiento de los objetivos del proyecto.
  - Asignar los diferentes tipos de recursos para el desarrollo del proyecto.
  - Manejar el riesgo del proyecto.

- Líder Técnico (1):
  - Planificar y gestionar el proyecto, la distribución de tareas y seguimiento de los resultados de todos los involucrados
  - Estar atento y experto en el tratamiento de datos e información para la toma de decisiones.
  - Seguimiento de los indicadores de rendimiento y controlar al equipo de trabajo.
  - Resolver incidentes y tomar maniobras de solución ante las dificultades presentes en el desarrollo del proyecto.

- Especialista De Seguridad (1):
  - Configuración de firewall de la entidad para la migración a IPv6
  - Creación de políticas de seguridad para IPv6
  - Pruebas de funcionamiento de las policías de seguridad.
  - Elaboración de la documentación de las actividades de migración correspondientes a seguridad.

- Especialista De Datacenter (1):
  - Migración de servidores a IPv6
  - Migración de la plataforma de virtualización
  - Realización de ventanas de mantenimientos necesarias para la migración
  - Dar soporte en sitio a los servidores.
  - Elaboración de la documentación de las actividades de migración correspondientes a Datacenter.

- Especialista De Routing And Switching (1)
  - Migración de a IPv6 de la capa e switching.
  - Realización de ventanas de mantenimientos necesarias para la migración
  - Activación del protocolo IPv6 sobre la capa 3 de todas la Vlan.
  - Elaboración de la documentación de las actividades de migración correspondientes a routing and switching.

- Tiempo de ejecución del proyecto 3 meses.

CARGO	CANTIDAD	SALARIO BASICO	COSTO TOTAL EMPLEADO X MES	TIEMPO EN MESES	COSTO TOTAL
· Gerente De Proyecto	1	$ 5.500.000	$ 8.077.043	3	$ 24.231.129
· Líder Técnico	1	$ 4.500.000	$ 6.608.490	3	$ 19.825.470
· Especialista De Seguridad	1	$ 4.000.000	$ 5.874.213	3	$ 17.622.639
· Especialista De Datacenter	1	$ 4.000.000	$ 5.874.213	3	$ 17.622.639
· Especialista De Routing And Switching	1	$ 3.000.000	$ 4.405.660	3	$ 13.216.980
TOTAL PARCIAL					**$ 92.518.857**
Gastos Administrativos				3	**$ 15.000.000**
TOTAL					$ 107.518.857

Tabla 7 Presupuesto Total del Proyecto

El costo total por empleado contempla pago de parafiscales y todas las prestaciones sociales que por ley le da derecho. (Costo total para el empleador).

11 CONCLUSIONES

- Se cumplió a satisfacción con la migración de toda la infraestructura, utilizando el método de DUAL STACK, el cual permito la convivencia de los protocolo IPv4 e IPv6 para que la transición se de manera adecuada hacia una red totalmente IPv6.
- Se demuestra que gran cantidad de los equipos que existen actualmente en la empresa Fenix con compatibles con IPv6, lo cual permite señalar que para realizar una migración de este tipo, solo es necesario realizar pequeñas configuraciones y algunas actualizaciones a nivel de hardware y software.
- Se logra ser pionero en la implementación de este tipo de migraciones en el país lo cual permitirá ser una guía y un ejemplo para que otras compañías realicen este tipo de migraciones y se preparen para actualizar sus redes desde ahora a IPv6.
- Con esta implementación se cumple con las recomendaciones expuestas con la circular 002 de 2011 del ministerio de las telecomunicaciones
- Con esta implementación la entidad Fénix se encuentra preparada para el momento de apagón de IPv4.

12 GLOSARIO

Ámbito (Scope): Para las direcciones IPV6, el ámbito es la porción de la red a la que se supone que se va propagar el tráfico.

BIT: Acrónimo de Binary digit. (Dígito binario). Un bit es un dígito del sistema de Numeración binaria. Mientras que en nuestro sistema de numeración decimal se usan diez dígitos, en el binario se usan solo dos dígitos, el 0 y el 1. Un bit o dígito binario puede representar uno de esos dos valores, 0 ó 1.

Datagrama: Conjunto estructurado de bytes que forma la unidad básica de comunicación del protocolo.

Dirección: Identificador asignado a nivel de la capa de red a un interfaz o conjunto de interfaces que puede ser empleado como campo de origen o destino en datagramas IPV6.

Dirección MAC: Es un identificador de 48 bits (3 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. Está determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits) utilizando el Organizationally Unique Identifier.

Dominio: Un dominio es la parte de una URL (dirección de una página o recurso en internet) por la que se identifica al servidor en el que se aloja.

Dual Stack: método de transición de IPv4 a IPv6 el cual indica que un equipo puede tener ambos direccionamientos.

Estado del enlace: Tecnología de protocolo de ruteo, que intercambia información de rutas, que consta de los prefijos de las redes conectadas a un router y su costo asociado. La información del estado del enlace se anuncia en el arranque, así como cuando se detectan cambios en la topología de red.

Firewall: maquina encargada del tráfico de internet (tanto de entrada como de salida) basado en reglas de comportamiento, se sitúa entre una internet y una intranet

Flujo: Una serie de datagramas intercambiados entre una fuente y un destino que requieren un tratamiento especial en los routers intermedios, y definidos por una dirección IP origen y destino específico, así como por una etiqueta de flujo con un valor distinto a 0.

Fragmentación: Proceso por el que se divide la carga de un datagrama IPV6 en fragmentos por la máquina emisora, de modo que todos los fragmentos tienen una MTU apropiada al camino a seguir hasta el destino.

Gateway: Equipo encargado de proporcionar los servicios a un host.

Interfaz: Una representación de un nexo físico o lógico de un nodo a un enlace.

IPv6: abreviatura escogida en IETF con la que se denomina la versión 6 del protocolo IP

Un ejemplo de un interfaz físico es una interfaz de red. Un ejemplo de un interfaz lógico es un interfaz de un túnel.

MTU: Unidad máxima de trasferencia (Maximum Trasfer Unit - MTU), expresa el tamaño en bytes del datagrama más grande que puede pasar por una capa de un protocolo de comunicaciones.

NODO: Espacio real en el que confluyen parte de las conexiones de otros espacios reales o abstractos que comparten sus mismas características y que a su vez también son nodos. Todos estos nodos se interrelacionan entre sí de una manera no jerárquica y conforman lo que en términos sociológicos o matemáticos le llamamos red.

OFFSET: Porción de datos enviados en el paquete con relación al paquete original

Paquete: Unidad fundamental de trasporte de información en todas las redes de cómputo. Un paquete está generalmente compuesto de tres elementos: Una cabecera (header) que contiene generalmente la información necesaria para trasladar el paquete desde el emisor hasta el receptor, el área de datos (payload) que contiene los datos que se desean trasladar, y la cola (trailer), que comúnmente incluye código de detección de errores.

RFC (Request For Comments): Documento de especificaciones que se expone públicamente para su discusión.

Socket: Tupla compuesta por una dirección IP y un número de puerto.

Tabla de ruteo: Conjunto de rutas empleadas para determinar la dirección e interfaz del siguiente nodo en el tráfico IPV6 enviado por un equipo o reencaminado por un router.

Tunneling: Encapsulado de un protocolo IPV6 dentro de un protocolo IPV4 o viceversa.

Router: Es un dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras." (Eduardo Jacob Taquet, 2004).

WAN: red de gran alcance suele utilizarse para la unión de redes LAN. (sanchez Gerardo L ahuatzin, 2016)

13 REFERENCIAS BIBLIOGRAFICAS

Castillo, G. G. (2005). Sistemas de comunicaciones-Redes II. En U. T. Mixteca, *Sistemas de comunicaciones-Redes II* (págs. 1-12). Oaxaca.

Cruz, E. A. (2014). *COMPARACIÓN DEL PROTOCOLO IPSEC SOBRE IPV4 E IPV6 EN UNA RED CON CARACTERÍSTICAS IGUALES.* Bogotá.

Deering R Hinden S. (1998). *Internet Protocol, Version 6 (IPv6) Specification.*

IPv6MX. (s.f.). *IPv6MX*. Obtenido de http://www.ipv6.mx/index.php/informacion/noticias/1-latest-news/333-adopcion-del-protocolo-ipv6-en-colombia

LACNIC. (10 de 12 de 2015). *portalipv6.lacnic.net.* Obtenido de http://portalipv6.lacnic.net/wp-content/caf-lacnic/CAF-LACNIC-Despliegue-IPv6-para-desarrollo-socio-economico-en-LAC.pdf

LACNIC. (23 de Abril de 2016). *LACNIC*. Obtenido de http://www.lacnic.net/es/web/lacnic/agotamiento-ipv4

LACNIC. (s.f.). *Ipv6 portal*. Obtenido de http://portalipv6.lacnic.net/mecanismos-de-transicion/

MINISTERIO DE LAS TELECOMUNICACIONES. (01 de 07 de 2016). *colombiatic.mintic.gov.co.* Obtenido de http://colombiatic.mintic.gov.co/602/articles-15639_archivo_pdf.pdf

Montes Erick Fernando Lujan. (2005). *Seguridad en Ip con el protocolo de seguridad IPsec para IPv6.* Trabajo de graduacion, Universidad San Carlos de Guatemala, Guatemala.

UNIVERSIDAD DEL QUINDIO. (20 de 08 de 2016). *www.mineducacion.gov.co.* Obtenido de http://www.mineducacion.gov.co/cvn/1665/w3-article-326627.html

Universidad UCOL. (2016). Obtenido de http://docente.ucol.mx/sadanary/public_html/bd/cs.htm

Wikispace. (2016). *Fundamentos de Redes.* Obtenido de https://fundamentos-redes.wikispaces.com/Tema+3.+Capa+de+aplicaci%C3%B3n