TRANSICIÓN AL PROTOCOLO IPV6, ASPECTOS DE SEGURIDAD INFORMÁTICA PARA TENER PRESENTE

RICARDO ANDRES CHICA MORA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2020

TRANSICIÓN AL PROTOCOLO IPV6, ASPECTOS DE SEGURIDAD INFORMÁTICA PARA TENER PRESENTE

RICARDO ANDRES CHICA MORA

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Director de Proyecto:
LIC. DANNY FERNANDO LEON JARAMILLO MSc.

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

BOGOTA., 29/05/2020

DEDICATORIA

Con cariño dedico este trabajo a mis padres, que aun en la distancia me han apoyado en cada proyecto que inicio, su amor y entrega fueron fundamentales en este proceso, cada consejo me guio en este viaje en busca de conocimiento. Dedico también este trabajo a los colegas que aportaron sus ideas para lograr la finalización de este proyecto.

AGRADECIMIENTOS

Agradezco a tutores y asesores que con su experiencia fomentaron la búsqueda de los elementos necesarios para llevar a cabo este proceso, sin sus conocimientos no se hubiera logrado finalizar esta monografía. De igual forma, un agradecimiento a las directivas de la Universidad Abierta y a Distancia UNAD, por todo el apoyo y gestión.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ANCHO DE BANDA: Cantidad de datos posibles a transmitir entre puntos en un lapso específico de tiempo.

ACTIVO INFORMATICO: Recurso de tipo Hardware y Software que forman parte del inventario de una entidad.

BINARIO: Sistemas de numero representado por dos dígitos (0 y 1).

CABECERA: Información ubicada al inicio de un bloque de datos que es almacenado o trasmitido.

CIBERATAQUES: Explotación deliberada de un sistema informático.

CRIPTOGRAFÍA: Procedimiento para la protección de datos, mediante el uso cifras o códigos para ocultar el contenido.

COLISIÓN: La resultante del proceso de nodos trasmitiendo a la vez.

CONMUTACIÓN: Proceso de envió de información en una red de dispositivos.

ENRUTAMIENTO: Búsqueda del camino más viable entre todas las disponibles, para la trasmisión de paquetes.

HOST: Dispositivo que forma parte de una red informática.

HUB: Punto de conexión común para dispositivos en una red.

INFRAESTRUCTURA: En redes, son elementos imprescindibles que permiten obtener servicios de telecomunicaciones en una empresa.

INTERFACE: Dispositivos o sistemas implementado para interactuar entre sí.

IP: Protocolo de red encargado de asignar una etiqueta de red a los dispositivos conectados a una red informática.

IPSEC: Medidas de seguridad que buscan la protección en trasmisiones por medio del protocolo IP.

NODO: Punto de redistribución o un punto final de comunicación.

PAQUETE: Unidad de datos formateada que se transporte por medio de una red de paquetes conmutada.
PING: Utilidad de software de administración de redes informáticas, implementada para verificar conexión o accesibilidad de un host en una IP.

PROTOCOLO: Conjunto de reglas que estipula como los dispositivos en una red intercambian paquetes.

ROUTER: Dispositivos de red que se encarga de reenviar paquetes entre redes de computadoras.

TOPOLOGIA: Disposición de una red donde se incluyen sus nodos y las diferentes líneas de conexión.

TRAMA: Unidad de envío paquetes de datos.

RESUMEN

El siguiente trabajo está enfocado en el estudio de los pasos necesarios para lograr un proceso de migración del protocolo IPV4 al protocolo IPV6 de manera exitosa, mencionando las herramientas necesarias a implementar, buscando que la transición se logre de una forma transparente, evitando complicaciones en los servicios de la entidad que desea realizar la actualización; esto con el fin de dar solución a las múltiples problemáticas que se han evidenciado en el protocolo IPV4, problemáticas que generan un atraso e impiden el uso de nuevas aplicaciones que son fundamentales para la evolución de los procesos de comunicación. El nuevo protocolo se presenta como solución y forma de subsanar las falencias que su antecesor ha dejado en evidencia. Comprendiendo que este proceso de migración tiene su grado de complejidad, se requiere de una rigurosa investigación y conceptualización, por tal motivo se presenta la siguiente monografía con el fin de guiar de forma correcta en el curso de la transición.

En este escrito, se plantean fases básicas las cuales buscan que la migración se logre con la mayor transparencia posible, pensando en la normalidad de los procesos de la empresa que asuma el reto, cada fase cuenta con una serie de actividades que incorporándolas en un cronograma dará vía al cambio entre el IPV4 e IPV6. Cada entidad podrá tomar como base estas fases y sus respectivas actividades para la construcción de un cronograma, este será ajustado a la necesidad de la compañía, sin saltar procesos que pudieran ser vitales para la adopción del protocolo IPV6.

PALABRAS CLAVES: PROTOCOLO, IPV6, IPV4, REDES, BROADCAST, ANCHO DE BANDA, CRIPTOGRAFÍA, ENRUTAMIENTO, HOST, HUB, INTERFAZ, IP, IPSEC, PAQUETE, ROUTER, TOPOLOGÍA, TRAMA, ENLACE, LACNIC, STACK, VLANS, FIREWALL.

ABSTRACT

The following work is focused on the explanation of the steps necessary to achieve a process of migration of the IPV4 protocol to the IPV6 protocol in a successful way, mentioning the necessary tools to be implemented, looking for the transition to be achieved in a transparent way, avoiding complications in the services of the entity that wishes to perform the update; this in order to solve the multiple problems that have been evidenced in the IPV4 protocol, problems that generate a delay and prevent the use of new applications that are fundamental for the evolution of communication processes. The new protocol is presented as a solution and way of correcting the shortcomings that its predecessor has left in evidence. Understanding that this migration process has its degree of complexity, a rigorous investigation and conceptualization is required, for this reason the following monograph is presented in order to guide correctly during the transition.

In this paper, basic phases are proposed which seek that migration be achieved with the greatest possible transparency, thinking about the normality of the company's processes that take on the challenge, each phase has a series of activities that incorporating them into a schedule will give way to the change between IPV4 and IPV6. Each entity may take as a basis these phases and their respective activities for the construction of a schedule, this will be adjusted to the need of the company, without skipping processes that could be vital for the adoption of the IPV6 protocol.

KEYWORDS: PROTOCOL, IPV6, IPV4, NETWORKS, BROADCAST, BANDWIDTH, CRYPTOGRAPHY, ROUTING, HOST, HUB, INTERFACE, IP, IPSEC, PACKAGE, ROUTER, TOPOLOGY, PLOT, LINK, LACNIC, STACK, VLANS, FIREWALL.

INTRODUCCIÓN

Actualmente, Internet se ha convertido en una red global que atiende a millones de usuarios y esto ha sucedido debido a la amplia aceptación del protocolo de Internet (IP). IPV4 es una de las versiones más reciente y la más utilizada actualmente con más de tres décadas de antigüedad, es un protocolo que ha presentado muchas limitaciones. La mayor limitación es su espacio de direccionamiento de 32 bits que da como resultado un aproximado de 4,3 mil millones de direcciones IP. El rápido crecimiento de Internet, banda ancha, suscriptores móviles y el despliegue de la tecnología NGN (red de siguiente generación) ha llevado a un consumo acelerado de direcciones IP, y esto da como resultado una escasez de direcciones IPV4 en todo el mundo.

Para superar este problema de escasez, se desarrolló el Protocolo de Internet versión 6 (IPV6), que mejora las incapacidades de direccionamiento encontradas en IPV4 mediante el uso de direcciones de 128 bits, lo que prácticamente pone a disposición un conjunto casi infinito de direcciones IP. Además, IPV6 tiene varias mejoras sobre IPV4, como ejemplo la posibilidad de asignar varias direcciones de red a un mismo dispositivo, el cifrado e IPsec (Internet Protocol Security) que ya se encuentran integrados; anteriormente se debía realizar una suma de verificación para detectar cambios accidentales, sin embargo, el protocolo IPV6 cuenta con un mecanismo de control de errores propio, evitando que se deban realizar los conocidos checksums (suma de verificación), a estos beneficios le sumamos que IPV6 presenta una mejora en el rendimiento, así se logra evidenciar como el protocolo IP en su sexta versión, es una gran alternativa para las empresas que quieran un mejor desempeño de sus sistemas y sus redes.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Es evidente la evolución de las comunicaciones por medio de las redes y que esta evolución exige una gran demanda de equipos o dispositivos conectados todo el tiempo, generando así que el protocolo IPV4 se encuentre en medio de una saturación, evitando un crecimiento de la infraestructura tecnológica de compañías que estén en el proceso de actualización, cayendo en el agotamiento que sufre el protocolo IP en su cuarta versión, esto genera obstáculos que limitan las posibilidades de innovación en los servicios.

El protocolo IPV6 se presenta para permitir el crecimiento de internet en lugares donde hay superpoblación, por ende, un gran número de dispositivos buscando conexión a internet y ante la necesidad de más IP's se generan múltiples inconvenientes. El protocolo IPV6 contribuye a que las personas que necesitan conectarse a la red lo puedan lograr y a su vez contar con excelentes niveles de seguridad que buscan mantener a salvo la información. Se evidencian mejoras en el cifrado de datos, esto garantiza que los datos sean auténticos, íntegros y permanezcan en absoluta confidencialidad.

En Latinoamérica Brasil ha sido pionero en la puesta en funcionamiento de IPV6, avanzando de forma constante y a una excelente velocidad, por otro lado, Colombia ha dado unos pequeños pero importantes pasos, a pesar de que su avance no ha sido tan notorio, y que solo una pequeña parte del país está cubierta por este nuevo protocolo, Colombia se encuentra en los primeros puestos en Latinoamérica en relación con el trabajo del protocolo IPV6.

La IANA (Internet Assigned Numbers Authority) en el año 2011 realizo entrega de los grupos finales y los últimos disponibles de direcciones en el rango del protocolo IPV4, y según los informes en Latinoamérica, la reserva de direcciones IP ya está siendo utilizada, esto es una clara explicación de la necesidad tan urgente de realizar la transición entre protocolos.

En Colombia existe una circular publicada por Mintic (Ministerios de Tecnologías de la Información y las Comunicaciones), que hace referencia a la "Promoción de la adopción del IPV6 en Colombia", en este documento se destaca la necesidad de evolucionar, notificando que es de vital importancia recurrir al proceso de migración. En el documento se enuncia el agotamiento que sufrió el IPV4, realizando una sugerencia a las compañías para que migren hacia el nuevo protocolo. Esta migración tiene como objetivo incrementar las conexiones, ampliando los usuarios conectados a banda ancha con una mejora en las conexiones.

Por otra parte, RENATA (Red Nacional de Tecnología Avanzada) que es la red nacional de investigación y educación de Colombia, redactó un informe en el año

2013 donde menciono que “las instituciones que no realicen la transición presentaran un atraso y sufrirán las problemática al no poder usar algunos recurso de internet”, si se analiza esta problemática, llegamos a la conclusión de que las desventajas de no estar actualizados son muchas, y traerán consecuencias de gran magnitud en los procesos que se quieran llevar a cabo dentro de una compañía. El proceso de migración no será de gran impacto presupuestal, sin embargo, el permitir que la transición se prolongue demasiado, provocara en un futuro que los costos se eleven demasiado.

1.2 FORMULACION DEL PROBLEMA

Basado en los anterior, y mencionando que en el proceso de migración puede presentar dificultades tales como la incompatibilidad y la necesidad de no interrumpir los servicios para no afectar los procesos de la compañía, según el testimonio y las experiencias vividas por entidades que ya realizaron la migración como Colciencias, Contaduría General de la Nación y otras más, se plantea un documento en el cual se pretende dar respuesta a la siguiente problemática, ¿Cómo realizar una transición al protocolo IPV6 en una empresa que aun labora con las limitaciones del protocolo IPV4, sin alterar las funciones de las aplicaciones que dependen del protocolo IP en su cuarta versión para su funcionamiento?

2 JUSTIFICACIÓN

La siguiente propuesta se basa en la interpretación del protocolo IPV6, ya que facilitará la conexión a banda ancha para los equipos que cuenten con este protocolo instalado, al encontrar una cantidad considerable de espacio de direcciones IP, permite que una empresa cuente con una herramienta que facilite la conectividad de múltiples dispositivos de forma simultánea a la red, buscando mejorar la calidad del servicio, sin olvidar que esta transición es sinónimo de seguir evolucionando y no permitir que el auge tecnológico y el futuro los deje en olvido.

Actualmente, la necesidad de un protocolo que brinde las garantías necesarias para que una institución o compañía cuente con características adecuada en el tráfico de datos es notoria ante la creciente demanda de conexión que es realizada a través de múltiples dispositivos, y a esto se le suma que las IP's públicas se vuelvan más escasas y obliga a los expertos a mejorar las practica para salvaguardar la corriente de información. El protocolo IPV6 es una solución necesaria para corregir la gran cantidad de errores y falencias que se han manifestado en la implantación del IPV4, lo que en pocas palabras significa que sus beneficios quedan reflejados en diversas áreas de la infraestructura donde se realice la migración, llevando al protocolo IPV6 a tomar la vanguardia en el campo de la tecnología, logrando aplicar mejores tiempos de respuesta a esas nuevas aplicaciones que surgen en el mercado, sin dejar de mencionar que realizar esta transición permite que una compañía tenga una red más segura en la cual podrá confiar.

La incertidumbre que se presenta al momento del cambio es un obstáculo complejo que encierra las mentes de los usuarios, la cual impide ver los grandes beneficios que posee este nuevo protocolo, todas las dudas se generan por falta de conocimiento. Considerando lo anterior, es importante involucrar actividades de capacitación que permita a los usuarios lograr una mejor perspectiva en relación con la adopción del protocolo de internet en su sexta versión.

En el siguiente documento se exponen las bases necesarias para lograr la transición la cual brindara beneficios importantes a quien elija acoger el protocolo IPV6, buscando la mejora continua de las conexiones, ampliando las posibilidades de adquirir herramientas actualizadas que soporten el protocolo IPV6.El documento presentado a continuación, busca explicar todo el proceso con el fin de capacitar usuarios, y que estos logren discernir con claridad la diferencia entre IPV4 e IPV6.

3 ALCANCES

Este proyecto busca orientar las entidades que estén interesadas en el proceso de transición desde IPV4 a IPV6, teniendo en cuenta las normativas emitidas por MIN TIC (Ministerio de Tecnologías de la Información y la Comunicación). Este escrito describe las diferentes fases para el proceso de transición, y las directrices concretas y fundamentales al momento de realizar la planeación de la transición.

Las actividades descritas en la presente monografía son actividades que permiten orientar a la entidad interesada en el cambio, en todo el proceso de migración y las diferentes acciones que se deben realizar al momento de ejecutar el proyecto de migración, esto involucra inventario de activos, informes que detallen los componentes y el diseño de la infraestructura de red de comunicaciones, esto con el fin de alimentar una propuesta de plan de transición.

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Presentar un documento que permita determinar el debido proceso de la migración de protocolo IPV4 a IPV6 teniendo presente aspectos relevantes en el tratamiento de la información y la seguridad informática.

4.2 OBJETIVOS ESPECIFICOS

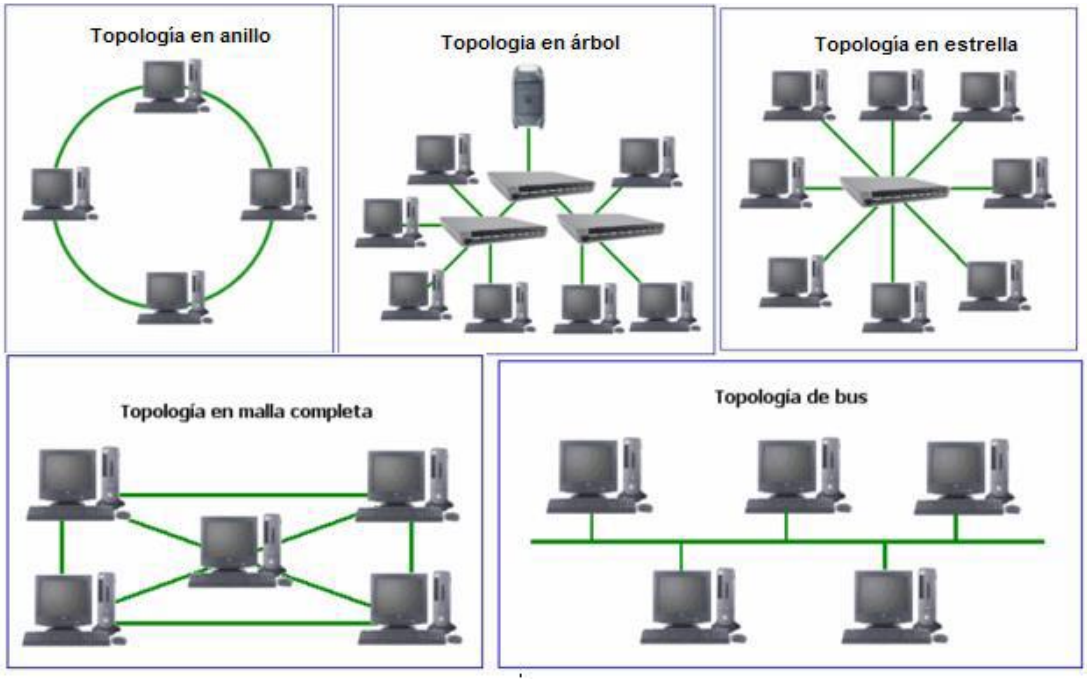
- Realizar un estudio sobre los mecanismos y procesos implementados en el protocolo IPV6.
- Establecer recomendaciones para mejorar la seguridad aplicando las nuevas tecnologías que soportan IPV6.
- Generar un documento que contribuya y brinde orientación en el proceso de transición de IPV4 a IPV6.

5 MARCO CONCEPTUAL

5.1 REDES DE DATOS:

Todo el grupo de elementos formados por software y hardware, cuya conexión por medios físicos permiten la comunicación para el intercambio de datos logrando así la posibilidad de compartir información. Podemos encontrar varios tipos de redes, como red de área local (LAN), red de área metropolitana (MAN), red de área extensa (WAN), y mucha más, y además encontramos diseños (topologías), como red en anillo, en árbol, en estrella, en malla y bus.[1]

Figura 1: Topologías comunes en redes de datos



5.2 PROTOCOLO:

Como ese conjunto de normas, procedimientos fundamentales para la transferencia de datos, conociendo el emisor y el receptor se logra el proceso de comunicación. Es una tecnología uniforme, cuando se presenta un acuerdo entre la pluralidad de redes que constituyen la Internet para enviar o recibir información, lo ofrece el lenguaje común, el cual lleva el nombre de protocolo TCP/IP (transmision Control Protocol/ Internet Protocol).

[1] FONSECA CASTRO, Diana. *Plan de Transición Del Protocolo De Red IPv4 a IPv6 Basada En Las Recomendaciones Realizadas Por El Min Tic Colombia.* [En Línea]. Fusagasugá. Disponible en: http://fusagasuga-cundinamarca.gov.co/Transparencia/MODELO%20INTEGRADO%20DE%20PLANEACION%20Y%20GESTION/Plan%20de%20Transicion%20del%20Protocolo.pdf

En este proceso podemos presenciar el momento en el que un usuario de una computadora se transmuta hacia cliente cuanto solicita acceso a una página Web, otro caso en el que se podría evidenciar esta transformación es cuando se realiza el acceso por medio de una línea telefónica, solicitando información acerca de productos o algún tipo de servicio a un proveedor, quien en este proceso tomaría el rol de servidor.

Los conjuntos de caracteres son elementos bases del protocolo de comunicación, reglas para que la comunicación posea una secuencia y una sincronización en cada mensaje formado, bajo los procedimientos que informan sobre posibles falencias. Normalmente la formación de este conjunto de caracteres se divide en:

- Caracteres imprimibles.
- Caracteres de Control.

Dicha comunicación, solo es posible cuando ambos puntos implementan la misma configuración en sus protocolos. Cuando se enuncian los niveles de comunicaciones, estos se refieren a las modalidades que se usan para la comunicación de las aplicaciones (Reglas de alto nivel) y las que definen como se trasmiten las señales (Reglas de bajo nivel). Estas últimas define le modo y la organización de la información.

La estación maestra, está encargada de la trasmisión en el momento del circuito de la comunicación, la estación receptora se llama estación esclava. Cuando nos referimos a una red centralizada, definimos la estación primaria como controladora de las trasmisiones. Esta estación también define que estación es maestra, está a la disposición de convertirse en estación receptora. Cuando hablamos de interrogación, nos referimos a la invitación que realiza la estación primaria con el fin de trasmitir un mensaje hacia la estación secundaria.[2]

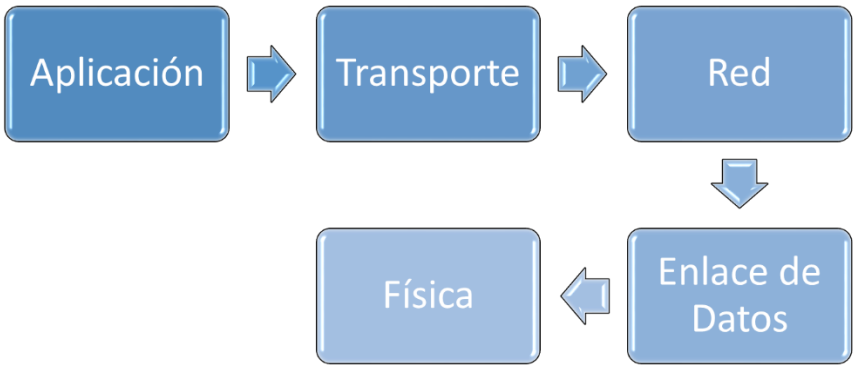
En términos generales podemos definir los protocolos en:

- Asíncronos: datos y módems asíncronos.
- Síncronos: datos y módems síncronos.

5.3 PROTOCOLO TCP/IP:

[2] *Protocolo de Comunicación, Capitulo 3.* [En Línea]. Disponible en : http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/734/A6.pdf

Figura 2: Protocolo TCP/IP



En un punto de la historia cuando la red fue creciendo, y pasó de conectar universidades e instalaciones del gobierno a conectar redes satelitales, se evidencio como se presentaban falencias en la interacción entre protocolos existentes y las avanzadas redes que iban a evolucionando de una forma notable, fue entonces cuando se produjo la necesidad de generar una nueva arquitectura de referencia moderna. Esta arquitectura es la conocida como modelo de referencia TCP/IP.

"TCP e IP son los protocolos más importantes"[3], esta arquitectura está formada por cinco niveles o capas:

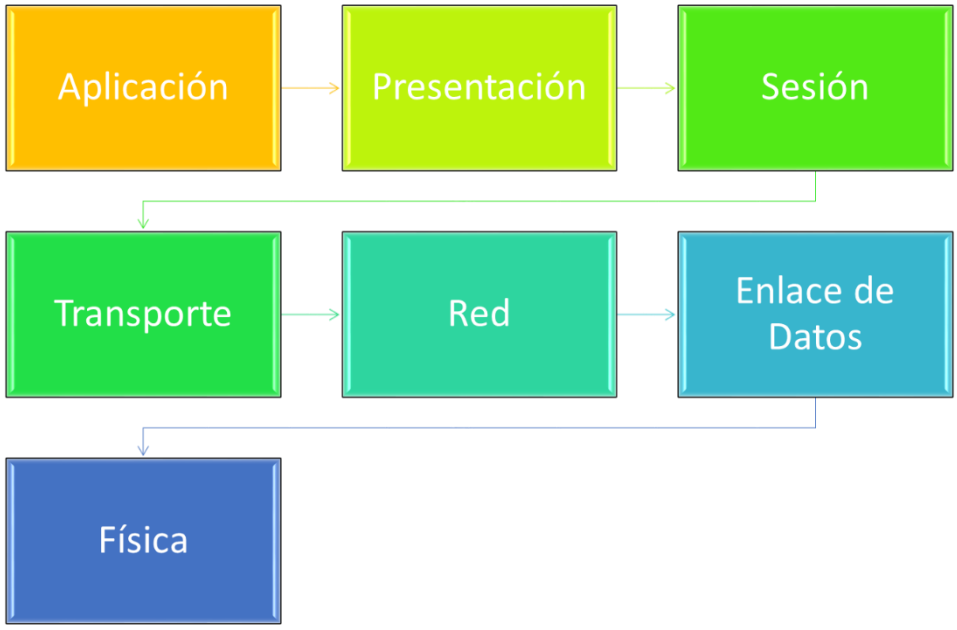
- Aplicación: contiene los protocolos SMTP que permite la interacción con correo electrónico, FTP usado para la trasferencia de archivos, Telnet para conexiones remotas, Http.
- Transporte: TCP, UDP.
- Internet: envió de información, ubicación en nivel de red.
- Físico: análogo nivel físico.
- Red: interfaz de red.

5.4 PROTOCOLO OSI.

Su objetivo principal es establecer lineamientos estructurados para el intercambio de información. En cuestión de las ventajas podemos decir que las capas nos brindan la comunicación de diversas computadoras en distintos niveles. Con el avance de la tecnología, se ha contado con la posibilidad el protocolo de alguna capa en específico sin necesidad de modificar las demás.

[3] ESTRADA CARDONA, Adrián. Protocolos TCP/IP de Internet. [En Línea]. México. Disponible en: http://www.revista.unam.mx/vol.5/num8/art51/sep_art51.pdf

Figura 3: Modelo OSI



Capa Física, especificaciones necesarias para ingresar a la red, por medio de las normas que abarcan lo físico, eléctrico, funcional y procedimental.

Capa de enlace de datos, respuesta obtenida cuando se produce comunicación entre nodos de primer nivel y nodos de segundo nivel. Otra función relevante es proporcionar la trama final de la envolvente de los datos, haciendo posible el flujo ordenado de datos entre nodos, y permite la detección y corrección de errores.

Capa de red, indica que configuración es la más indicada para la función suministrada por la red.

Capa de transporte, control sobre la integridad del mensaje, desde que sale hasta que llega, incluyendo todo el proceso de segmentación y recuperación de errores, al igual que la ruta. En relación con las comunicaciones, esta capa es la más alta.

Capa de sesión, su tarea es prever la disponibilidad de la red, procedimientos para el ingreso de los paquetes y la salida de estos de la red.
Capa de presentación, conversión de código o de sintaxis necesaria para la respectiva presentación de los datos a la red.

Capa de aplicación, nivel más alto en relación con la jerarquía, análoga al administrador general de la red.

5.5 IPV4.

Protocolo implementado para comprobar dispositivos conectados a una red por medio de un sistema de direccionamiento. La estructura el protocolo IP en su cuarta versión fue diseñada para el uso en sistemas interconectados de redes de comunicación de host con conmutación de paquetes.

En la actualidad el protocolo más utilizado para realizar las conexiones es el IPV4, bajo un esquema de direcciones de 32 bits, este esquema genera una cantidad total de 2 ^ 32 direcciones (un aproximado de 4 mil millones de direcciones IP).

"El protocolo Internet está diseñado para la comunicación de computadoras mediante el intercambio de paquetes, para esta comunicación el protocolo implementa las funciones de direccionamiento y fragmentación, por lo que debe proporcionar el soporte necesario para que pueda viajar el paquete, así como la fragmentación y el reensamble del paquete."[4]

5.5.1 Estructura del datagrama IPV4

Es una división en bloques de 32 bits, correspondiente a 4 bytes, esto va en el siguiente orden, inicia de izquierda a derecha y de arriba abajo. Siempre ha de iniciar con el bit 0, es de vital importancia conservar un orden ya que dependiendo el equipo al que se está intentando comunicar será el procedimiento que lleve a cabo para guardar en la memoria los bits.

5.5.2 Direccionamiento IPV4.

las direcciones (origen y destino), poseen un numero de 32 bits, los equipos deben tener un numero especifico, que en este protocolo son 4 octetos de 8 bits. Existen diferentes tipos de redes, descritos a continuación:

- Clase A: Desde 0.0.0.0 hasta 127.255.255.255
- Clase B: Desde 128.0.0.0 hasta 191.255.255.255
- Clase C: Desde 192.0.0.0 hasta 223.255.255.255
- Clase D: Desde 224.0.0.0 hasta 239.255.255.255
- Clase E: Desde 240.0.0.0 hasta 247.255.255.255

[4] PEREZ NAVA, Juan. HERRERA GUTIERREZ, Tecnologías y Mecanismos de Transición de Ipv4 a Ipv6. [En Línea]. México. Disponible en: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/2807/Tesis.pdf?sequence=1

El direccionamiento inicial en redes basadas en IP se realizó mediante el principio de clase de red (había clases que compartían espacio de direcciones para bloques grandes) Sin embargo, este esquema demostró ser poco práctico y hoy en día se usa el direccionamiento sin clase en Internet, conocido como Enrutamiento sin dominio entre clases, o CIDR abreviado. En general, los bloques CIDR pueden describir el rango de direcciones IP como las subredes de Internet. Por lo tanto, el estándar para la notación CIDR es un registro de "/" y un número de 0 a 32 seguido de la dirección IP que especifica los bits de la máscara de subred, ejemplo, 12.13.14.0/24.

5.5.3 Estructura de una dirección IPV4.

Todos los elementos que se encuentren en una red tienen por obligaciones estar definidos de manera independiente y exclusiva. Al ubicarse en la red, se hace imprescindible reconocer los paquetes que están involucrados en la transferencia por medio de sus respectivas direcciones IP, tanto de salida como, de entrada. Con el protocolo IPV4, se identifica que las direcciones de los paquetes tanto de origen como de destino tendrán 32 bits en el encabezado de capa 3.

Cada patrón de binarios que representa direcciones IP en su cuarta versión se relaciona implementando un punto decimal que se encarga de separar los bytes. Las direcciones IPV4, una porción de los bits pertenecientes al orden superior cumple el papel de representar la dirección de red. Cuando nos referimos a la red en la capa 3, hacemos énfasis a un grupo de host con patrones semejantes en la porción de dirección de red de sus direcciones. Se entiende entonces que 32 bits definen una dirección IPV4, sin embargo, hay una cantidad variable de bits que forman parte de host de la dirección. La cantidad de bits implementados en esta porción permite conocer la cantidad de equipos que tienen la posibilidad de conectarse en la red.

5.6 IPV6

La sexta versión del protocolo IP permite la transferencia de datos por medio de la una red de conmutación de paquetes. El intercambio de mensajes implica salida y entrada de datos en paquetes entre nodos en una red. El Grupo de Trabajo de Ingeniería de Internet (IERTF) público en 1998 el estándar de trabajo para el protocolo IPV6. La especificación IETF para IPV6 es RFC 2460. La intención de IPV6 era reemplazar el servicio ofrecido por IPV4 ampliamente utilizando lo que se considera la columna vertebral de la internet moderna. IPV6 a menudo se denomina “Internet de próxima generación” debido a sus capacidades ampliadas y su crecimiento a través de implementaciones recientes a gran escala. En 2004, Corea y Japón tuvieron el reconocimiento por tener los principales despliegues públicos de IPV6.

5.6.1 Capacidades de direccionamiento extendida

El incremento el tamaño de direcciones IP, permite soportar más niveles de direccionamiento jerárquico, un numero mucho mayor de nodos direccionables, y una configuración más sencilla de direcciones. Agregando el campo “ámbito” a las direcciones multienvío, la escalabilidad del enrutamiento multienvío se mejora. Se define entonces un nuevo tipo de dirección, que permite él envió de una cantidad mayor de paquetes a cualquier grupo de nodos.

Tabla 1: Datagrama IPV6

<table>
<tr><td>Versión</td><td>Clase del trafico</td><td colspan="2">Etiqueta del Flujo</td></tr>
<tr><td colspan="2">Longitud de la carga útil</td><td>Jefe siguiente</td><td>Límite del salto</td></tr>
<tr><td colspan="4">Dirección de fuente</td></tr>
<tr><td colspan="4">Dirección de destino</td></tr>
</table>

La constante evolución y crecimiento de dispositivos requiere una gran disponibilidad de bloques adicionales de IP’s. En la actualidad IPV4 permite un máximo de aproximadamente 4.3 millones de direcciones IP únicas, por el contrario, IPv6 admite un máximo teórico de 2128 direcciones.

Ambos protocolos comparten una dirección similar, y a esto se le puede sumar que los protocolos de la capa de transporte que funcionan con Ipv4, funcionaran de la misma forma con el protocolo IPV6.

Cuando nos referimos a las ventajas de la versión 6 de este protocolo, es importante mencionar unas de sus principales ventajas, esta es el mayor espacio que posee

para direcciones. Al contar con una longitud de 128 bits de las direcciones, sobre pasa las limitantes encontradas en IPV4 que solo cuenta con una longitud de 32 bits. Esto genera un número casi ilimitado en las direcciones IP únicas. El tamaño del espacio de direcciones IPV6 lo hace menos vulnerable a actividades maliciosas como el escaneo de IP.

El soporte nativo para los equipos móviles, son una mejora notable y fundamental en IPV4. La compatibilidad de IPV6 con el protocolo Mobile IPV6 (MIPV6), permite que los dispositivos móviles se logren alternar entre redes y recibir una notificación de itinerantica autónoma de la ubicación física.

"Cada dirección IPV6 tiene un ámbito, que es un área dentro de la cual esta puede ser utilizada como identificador único de una o varios interfaces. El ámbito de cada dirección forma parte de la misma dirección."[5]

5.7 NOMENCLATURA DE LAS DIRECCIONES.

Unicast, identificación de una sola interfaz.
Multicast, identificación de un conjunto de interfaces, ubicados en nodos distantes
Anycast, identificación de conjuntos de interfaces que probablemente se encuentren en nodos distintos.

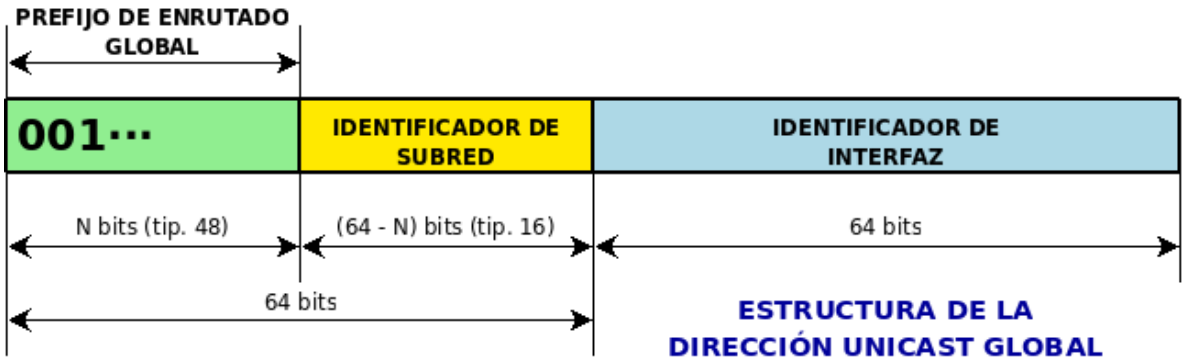
5.7.1 UNICAST

Grupo de direcciones cuya característica principal es identificar del destino el único punto final. Las interfaces por obligación deben tener como mínimo un enlace local Unicast. Los datagramas se enviarán y se entregarán a un solo punto.

La transmisión de unidifusión, en la que se envía un paquete desde una única fuente a un destino específico, sigue siendo la forma predominante de transmisión en las LAN y dentro de Internet. Las redes LAN admiten la modalidad de transferencia unicast.

[5] CORREA, Adelaida. Candamil, Martha. Mecanismo de transición Ipv4 a Ipv6. [En Línea]. Bogotá. Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/8797/MONOGRAFIA%20MECANISMOS%20DE%20TRANSICI%C3%93N%20DE%20IPV4%20A%20IPV6.pdf?sequence=1

Figura 4: Direcciones Unicast Globales



5.7.2 BROADCAST

Proceso donde se envía información desde un punto a todos los destinos posibles. Debería existir solo un remitente en este caso, sin embargo, la información se entrega a todos los receptores posible que se encuentren conectados. Este tipo de transmisión es compatible con la mayoría de las LAN, y es posible enviar la misma información a todos los puntos conectados por LAN.

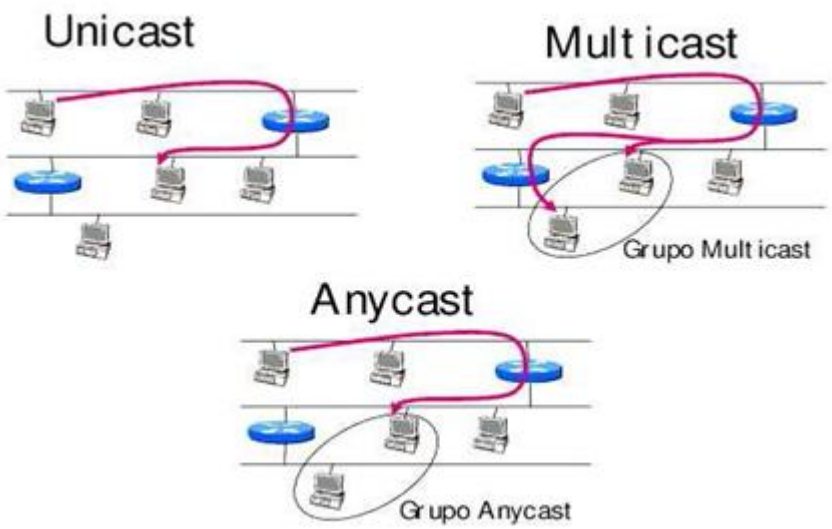
5.7.3 ANYCAST

Si se habla de una dirección IPV6 Anycast, se refiere a una dirección asignada a varias interfaces, la mayor característica de este proceso es que la información enviada toma el camino hacia la dirección Anycast más cercana, entre las posibilidades de entrega que tenga que abordar. Este tipo de direcciones son asignadas desde el espacio de direcciones únicas.

Unas de las características clave de este tipo de transmisión es que la estrategia de red puede permitir que se envíen mensajes a un grupo de receptores que tienen la misma dirección de destino. Anycast es un método de dirección y una metodología de enrutamiento contrastada con otras, por ejemplo, Unicast implementa una conexión uno a uno entre un servidor y una dirección de destino. Otras modalidades de trasmisión, como la multidifusión, envían señales desde un punto a varios puntos.

Anycasting se rige por el BGP (Border Gateway Protocol), y es usada por IPV4 e IPV6 y posee su propia configuración de seguridad que se observa cuando se decide como enrutar el tráfico de red. Hay expertos que afirman que la duplicación de los servicios de DNS de Anycast puede ser una forma de no padecer ante diferentes tipos de ciberataques donde los hackers buscan obtener acceso a las plataformas a través del secuestro del tráfico de red. Otros expertos señalan que anycast tiene conmutación por error automática, lo que promueve la tolerancia a fallas y la gestión de emergencias.

Figura 5: Anycast, Unicast, Multicast



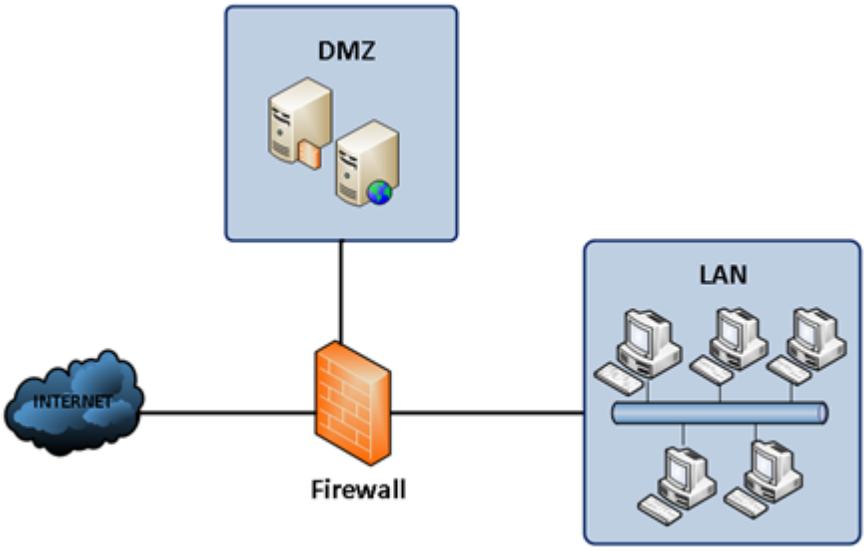
5.7.4 MULTICAST

La transferencia de datos entre un solo remitente y múltiples receptores, que se encuentren conectados a una red. La multidifusión es compatible con redes inalámbricas como parte de la tecnología CDPD (Cellular Digital Packet Data).

Antes de que cualquier equipo pueda recibir información, el equipo deberá estar subscrito a un grupo de comunicación, dando a conocer esta suscripción por medio de mensajes IGMP. Una vez conozca la información, el router se encargará de redirigir esta información.

5.8 ZONA DESMILITARIZADA (DMZ).

Figura 6: Red DMZ



Es un diseño conceptual de red el cual tiene como objetivo es proteger de forma más completa la red interna (intranet), de una organización, esto está basado en la separación de aquellos servicios privados (Bases de datos, servidores, etc.) de la red que ofrece servicios al público (internet).[6]

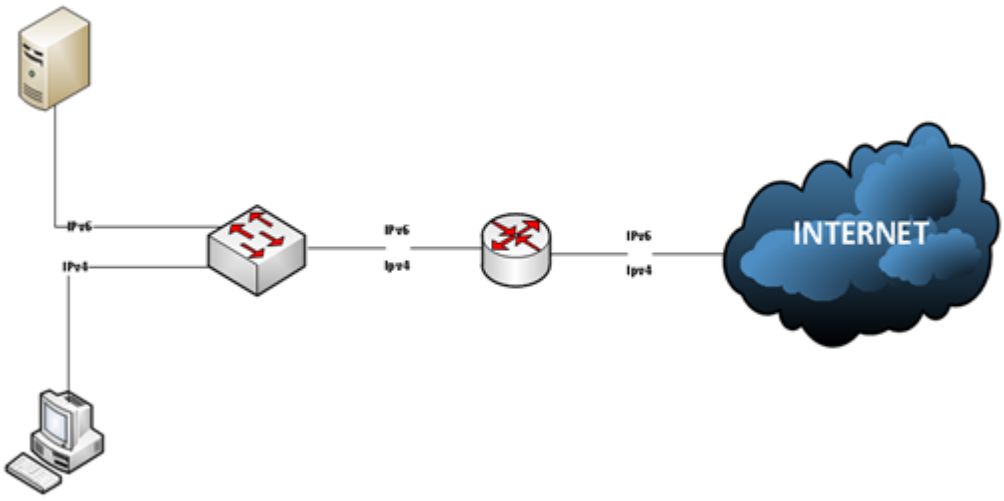
5.9 DUAL STACK (DOBLE PILA)

Esta herramienta está planteada para permitir que un nodo utilice un stack IPV4 y un Stack IPV6 al mismo tiempo, encontrando así dos ventajas, con un nodo doble pila se encuentra el camino viable para comunicar nodos que cuentan con Stack IPV4 de una forma nativa, y por el otro lado permite comunicación con nodos que solo tenga habilitados el Stack IPV6 de forma nativa.[7]

[6] RAMIREZ PULIDO, Diego. GUZMÁN PANTOJA, Jaime. BELTRAN DIAZ, Jesús. *Diseño De La Transición Del Protocolo IPV4 Hacia IPV6 En La Agencia Colombiana Para La Reintegración-ACR Con Base En Consideraciones De Seguridad En Implementación De Ipv6.* [En Línea]. Bogotá. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/2803/1/IPV6.pdf

[7] Ibíd.

Figura 7: Dual Stack

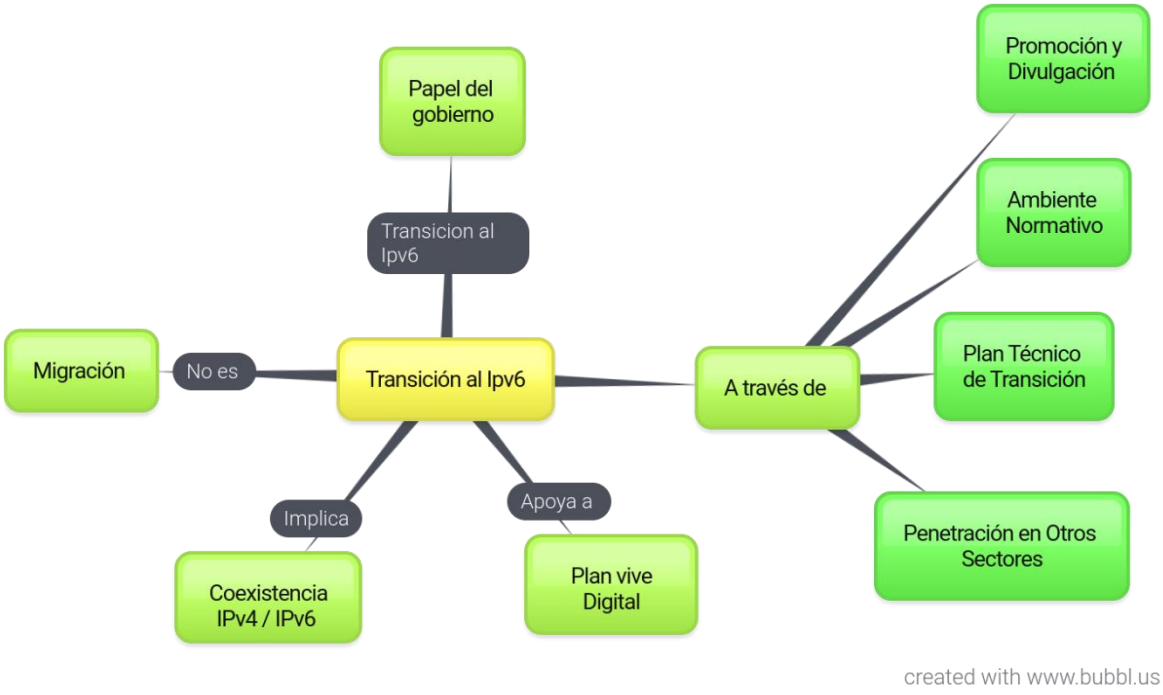


6 MARCO TEÓRICO

En el traspaso de IPV4 a IPV6 muchas organizaciones han dedicado esfuerzos y tiempos con el de lograr la expansión de este protocolo, cada compañía que ha finalizado este paso ha permitido evidenciar mejores resultados los cuales han podido permitir adquisición de nuevas tecnologías. A diferencia de las empresas de México, país que ha sido pionero en este proceso, lentamente las compañías e instituciones han mostrado el interés y la necesidad de surgir en la temática de IPV6.

Como bien se ha dicho, este protocolo es una actualización de forma general de su antecesor, por ende, desde su diseño se dedujeron que tenía que mientras se realizaba su lenta implementación, IPV6 debería seguir trabajando junto al IPV4.Todo esto proceso ha generado inconvenientes entre ellos la incompatibilidad entre protocolos, pero para dar solución a estas problemáticas se han ido desarrollando mecanismos para lograr una mejor transición.

Figura 8: Transición al IpV6



El despliegue de redes IPV6 está creciendo en todo el mundo. Se espera que el reemplazo completo de IPV4 tarde algún tiempo, ya que sigue siendo el protocolo de Internet más utilizado. Los Estados Unidos, China e India están liderando implementaciones recientes del protocolo IPV6 y tienen grandes inversiones en infraestructura de red IPV6. El gobierno de los Estados Unidos ha ordenado que las agencias federales deben completar la transición a una infraestructura IPV6 a más tardar en 2008. Las compañías de software también están lanzando sistemas operativos que admiten el estándar IPV6. En 1997, IBM se convirtió en el primer

proveedor comercial en soportar IPv6 a través de su sistema operativo AIX 4.3. Una de las versiones finales del sistema operativo Windows de Microsoft, Windows Vista, tiene compatibilidad total con IPv6 habilitada de forma predeterminada.

Para el año 2012, las 4.3 mil millones de direcciones con las que contaba el protocolo IPV4, se estaban agotando, ya que surgió un incremento de dispositivos (Computadores, tablets, impresoras, consolas de video juegos, y un sinfín de equipos que requieren de dirección IP. El nuevo sistema de direccionamiento de internet cubre la necesidad de más direcciones de computadora.

El mundo ya ha comenzado a adoptar IPV6, con las grandes propiedades web de Google y Facebook oficialmente en junio de 2012. Otras organizaciones son más lentas que otras para hacer el cambio. Debido a que alargar cada dirección de dispositivo posible requiere mucha administración, este cambio masivo no se completará de la noche a la mañana. Pero la urgencia está ahí, y los organismos privados y gubernamentales están haciendo la transición ahora. Espere que IPV6 sea un estándar universal para fines de 2012.

Según MINTIC, podemos encontrar unos beneficios, que son putos claves a tener en cuenta en el proceso de transición, entre los que podemos encontrar.

- El incremento de equipos conectado a la red de la empresa o entidad que desea implementar esta solución
- Proceso transparente.
- Mayor movilidad por mayor cantidad de IP’s
- Aumenta la seguridad.
- Minimizar gastos.
- Posibilidad de implementar nuevas aplicaciones y servicios.

6.1 EL ESTADO ACTUAL DE IPV6.

A pesar de estar finalizado en 1998, muy pocos lugares en Internet se han convertido a IPV6. En mayo de 2017, 37 países tenían más del 5% de su tráfico de Internet a través de IPV6. Sólo siete países tenían más del 15%. Sin embargo, a pesar de las cifras, este protocolo se está volviendo cada vez más popular.
En varias instituciones públicas y privadas hay un arduo trabajo para generar un impulso sobre la expansión de IPV6, entre estas instituciones está La comisión europea y el Departamento de Defensa Norteamericano. En Latinoamérica el país que precursor fue México, en temas de investigación y experimentación relacionados con el protocolo IPV6.

Los países siguientes que se sumergieron en procesos de transición fueron España, Chile, Argentina, Uruguay, Brasil.

6.2 IPV6 EN COLOMBIA:

Colombia ya ha comenzado a surgir en la temática de IPV6, con las siguientes entidades: la Corporación Autónoma Regional de Boyacá (Corpoboyacá), el Servicio Geológico Colombiano, el Instituto Nacional Penitenciario (INPEC), Ministerio de Minas y Energías, Ministerio de Tecnologías de la Información y las Comunicaciones (TIC, 2014)"[8].

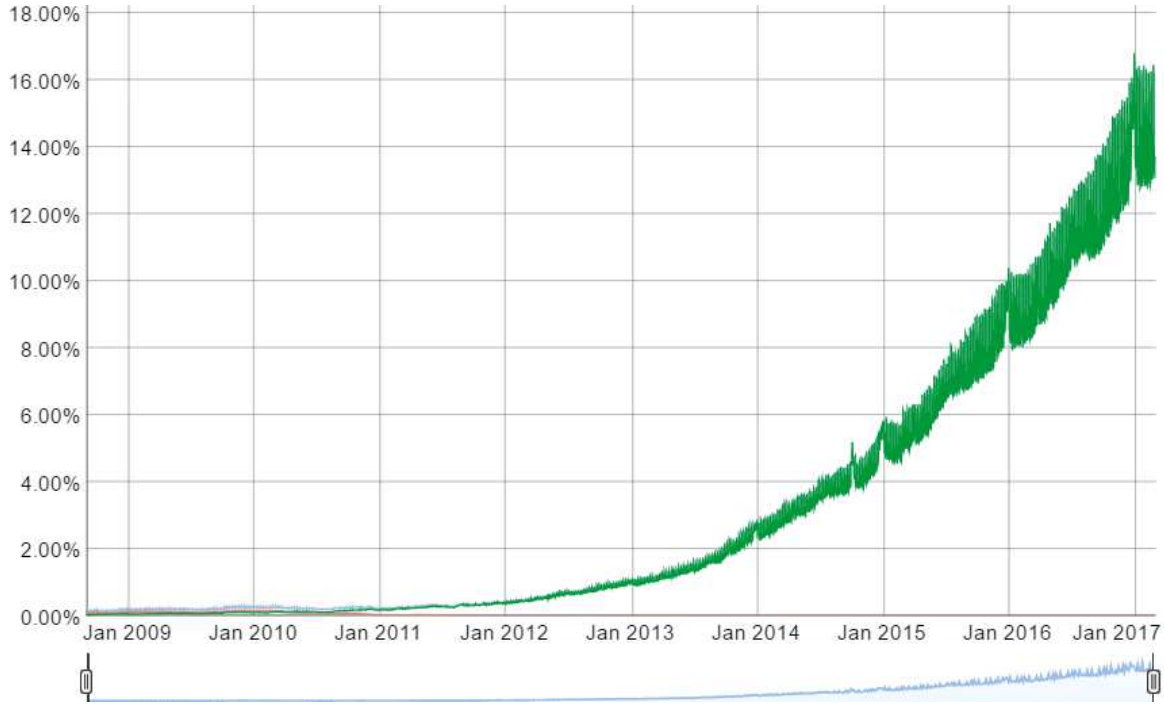
Cada labor de asistencia implica una serie de actividades, realización de marco referencial en el que se identifique la importancia de IPV6, así como una divulgación de anuncios actualizados de la LACNIC en materia del escaso direccionamiento IPV4.

Explicación de la circular 002 de 2011 y el manual de GEL 3.1, e información sobre los lineamientos para llevar a cabo la transición. UniNet, lidero un proyecto de promulgación sobre redes basadas en IPV6. A esta causa se sumaron la Universidad de Pamplona, la Universidades de Magdalena y la del Cauca.

Según un estudio realizado por CISCO, en el 2017 el despliegue del protocolo IPV6 en Colombia fue de un 23.96%, este hecho también está acompañado por un estudio que realizo Google, donde se evidencia un incremento en la adopción de este protocolo.

[8] RAMIREZ PULIDO, Ferney. GUZMAN PANTOJA, Jaime. BELTRAN DIAZ, Jesús. *Diseño De La Transición Del Protocolo Ipv4 Hacia Ipv6 En La Agencia Colombia Para La Reintegracion-Acr Con Base En Consideraciones De Seguridad En Implementación Ipv6* [en línea]. Bogotá. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/2803/1/IPV6.pdf

Figura 9:PORCENTAJE DE USUARIOS QUE ACCEDEN A GOOGLE POR DIRECCIONES IPV 6



Por otro lado, según las cifras arrojadas por la LACNIC, Colombia ocupa un gran puesto en cuanto a las organizaciones que decidieron implementar el protocolo IPV6. "Allí se establece que de las 62 organizaciones que han declarado su transición al protocolo IPV6, 13 son de Colombia, teniendo diez organizaciones que ya han implementado el protocolo, dos que están actualmente implementándolo y una que está en planificación de implementación."[9]

En la circular 002 de junio del 2011, se ha dispuesto desde el MINTIC, un plan de transición el cual se identifican los pasos necesarios para realizar el traslado de los servicios de red hacia el protocolo IPV6.

Mintic para el año 2009, identificó y realizó el planteamiento de la problemática que se sufría IPV4, está dejando en evidencia problemáticas que sufren las organizaciones al momento de asignar direcciones. Para el siguiente año se presenta una formulación inicial, de la mano con el sector TI, se realizan los siguientes aportes:

- Un documento inicial (borrador) de la resolución en la cual se establece lo necesario para realizar la migración y adoptar el protocolo IPV6.

[9] MORENO AGUDELO, José. *Transición de protocolo IPV4 A IPV6, para una Empresa del Estado, con Aplicación en una ciudad Intermedia.*

- Se realizó el evento “Experiencias internacionales en políticas para la adopción del protocolo de interconectividad de redes IPv6 aplicadas al caso colombiano”.

En el año 2011, Mintic por medio de la suscripción de convenios con la U. Nacional y Renata, se articula un documento de estudio como insumo para realizar el proyecto, del cual se logró lo siguiente:

- Plan de promoción y divulgación
- Circular 002 del 6 de julio de 2011 “Promoción de la adopción”
- Lineamiento del Manual GEL 3.0

Para el mismo año participaron en algunos eventos de divulgación y sensibilización IPV6:

- “I Foro día mundial de IPV6, Capítulo Colombia”
- “II Seminario sobre Promoción y Divulgación de Políticas para la Adopción de IPV6”
- 12 mesas sectoriales.

De manera continua Mintic siguió trabajando con gran constancia con el fin de finalizar la resolución, para el año 2012 mediante contrato suscrito con Cintel, se logran elaborar los siguientes documentos:

- Políticas de adopción de IPv6 y desarrollo normativo.
- Lineamientos del Manual GEL 3.1
- Actividades transversales.
- Plan de Acción 2012 - 2014 Vive Digital.
- Abordaje del plan técnico de transición

En el mismo año Mintic en eventos y sensibilizaciones.

- “Semana Regional de IPV6”
- “Evento Ciudadanía & e-Gobierno”
- II foro día mundial de IPV6, Capítulo Colombia.

Realizaron un acompañamiento a diferentes entidades del estado por medio de la estructuración y entrega de proyectos de diagnóstico para adopción de IPV6, esto en casi 40 entidades y procesos de capacitación e inicia el micrositio www.mintic.gov.co/ipv6. Después de ser partícipes en todo el proceso de IPV6 y su llegada a Colombia, continúan con la formulación del borrador de las políticas por medio de la resolución de migración, al igual la asesoría a 27 entidades esto para el año 2014.

Mismo año en el que se generan sensibilizaciones y capacitaciones sobre el protocolo de internet en su sexta versión, al personal de las oficinas de TI del Mintic,

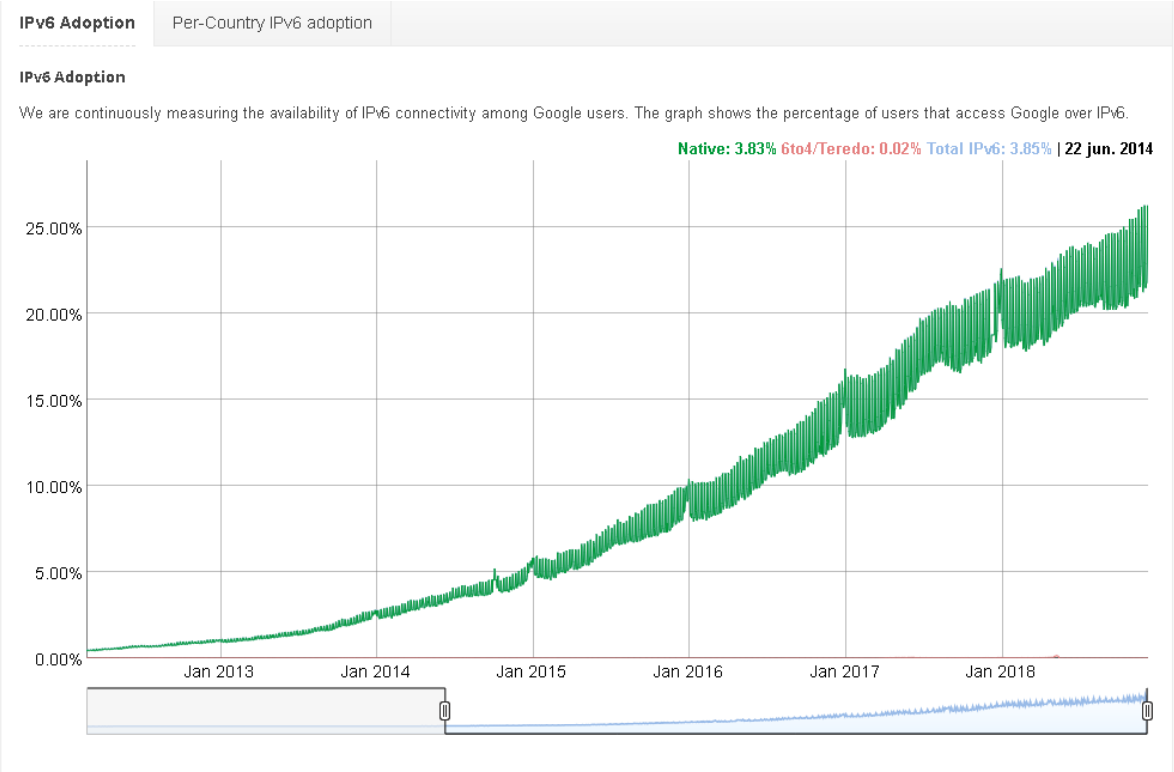
el mismo modo de estructura el plan de diagnóstico para la adopción de IPV6 en MinTic con un 92% de compatibilidad con el apoyo de Renata.

En el año 2014, EL Ministerio de Tecnología de la Información y Comunicaciones, aseguro que el 92.13% de su infraestructura tiene compatibilidad con el protocolo IPV6, por otra parte, ha impulsado grandes procesos en la industria, procesos de transición, gestionando acompañamientos que orienten y generen diagnósticos sobre las infraestructuras TI en relación con el protocolo IP en su sexta versión.

Figura 10:Adoptando IPv6

Actualmente no se conoce con exactitud la cantidad de usuarios que usan IPV6. Sin embargo, Google afirma que desde el año 2012, la adopción de IPV6 ha incrementado en más de 165%.

Figura 11: Estado de IPv6 en el mundo



Según LACNIC, la organización no gubernamental internacional encargada de la asignación y el proceso de gestión de aquellos recursos de numeración de la red (IPV4, IPV6), número autónomos y resolución inversa para la región, las siguientes son las empresas que están implementando IPv6 en América Latina y Caribe.
A continuación, se presenta algunas descripciones dadas por empresas que ya realizaron la migración.

(La siguiente información es tomada de la página oficial de LACNIC)

Tabla 2: Datos LANIC

América Latina y Caribe	
Empresa	Descripción
Level3	Esta entidad posee IPV6 nativo instalado en sus redes de backbone tanto en servicio públicos como privados, siendo así el único proveedor de telecomunicaciones que cuenta con estas características. Han brindado este servicio a más de 40 clientes, en algunos casos han mezclado ambos protocolos (IPV4 – IPV6) dentro de una misma VPN
IFX Networks	Tiene desplegado IPV6 en clientes de USA, Argentina, Colombia, Brasil, Perú, Ecuador, Chile, Uruguay. El despliegue IFX de IPV6 para MPLS/VPN se encuentra en proceso finalización de la implementación por medio del uso 6VPE.
ARGENTINA	
BAEHOST (InTerBS SRL)	La entidad implementó IPV6 de manera nativa para el año 2014, su medio de propagación fue por nap nacional de Argentina y proveedores internacionales.

BT Latinoamérica	Su red MPLS cuenta con un soporte IPV6 desde inició del 2007 utilizando el “feature” 6PE. Dicho elemento permite a los enrutadores de borde operar en el modo “dua-stack” soportando ambos protocolos de manera simultánea, además incorpora nuevas funcionalidades en los planos de envío y control para el transporte de paquetes IPV6 en una red MPLS.
Cooperativa Telefónica de Villa Gobernador Gálvez Limitada (TelVGG)	Cuentan con IPV6 implementado en su backbone y las zonas desmilitarizadas de las granjas de servidores. Están en la capacidad para la asignación de prefijos /48 a sus respectivos clientes xDSL por medio de PPPoE y a usuarios de líneas dedicadas por medio de metro ethernet.
GESATEL	Desde que obtuvimos la membresía en LACNIC, nos comprometimos en el estudio, desarrollo y despliegue de IPV6 en la operación. Los desafíos fueron varios y uno de los mayores ha sido interconectar y levantar los enlaces IPV6 con nuestros provedores-carriers; también descubrimos que muchos sitios web no soportan IPV6, por lo que fuimos monitoreando el paulatino despliegue de las CDN´s (proveedores de contenido) a la par que nosotros realizábamos lo nuestro en el mismo campo.

Honorable Cámara de Diputados de la Nación	Para inicios del año 2014, comenzó su proceso de implementación IPV6 en su red interna, finalizando el 2015 quedo implementado completamente el protocolo IP en se sexta versión, su evolución continua y en el año 2017, contratan el vínculo principal a internet por medio de bloques IPV4 e IPV6, bloques provistos por el ISP Claro Argentina. Adquirieron LANIC un Sistema Autónomo con un bloque /24 IPV4 y así también un bloque. /48 IPV6.
Telecentro S.A.	Su implementación de IPV6 va de punto a punto en toda la infraestructura de red. Conexiones con Upstream Providers y con todas las CDN's son nativas en Dual-Stack. Por medio del modelo 6VPE el CORE MPLS transporta de manera transparente IPV6. Las conexiones a IPV6 están habilitadas en todos los puntos de red para usuarios externos, así como para los clientes corporativos. Su despliegue se logró con satisfacción, ya que realizaron un arduo trabajo de investigación, evidenciando incidencias con pruebas y buscando la manera más factible de la integración con el sistema de provisioning (incluidos servidores DHCP, DNS, etc.). Se logra así una transición e implementación al 100%, totalmente transparente para el usuario final.
BRASIL	

Americana Digital	El protocolo IPV6 está en funcionamiento desde el Core de la red, hasta los clientes de manera nativa. Apoya y participa en proyectos cuyo fin es promover el uso de IPV6.
NipCable do Brasil Telecom LTDA	Operadora brasileña que posee un tránsito IPV6 en toda su red, cuentan con un sitio Web que provee una conexión doble pila, y brindan sus servicios con implantación de IPV6 Nativo en sus redes a más de 10 clientes.
CHILE	
Cable Color	El IPV6 está habilitado con Internexa de Upstream publicando el bloque 28:03: a100: :/32 asignado por LACNIC Sus equipos están configurados con DualStack lo que permite que el transito fluye a sus clientes en IPV4 e IPV6 simultáneamente.

GTD	Su IPV6 está habilitada con sus Upstream Provider Global Crossing, Sprint y Telecom Italia, para los cuales anunciaron un bloque 200:160: :/32 el cual fue asignado por LACNIC, también se asignaron bloques a otros clientes permitiendo tránsito a sus redes IPV4/IPV6. Su equipo de CORE, acceso y distribución están configurados de tal forma que permitiendo que a sus clientes tengan una entrega hacia internet IPV4 al igual que IPV6, también han ofrecido a sus clientes la posibilidad de monitorear su conectividad IPV6 con herramientas propias.

Universidad Técnica Federico Santa María (UTFSM)	Desde enero del 2009 tienen en funcionamiento IPV6 de manera dual. Su red cuneta con una red de prefijo /32, la cual delegada directamente por LANIC. La universidad requiere debido a sus carreras que cada área de trabajo cuente con IPV6 nativo y no solo en la casa central, sus planes son actualizar las secciones necesarias para brindar conectividad IPV6 a todas las sedes y campus de la Universidad.

NIC Chile	Para inicio del 2006, NIC realizo las pruebas de conectividad IPV6, desde entonces estaba de manera experimental, esta fase tomo dos años y desde el 2008 ya cuentan con IPV6 nativo. En la actualidad cuenta con conectividad IPV6 en producción, han participado en el proyecto “Google Over IPV6” desde el año 2009.
COSTA RICA	
COOPEALFARORUIZ R.L.	Se encuentran generando tráfico IPV6 a clientes residenciales, cuenta con un CORE netamente IPV6, así como su sitio web. En temas de aprovisionamiento cuentan con DNS en IPV4 y también en IPV6, su borde labora en Double Stack.
COLOMBIA	

Empresa de Recursos Tecnológicos E.R.T E.S. P	Cuentan con IPV6 con el prefijo IPV6:2800:9F0: :/32, anunciando Internet por medio del AS 27845. Para los suscriptores de conectividad con E.R.T está disponible por medio dual stack.
Telmex Colombia (Claro Fijo)	Con el rango 2800:480::32 (AS 14080), tienen implementado y operativo IPV6. Su CORE tiene la capacidad de soportar dual-stack con 6PVE.
UNE EPM Telecomunicaciones S.A.	Toda su infraestructura de enrutamiento cuenta con IPV6 dual stack, al igual que en los enlaces de interconexión locales e internacionales. Siguen trabajando en el despliegue de IPV6 en el servicio de banda ancha en las tecnologías ADLS, CM y PON
Universidad del Atlántico (UA)	Los servicios DNS, configuración de Firewall, Web, configuración de servidores cuentan con IPV6, soportándose con Claro Colombia para las conexiones a Internet.

HV Televisión SAS	Han publicado bloques IPV6 por medio de BGP con la ayuda de sus proveedores. Sus servidores DNS resuelven IPV6, así como su página Web. Hay una fracción de la red LAN funcionando con IPV6, contando con la posibilidad de ofrecer a sus clientes direccionamiento IPV6
Ministerio de Tecnologías de la Información y las Comunicaciones	Mintic para el año 2015 adjudico el proceso por el cual lograron adoptar IPV6 con éxito en la infraestructura de los servicios TI de la entidad, sus servicios funcionan bajo IPV6. Su segmento asignado por LANIC fue 2801:11:4000/48.

(La siguiente información es tomada de la página oficial de LANIC)

7 RAZONES PARA REALIZAR LA MIGRACIÓN HACIA EL PROTOCOLO IPV6

A lo largo de este escrito se ha mencionado que el protocolo IPV4 está siendo afectado por falencias que perjudican de forma notable la red de cualquier entidad, ya que en términos técnicos el sistema de direccionamiento es insuficiente para acobijar toda la gran cantidad de equipos que en la actualidad se encuentran conectados a la misma red. La demanda de direcciones IP no podrá tener una respuesta oportuna por parte de la versión actual del protocolo IP, adicionalmente se encuentran tablas de enrutamiento demasiado grande por la considerable cantidad de IP's sin poseer una autoconfiguración.

Por otra parte, al revisar esta situación desde un punto de vista social, se logra identificar que la necesidad de conexión a Internet por parte de los usuarios se ha incrementado exponencialmente, exigiendo que la cuarta versión del protocolo IP cumpla funciones que se encuentran fuera de su alcance. Este hecho es generado por que el protocolo IPV4 no proporciona capacidades como la privacidad, servicios de multimedia, la seguridad o atención a aplicaciones de gran demanda.

Esta transición empezó a tomarse en consideración cuando se identifica que el protocolo IP en su cuarta versión implementado para principio del año 1983, no prometía satisfacer la demanda de solicitudes realizadas por los hosts que para el año posterior a su implementación había incrementado de manera exponencial. Si nos referimos la presente, existe una cantidad inimaginable de host fijos registrados de DNS, y un número que aún sigue creciendo de host asignados dinámicamente.

El protocolo IPV6 como se ha mencionado con anterioridad cuenta con un amplio y flexible rango de direcciones IP, permite que se logre una habilitación en lo que refiere a las arquitecturas de ruteo flexibles, globales, jerárquicas, arquitecturas que posean varios niveles. Pero estos cambios y la implementación de este nuevo protocolo no solo benefician al usuario final, los ISP (Proveedores de Servicio de Internet), tendrán la capacidad elevada de asignación de direcciones IP a sus respectivos clientes, con el fin de ofrecer un servicio de Internet que los usuarios puedan explotar al máximo.

Cuando se habla de aspectos importantes que destacan del protocolo IP en su sexta versión, se hace referencia entre muchas cosas a la autoconfiguración sin intervención de servidores, esto permite que la conexión automática de cualquier dispositivo sea una tarea sencilla, IPV6 garantiza la adaptarse a las nuevas tendencias de movilidad que actualmente encontramos en dispositivos tecnológicos. Nos encontramos en una era donde los servicios se están diseñando con el fin de impedir que el humano se desplace sin poder llevar consigo su elemento tecnológico, ya que aun en casos donde la persona tenga que desplazarse de un lugar a otro y requiera conectividad, esta deberá estar disponible con servicios

mejorados y que no requieran un cableado, y a diferencia de IPV4, el nuevo protocolo IP ofrece una propiedad de movilidad mucho más eficiente.

Los diseñadores de IPV6, se concentraron en solventar las falencias que IPV4 fue mostrando con el pasar del tiempo desde su origen, esto influyo para el intento de mejorar la forma en la que los datos se codifican para así construir la cabecera del nuevo protocolo, por ende, la mejora de la red. La cabecera del protocolo IPV6 ha sido simplificada, al igual que se le han asignado nuevas funcionalidades, como ejemplo la identificación de flujos, que permite que los mecanismos de calidad de servicio de Internet tengan mejores operaciones.

En la creación de IPV6 se incluyó un multicast, un soporte mejorado de multidifusión, esta característica embebida en el protocolo es primordial para el uso de redes de banda ancha para la distribución de contenidos. Como se ha podido identificar la extensibilidad que busca el protocolo IPV6 es infinita, el diseño de este protocolo está en la obligación de permitir la extensión de internet sin intervenciones o errores que se evidenciaron en su antecesor, por eso el trabajo a cumplir del protocolo IPV6 es permitir la incorporación de nuevas características o piezas de protocolo, sin la necesidad de realizar una actualización general en todos los dispositivos que se encuentra conectados la red. Se cuenta con una libertad de actualizaciones para aplicar al igual solo en los equipos que necesiten una determinada extensión.

A continuación, se presenta una tabla en la que de manera resumida se pretende hacer énfasis en algunas de las diferencias entre IPV4 e IPV6.

Tabla 3: IPV4 VS IPV6

Característica	IPV4	IPV6
Tamaño de las direcciones y tamaño de la red	32 bits Network size 8-30 bits	128 bits Network size 64 bits
Tamaño paquete de cabecera	Opciones limitadas por un pequeño número de IP	Numero de IPV6 ilimitado extensiones de cabecera
Fragmentación	El remitente o cualquier enrutador intermedio permitido para fragmentar	Solo el remitente puede fragmentar
Protocolo de control	Mezcla de non-IP (ARP). ICMP, y otros protocolos	Todos los protocolos de control se basan en ICMPV6
Mínimo permitido de MTU	576 bytes	1280 bytes
Path MTU Discovery	Opcional, generalmente no usada	Fuertemente recomendada

Tipos de direcciones	Uso de unicast, multicast, y broadcast para el tipo de direccionamiento	El direccionamiento broadcast no usado, uso de unicast, multicast y anycast para los tipos de direcciones
Asignación de direcciones	Uso de una dirección por Host	Uso de múltiples direcciones por interfaz
Configuración de direcciones	La configuración es manual o con host de configuración como el protocolo DHCP	Los dispositivos se configurar de forma independiente con el uso de direcciones con autoconfiguración o el uso de DHCP

8 SEGURIDAD EN IPV6

La posibilidad de implementar el modelo de seguridad IPsec (Internet Protocol Security), permite que la red cuente con un refuerzo que proporciona integridad, autenticidad y confidencialidad al proceso de comunicación de extremo a extremo. La arquitectura extensible del protocolo IP en su sexta versión, permite una implementación natural del protocolo IPsec.

IPsec formado por un conjunto de protocolos abiertos, proporciona seguridad en las transferencias de información en el protocolo OSI, al igual que a los protocolos de capas superiores, esta suite de protocolos permite la autenticación y autenticación mediante criptografía simétrica o asimétrica de un flujo de dato, entre los servicios ofrecidos se encuentran el control de acceso, integridad sin conexión, detección y rebote de repeticiones, autenticación de comienzo de datos, ofrece la confidencialidad de flujo de tráfico limitado o por medio de cifrado. IPsec ofrece protección para aquellos protocolos que sean transportados por medio de IP, gracias a la efectividad proporcionada en la capa 3.

Así podemos destacar características importantes:

- Es un protocolo centrado en el cifrado y autenticación IP, que hace parte de los componentes de IPV6. Su uso en la sexta versión del protocolo IP es una obligación, esto asegura las comunicaciones entre enrutadores BGP (Boundary Gateway Protocol).
- Al ser u conjunto de servicios embebido en IPV6, permite controlar aspectos como acceso, la confidencialidad de la información, así como su integridad y la autenticación desde el origen de los datos.
- Un ejemplo claro de escenario donde Ipsec puede ofrecer servicios es OSPFv3 (Open Shortest Firts Path), que implementa en su operatividad AH. Así como en túneles donde existe la posibilidad de configurar IPsec en medio de túneles.

8.1 ESTRUCTURA DEL PROTOCOLO IPSEC

8.1.1 Autenticación AH

Ofrece seguridad cubriendo aspectos como la protección contra duplicados de información, autenticación del origen, así como su integridad, AH brinda protección a la mayoría de las zonas de encabezado IPV6, a excepción de los que en el enrutamiento lleguen a sufrir cambios. Esta autenticación se realiza por medio de un algoritmo de cifrado.

8.2 RFC DE SEGURIDAD

Revisión del RFC 4942, que hace énfasis en aquellas consideraciones de seguridad para la coexistencia y migración hacia IPV6. Revisión del RFC 6177, allí se encuentran especificaciones de carácter técnico, que se enfocan en las recomendaciones a seguir para la solicitud de asignación segmentos de IPV6 en rango /48 a /56.

La oportuna revisión de cada procedimiento de RFC de seguridad que contribuye a la implementación de software de aplicativos, redes, dispositivos móviles, sistemas y herramientas de cifrado, equipos que permitan comunicación, entre otros. Para RFC de seguridad, es recomendable la correcta clasificación de los activos pertenecientes a la entidad que inicie el proceso de transición, con la estructura de una matriz de riesgo que logre establecer los niveles de seguridad.

8.3 VPNS

Para las entidades que cuenten con conexiones privadas virtuales punto a punto, las que permiten la comunicación de dos o más redes LAN, es aconsejable que se tenga en cuenta todo el control de tráfico entre todos los puntos posible de la red IPV6, en conclusión, IPV6 y su tráfico acceden por gran cantidad de recursos que se encuentren compartidos, en una red que cubre gran área. Por tal motivo, es imprescindible utilizar IPsec para que se encargue de la seguridad de todo el tráfico generado por las comunicaciones entre VPNs.

8.4 MONITOREO DEL PROTOCOLO IPV6

El monitoreo es necesario tanto en la fase de pruebas o finalización de la implementación como en el establecimiento de los niveles de funcionamiento y criticidad de la red con IPV6 en su servicio activo. Para ello es requisito la prevención de aquellos problemas que se puedan presentar, así como la detección y diagnóstico de fallas, para este proceso es necesario también tener en cuenta la determinación de acciones para solventar incidencias de seguridad y generar plan de contingencia al alcance de la mano.

Cuando se procede a realizar el monitoreo de los servicios de red que cuentan con IPV6, es necesario tener claridad sobre unos ítems relacionados a continuación:

- El estado en el que se encuentran las aplicaciones, así como el estado de los servicios activos.
- La correcta medición de los dispositivos conectados a la red y sobre las interfaces.
- Los canales disponibles para la comunicación a Internet y la actividad de cada Host que interviene en la comunicación.

Contar con herramientas precisas y eficientes de monitoreo permite que este proceso se realice con una mayor precisión. Herramientas que permitan analizar el tráfico de la red con IPV6 que generen graficas de análisis de las interfaces de red, que estudien el comportamiento de las librerías IPV6. Como nota importarte, se menciona y se hace énfasis en que casa entidad durante todo el proceso de transición, es necesario que desarrollen la capacidad de implementación de herramientas encargadas del monitoreo, siendo libres en escoger la herramienta que consideren pero que cumpla con los requerido y genere los resultados correctos.

8.5 SEGURIDAD EN LOS CENTROS DE DATOS CON RED IPV6

Para una entidad, es necesario resguardas la seguridad de los centros de datos, ya que cumple la función de ser la columna vertebral de los procesos tecnológicos de las empresas, por ende, podemos destacar lo siguiente:

- IPV4 en el borde, toda la infraestructura del centro se encuentra operando con IPV4, y se inician traslados en el borde hacia IPV6.
- Pila Doble: En este punto se encuentra operando la pila doble, de acuerdo a las necesidades de la entidad, la cual puede definir en qué sectores de la infraestructura se hace preciso el funcionamiento de la pila doble.
- IPV6, finalizando el proceso de transición, en este punto el centro de datos deberá estar funcionando con IPV6.

Los ítems descritos anteriormente, no se relacionan con el fin de seguir una secuencialidad, ya que la entidad es libre de elegir que camino toma para la operabilidad del centro de datos, los escenarios descritos ofrecen diferentes beneficios que la entidad está en la obligación de analizar para elegir el más apropiado para su infraestructura.

8.6 IPV6 Y SUS PILARES DE SEGURIDAD DE LOS DATOS

8.6.1 Integridad

En IPV6, la integridad hace énfasis en la relación entre cabecera de autenticación y el encapsulado de seguridad de la carga útil (ESP), con la integridad de la información, garantizando que los datos viajen seguros por medio de la red con las propiedades de IPV6.El AH en el interior de la composición de lo que ofrece IPV6, implementa una llave de autenticación la cual le permite generar autenticidad, así como integridad la cual está cifrada en los datagramas de IPV6.

En la fórmula para el cálculo de la autenticidad, son necesarios la clave de nodo origen y salida, característica que no es predeterminada en todos los algoritmos de

autenticación que se lleguen a utilizar en el AH de IPV6.El esquema de seguridad del protocolo, actúa en el momento en el que el nodo de origen interpreta la información para validar su autenticidad, proceso realizado antes del envió de la información cifrada. Este paquete viaja por la red IPV6 y el nodo que está dispuesto a recibir, procede a una revisión.

8.6.2 Disponibilidad

La disponibilidad debe brindar a los usuarios la garantía de encontrar a disposición la información cuando sea necesario acceder a ella, bajo una autorización, la disponibilidad se concentra en el acceso de aplicaciones, personas o procesos, a los datos cuando estos sean requeridos.

8.6.3 Confidencialidad

IPsec cuenta con dos herramientas que refuerza la seguridad de IPV6, el ESP encapsulado de carga útil, encargado de proporcionar confidencialidad mediante un método de cifrado de datos. También IPsec, cuenta con la cabecera de autenticación conocida también como AH, que cumple la función de proporcionar autenticidad de la información. El ESP, generalmente tiene la capacidad de implementar un algoritmo de cifrado, delegado para proporcionar más seguridad en la gestión de la información.

***Modo transporte**:* En este modo, solo se realiza la carga útil o los datos que se transfieren del paquete IP, por otra parte, el enrutamiento permaneces intacto ya que no sufre modificaciones ni se cifra la cabecera IP. Al usar la cabecera de autenticación, la IP no pueden ser traducidas ya que esta acción invalidaría el hash. El modo de transporte es usado para las comunicaciones punto a punto sobre cualquier host y sobre un canal inseguro.

***Modo túnel**:* Todo el paquete IP es cifrado y autenticado, para su correcto funcionamiento este deberá ser encapsulado en un nuevo paquete. Este modo es utilizado para comunicaciones red a red. Su propósito es establecer sobre canales inseguros una comunicación entre dos redes remotas.

8.6.4 Privacidad

La privacidad y la autentificación son el par de esquemas que se pueden combinar para que, al momento del viaje de los paquetes, la trasmisión se realice con seguridad, esto acompañado del planteamiento de categorías de privacidad en los protocolos IPV4 e IPV6.

- El procedimiento del cifrado antes de que se genere la autenticación se presenta cuando la información viaja y es autenticado en su totalidad, no sin antes pasar por un esquema de cifrado desde el origen hasta la entrega. El

proceso se lleva a cabo inicialmente cuando se aplica ESP a la cantidad de datos a proteger y que serán transportados, finalmente se agrega el texto prístino al inicio de la cabecera de autenticación IP.

- La autenticación antes de que se genere el cifrado, se presenta al momento del encapsulamiento de la cabecera de autentificación en el interior del paquete IP ubicado de manera interna. Dicho elemento se protege con un esquema de privacidad, técnica recomendada solo para ESP en la modalidad llamada túnel.

Cuando nos referimos a la seguridad en relación al proceso de transición, es importante hacer mención sobre los servicios que serán afectados por en cuestión de seguridad por el plan de implementación IPV6:

- Video conferencias.
- Servicios proxy.
- Directorio activo
- Aplicaciones y base de datos.
- Correo electrónico.
- Telefonía IP
- DNS
- Dominio de red.
- Canal de comunicación de Internet.
- DHCP
- Mensajería instantánea.
- Servicio Web y accesos a Internet
- Dispositivos de seguridad, entre ellos encontramos:
    - NAC (Network Access Control)
    - Firewalls
    - Servitors AAA (Authentication. Authorization and Accounting)
- Equipos de comunicación fijo y portables.

8.7 ANÁLISIS DE RIESGO

Gestionar el riesgo, le permite a una empresa identificar, evaluar y guiar en la toma de acciones sobre cualquier eventualidad que se presente, optando por reducción de las amenazas que se puedan manifestar. La necesidad de poseer información que permita examinar riesgos para tomar decisiones y la mitigación de los impactos que puedan afectar los activos de la entidad, son de los muchos argumentos que se deben tener en cuenta, para hacer efectivo un plan de gestión de riesgo de los activos informáticos.

Tabla 4:Valoración de activos de información (Mintic)

Activos	Confidencialidad	Integridad	Disponibilidad
Aplicaciones – BD			
Equipos de comunicaciones			
Equipos de cómputo y de almacenamiento			

Tabla 5: Gestión del riesgo para el proceso de migración (Mintic)

Fases de transición IPV4 – IPV6	Propiedades de la fase	Actividades gestión de riesgo
Planeación		
Implementación		
Pruebas		

Tabla 6: Hacking Ético (Mintic)

IPV6 en relación a:	Servicios	Direccionamiento Web
Portales Web		
Equipos de comunicaciones		
Servidores y aplicaciones		
Equipos de almacenamiento		
Otros		

En relación con la tabla anterior, es importante tener presente una serie de consideraciones cuando se deba iniciar un proceso de pruebas de penetración a IPV6.

- Obtención de datos
- Identificación de la red empresarial
- Sumario pasivo
- Recopilación de información pública de libre acceso
- Identificación de nombres de dominio.
- Sumario activo
- Identificación de red
- Mapeo de la infraestructura (red)

- Búsqueda de servicios activos
- Identificación de puertos
- Comprobación de puertos

8.8 SEGURIDAD EN LA NUBE CON IPV6

Cuando se trabaja con la seguridad en la nube, ya sea en el protocolo IPV4 o IPV6, se debe organizar estrategias que involucran aspectos físicos y lógicos, basados en esto, las entidades estarán en la obligación de crear políticas de seguridad que se adapten a las necesidades y que abarquen los aspectos relevantes que puedan poner en riesgo la seguridad de los datos, y el equipo de trabajo deberá estar en la capacidad de aplicarlas de manera correcta sin alteraciones y que logren la correcta administración sobre la infraestructura.

Recomendaciones para reforzar la seguridad de dato antes de subirlos a la nube:

- Se debe verificar que las condiciones ofrecidas por el proveedor sean óptimas2 para preservar la seguridad de la información, y dejar evidencia de que el servicio posee la calidad esperada y requerida.
- En las políticas de la entidad, deberá existir un apartado en el que se indique que información es posible alojar en la nube y que información se debe restringir.
- Criticidad de la información.
- Se debe garantizar que la seguridad en la nube abarque las capas de funcionamiento en la nube:
    - Capa de infraestructura.
    - Capa de almacenamiento
    - Capa de gestión de infraestructura
    - Capa de aplicación
    - Capa de servicio.

8.9 MITIGACIÓN DE RIESGOS EN IPV6

En el proceso de migración, el cual se debe realizar por fases, es fundamental que se identifiquen los riesgos en especial en la fase de implementación, para que el proceso no sufra impactos por posibles amenazas que afecten la seguridad, por tal motivo se realizan recomendaciones a tener en cuenta:

- Cuando se procede a configurar la doble pila, se evidencia que un dispositivo posee la capacidad de soportar el protocolo IPV4 y el protocolo IPV6, pero las reglas que se aplican en lo elementos encargados de la seguridad y el tráfico indeseado para IPV4, no funciona de igual forma para IPV6, por lo

cual las entidades deberán adoptar por implementar estrategias que permitan controlas este tipo de situaciones.

- Una de las recomendaciones que también sugiere el Ministerio de Tecnologías de la Información y la Comunicación (Mintic), es la deshabilitación de los protocolos de red que no se encuentran en uso. En la mayoría de los casos, el nuevo Hardware tiene el servicio IPV6 activado por defecto, sin embargo, es necesario suspenderlo cuando se identifiquen problemas en el Core de la red, que puedan causar problemas en las operaciones y la infraestructura de la entidad.
- Entre las políticas de seguridad, se deberá plantear un apartado que haga énfasis en el apagado de equipos, cuando se presente dispositivos que tengan la capacidad de asediar tráfico que implemente IPV4 sobre las redes Wifi de la organización.
- Al momento de la implementación y después de ella, se pueden presentar sucesos que dejan en evidencias vulnerabilidades como:
    - Problemáticas con la activación, a causa de despliegue de condigo de algún programa en la capacidad de usar el protocolo para realzar ataques.
    - Los ISP y la utilización de CGN (Carrier Grade Nat), que transmite a los usuarios intranquilidad o falsa seguridad, situación que puede complicar el desarrollo de técnicas NAT sobre la red, esto debido al hecho del uso de ambas versiones del protocolo IP sin tener el cuidado en el firewall.

8.10 RFC SEGURIDAD IPV6

A continuación, se relaciona la lista de RFC que son aplicables a la seguridad en relación con el protocolo IPV6:

- RFC 4718: IKEv2 Clarifications and implementation Guidelines
- RFC 2406: IP Encapsulating Security Payload (ESP)
- RFC 4807: IPsec Security Policy Database Configuration – MIB
- RFC 3414: User – Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 4982: Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGA).
- RFC 4581: Cryptographically Generated Addresses (CGA) extention field format.
- RFC 4877: Mobile IPV6 Operation with IKEv2 and the revised IPsec Architecture.
- RFC 5996: Internet Key Exchange (IKE V2) Protocol.
- RFC 5282: Using Authenticated Encryption Algorithms with the encrypted payload of the internet key Exchange version 2.
- RFC 4303: IP Encapsulation Security Payload.

- RFC 4302: IP Authentication Header
- RFC 2401: Security Architecture for the Internet Protocol
- REF 4301: Asociaciones de Seguridad.
- REF 3756 IPV6 Neighbor Discovery (ND) trust Models Threats
- RFC 4449: Securing Mobile IPV6 Route Optimization Using a Static Shared Key.
- REC 4487: Mobile IPV6 and Firewalls.
- RFC 4835: Cryptographic Algorithm Implementation
- RFC 4843: An IPV6 prefix for Overlay Routable Cryptographic Hash Identifiers.
- RFC 4864: Local Network Protection for IPV6
- RFC 4891: Using IPsec to secure IPV6 Tunnels
- RFC 4218: Threats Relating to IPV6 Multihoming Solutions
- RFC 4942: IPV6Trnsition/Coexistence Security Considerations
- RFC 5269: FMIP Security Distributing a Symmetric fast mobile IPV6
- RFC 5619: Software Security Consideration.

9 FASES PARA EL PROCESO DE TRANSICIÓN

9.1 FASE I, PLANEACIÓN

Iniciamos con el proceso de transición, lo cual deberá tener una cronograma y plan de trabajo que permita realizar la transición lo más transparente posible para el usuario final. En esta fase es necesario empezar con un inventario de activos de información, el resultado deberá ser consolidado con el plan de diagnóstico de la infraestructura de TI de la organización en cuestión.

Hay actividades necesarias a tener en cuenta en el desarrollo de esta fase:

- Es necesario realizar un inventario el cual será validado, identificando los elementos de información de servicios tecnológicos pertenecientes a las organizaciones que estén dispuestas a proceder con la transición y las relaciones encontradas con estos activos. Para el desarrollo de esta actividad se debe preparar dos inventarios, elegir uno para tomar datos del Hardware de la compañía y el otro debe dedicarse al software, esto permitirá la identificación de equipo y programas que soporten la tecnología IPV6, por ende, se identifican aquellos que su actualización es necesaria. Como nota adicional pero no poco importante, el trabajo del inventario deberá ser un proceso acompañado por los fabricantes de los dispositivos. Consiguiente se deberá desarrollar y ajustar un plan de diagnóstico del protocolo de IP en su sexta versión en la red de la compañía, basado en el resultado obtenido y establecido en el inventario de activos de información.
- Para preparar el diagnóstico es necesario la estructuración de la validación preliminar de la infraestructura tecnológica que conceda el permiso de medir el grado de avance en la adopción del nuevo protocolo. En esta validación se debe evidenciar que grado de compatibilidad existe entre IPV6 y la infraestructura TI soportada por la compañía.
- Se deberá proponer un nuevo diseño de red sobre IPV6 de acuerdo con el análisis de la topología de red que actualmente está implementada en la entidad.
- Proponer el plan detallado del proceso de transición hacia el nuevo protocolo basado en el plan de diagnóstico obtenido en puntos anteriores y la red.
- Formular planteamiento del cambio de los servicios descritos a continuación:
    - Servicio de Resolución de Nombres (DNS)
    - Servicio de Asignación Dinámica de Direcciones IP (DHCP)
    - Directorio Activo
    - Web Servicie
    - Servidores de monitoreo
    - Servicio de correo electrónico
    - Validación del servicio de la Central Telefónica
    - Sistemas ininterrumpidos de potencia

    - Backups
    - Servicio de ambiente colaborativo
- Validación de los sistemas actuales de la compañía, sistemas que permiten la gestión de información, comunicación, almacenamiento para finalmente evaluar comportamiento con la adopción del nuevo protocolo.
- Con el proceso de diagnóstico se identifican los equipos de computación y comunicación que logren soportar IPV6, cuales requieren actualización y cuales definitivamente no son óptimo para la implementación de este protocolo.
- Inspección de los esquemas que forman parte de la seguridad de la red de comunicación y sistemas de información.
- Las políticas para enrutar IPV6 entre segmentos de red internos, el propósito es que el tráfico IPV6 originado internamente sea controlado por medio de DMZ desde un cortafuego asignado a cada entidad. La recomendación es para la revisión de los RFC respecto a políticas de seguridad y enrutamiento IPV6.
- Deberá existir un protocolo para pruebas de validación de aplicativos, equipos de comunicación y de cómputo, coexistencia de IPV4-IPV6 y planes de seguridad.
- Realizar proceso metódico para la ejecución y configuración de las pruebas previas de nuevo protocolo instalado, la metodología implica la creación de VLAN. La VLAN deben incorporar múltiples dispositivos y servicios de misión crítica, que debe contemplar la funcionalidad del software, distinción del hardware en los diferentes elementos, revisión de los elementos en la red de comunicaciones, la conducta de estos elementos en la red de comunicaciones, el comportamiento en relación con los aplicativos de la entidad, análisis de los servicios ofrecidos e incremento de carga de tráfico sobre la VLAN. Estas pruebas deben realizar un trabajo mancomunado con mejores prácticas y metodologías de transición al nuevo protocolo preservando el criterio técnico Dual Stack. Si el resultado obtenido con la implementación de esta VLAN para la realización de pruebas es óptimo, lo siguiente será replicar esta red sobre la red completa de la organización, garantizando la correcta implementación y funcionamiento del nuevo protocolo sobre la red que soporta la entidad.
- Las pruebas para realizar deberán estar controladas por zona aislada y monitoreadas, con un segmento de red independiente alejado que permite configuraciones y activaciones necesarias que permiten confirmar la funcionalidad de IPV6, esto con el fin de no alterar las actividades de los usuarios mientras se ejecutan pruebas.
- Los acuerdos de confidencialidad son ineludibles, estos deberán hacer énfasis en el manejo y tratamiento de la información ante terceros cuando se decida realizar la transición.
- El equipo de trabajo del Área TI, deberá estar preparado bajo planes de capacitación establecidos por la entidad correspondiente para asimilar la

transición del protocolo IPV4 a IPV6. Las sensibilizaciones a todos los empleados son una estrategia fundamental para permitirles que conozcan y se familiaricen con el nuevo protocolo, dando a conocer el grado de impacto que tendrá la entidad con esta transición.

- La entidad que adopte el nuevo protocolo deberá realizar un proceso de sincronización con sus correspondientes proveedores de servicio, para definir el enrutamiento de IPV6 nativo.

9.1.1 Productos Entregables

Como resultado de esta fase, se deberán entregar lo siguiente:

- El plan que permite bajo una serie de eventos la adopción de IPV6 en la entidad.
- Un plan de diagnóstico conformado por ítems importantes que deberán estar incluidos:
    - Inventario diseñado para Hardware y Software de la entidad.
    - Documentación actualizada donde se relacionan los cumplimientos de IPV6 por los elementos correspondientes al Hardware y al Software.
    - Indicaciones y recomendaciones para adquirir documentos de cómputo, también de comunicaciones y finalmente el cumplimiento de IPV6 en relación a IPV6
    - Informe sobre las direcciones IPV6 bajo un plan de direccionamiento.
    - Estrategia para el manejo de excepciones, explicando las acciones necesarias en las diferentes situaciones de hardware y software que presente que sean en relación con la incompatibilidad con IPV6.
    - Informes sobre la preparación de sistemas de comunicaciones, bases de datos y aplicaciones.
    - Lineamientos de implementación IPV6, estas deberán tener acuerdo con las políticas de seguridad de información y los controles de la seguridad informática.
- Debe planificar capacitaciones sobre IPV6 a los funcionarios de las áreas correspondientes al manejo de TI de la organización.

9.2 FASE II, IMPLEMENTACIÓN

Para la fase de implementación, es necesario cumplir con las siguientes actividades.

- En la primera fase necesario realizar un plan de diagnóstico, construido con apoyo del inventario de los activos de información de la infraestructura de las entidades, y teniendo presente el diseño de la red bajo IPV6, también definido en la fase I, es necesario habilitar el direccionamiento IPV6 para todos los elementos (Hardware y Software).

- Iniciar ejecuciones de pruebas piloto con el nuevo protocolo (IPV6), tomando como base los ensayos realizados en cada sección de la red, así como en las VLANs creadas y configuradas, estas pruebas se realizarán con una población pequeña perteneciente a la entidad donde se realice el proceso de migración, la cual estará encargada de aprovechar la paridad de la red, apoyado con un servicio de filtrado, buscando la transparencia y el funcionamiento normal del servicio de red.
- Asumiendo que las entidades en el proceso de transición ya han construido un modelo de transición, en este punto se deberá aplicar, buscando que la cohabitación se tolere en las aplicaciones, infraestructura y servicios bajo el protocolo IPV4 y el protocolo IPV6, en modalidad de transición en doble pila.
- Diseñar una nueva topología de red que se base en los lineamientos del protocolo IP en su sexta versión bajo doble pila; una forma de que los servicios que funcionan con IPV4 y los servicios que operan con IPV6 funcionen con normalidad de manera separada pero su coexistencia sea un éxito en el interior de la compañía que decida realizar el proceso de migración.
- La funcionalidad en IPV6 de los servicios relacionados a continuación será validada:
    - Servicio de resolución de nombres
    - DHCP
    - Directorios activos
    - Web servicies
    - Servicios de Voz
    - Servidores de Monitoreo
    - Servicio de la central telefónica
    - TDT
    - Servicio de respaldo
    - VPN
    - Integración entre sistemas de información
    - Sistemas de almacenamiento
    - Servicio de administración de red
    - Sistemas en la nube
    - Sistema interrumpido de potencias.
- Iniciar las políticas de seguridad sobre IPV6, en equipos de seguridad y comunicación que posea cada entidad.
- Realizar un trabajo mancomunado con los ISPs para establecer un enrutamiento necesario del segmento de IPV6 y las conexiones integrales, este proceso deberá ser desde el interior de las redes LAN, hacia el exterior de las redes WAN garantizando que las entidades puedan generar tráfico IPV6 nativo ante internet.

9.2.1 Productos entregables

- Informe de un plan detallado de implementación del nuevo protocolo.
- Escrito que contenga las configuraciones del nuevo protocolo aplicadas en las plataformas de hardware, software y servicios que intervinieron en la fase II, se relaciona las configuraciones aplicadas a los canales de comunicaciones con acceso a internet.
- Documentación sobre las pruebas a nivel de comunicaciones, de aplicaciones y sistemas de almacenamiento.

9.3 FASE III, PRUEBAS DE FUNCIONALIDAD

En esta fase se deberá realizar las pruebas necesarias para comprobar la funcionalidad, estas pruebas deberán abarcar las actividades relacionadas a continuación:

- Ejecutar pruebas y realizar monitoreo para verificar la funcionalidad del protocolo IPV6 en sistemas de almacenamiento, sistemas de comunicaciones, sistemas de información, estas pruebas deberán ejecutarse en un entorno que genere tráfico de IPV6 desde el interior de las compañías hacia internet y viceversa.
- Ejecutar ejercicios de pruebas sobre la funcionalidad del protocolo IPV6 frente a las diversas políticas de seguridad establecidas por cada entidad.
- Afinar las configuraciones de Hardware, software y servicios de las entidades, basándose en los resultados obtenidos den la fase II.
- Realizar un inventario final de los aplicativos, que contenga también los sistemas de comunicación bajo el esquema del protocolo IPV6 y de los servicios.

9.3.1 Productos Entregables

- Cuando se apliquen cambios detallados de las configuraciones, se deberá dejar todos los cambios establecidos en documentación.
- Acta de cumplimiento con respecto al funcionamiento de los servicios y aplicaciones que sufrieron intervenciones durante la fase de la implementación.
- Documentación de inventario final sobre el nuevo protocolo IPV6.

10 REQUERIMIENTOS PARA EL PROCESO DE TRANSICIÓN

- Seguir a cabalidad las actividades de cada fase, cumpliendo con el proyecto donde se relacionan los pasos para la implementación en la infraestructura tecnológica perteneciente a la entidad interesada en la transición

- Garantizar que el servicio suministrado tenga altos estándares de calidad, y no deberá afectar las operaciones normales de cada entidad.
- Asegurar que el funcionamiento y la operatividad de los servicios se encuentre en óptimas condiciones.
- Seguimientos a cada fase del proceso de migración, aclarando que cada entidad que decida realizar la transición de IPV4 a IPV6, posee la responsabilidad del correcto desempeño y la funcionalidad de casa servicio activo.
- Cada entidad deber poner a disposición recurso humano idóneo, el cual será necesario para el desarrollo de las actividades de cada fase en de transición con la coordinación de las áreas TI de cada entidad.

11 CONCLUSIONES

En el presente escrito, se plantearon las fases (Planeación, Implementación, Pruebas de funcionalidad), en donde se mencionan las actividades que permiten orientar a las empresas en el proceso de transición hacia IPV6. En la fase de implementación el proceso de migración debe ser estructurado tomando como fuente las políticas de seguridad que establezca la entidad que busca la migración. Estas políticas forman la base, para que IPV6 contemple la confidencialidad, integridad y disponibilidad de la información.

La disposición de la infraestructura TI de las áreas de la entidad configuradas o administradas por Firewall y sus respectivos servicios segmentados afianzan la capacidad de IPV6 en los temas de conexión y seguridad en la que se inicie el tráfico por medio de este protocolo, que ofrece la garantía de una mayor posibilidad de conexiones gracias al incremento a 128 bits, esto apoyado mediante vías de direccionamiento disponibles en IPV6 (Anycast, Multicast, Unicast).En el estudio realizado, se identifica en IPV6 un notable mejoramiento en comparación a su antecesor en cuestión de la capacidad de autentificación y privacidad de los paquetes enviados y recibidos.

Es importante que los nombres de los servicios que operan con IPV4 se mantengan iguales al momento de realizar la transición y el tráfico de red se enrute por IPV6. Esta recomendación tiene como fin la transparencia en la resolución de nombres de dominio para ambos protocolos y al igual que en el protocolo IPV. En IPV6 es aconsejable no usar direcciones literales, esto en el caso de librerías y en el desarrollo de aplicaciones. Otra recomendación importante para preservar la seguridad de la información es la verificación de las segmentaciones de los bloques IPV6, cuando estos se han configurado por zonas DMZ (Zonas desmilitarizadas), la base es lo requerido por cada entidad, quienes establecen sus respectivos niveles y/o criterios de seguridad.

Dentro del análisis expuesto, se ha evidenciado que en el proceso de migración se pueden generar riesgos que afectan la seguridad de los datos, por tal motivo en cada fase planteada es necesario análisis las variantes que lleguen a desencadenar vulnerabilidades ya que IPV6 no es un protocolo que opere de forma independiente, por el contrario, es apoyado por otros servicios como Ipsec, SIP, TCP, UDP, entre otros. Desarrollar un plan de contingencia permite garantizar disponibilidad a todos los usuarios si en algún momento se presentan inconvenientes que atenten contra la seguridad de la información.

Finalmente se ha generado un documento, donde se relacionan los parámetros necesarios para que IPV6 opere con normalidad en una infraestructura TI que cuenta con IPV4 para esto es importante la revisión del nivel de impacto de aplicativos en funcionamiento o servicios tale como DNS, el sistema de correo

electrónico, el servicio DHCP, directorio activo, el sistema Proxy, Sistemas de monitoreo y sistemas de gestión.

BIBLIOGRAFÍA

[1] AHUATZIN SANCHEZ, Gerardo. *Capitulo I. Panorama actual del cambio de IPV4 a IPV6.* [En Línea]. Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo1.pdf

[2] ALONSO, Juan. *Agotamiento del espacio Ipv4.* [En Línea]. Disponible en: http://www.eslared.org.ve/walc2012/material/track2/03-Agotamiento.pdf

[3] BEJARANO RAMIREZ, Ana. MIRANDA CASTILLA, Diego. HENRIQUEZ CELEDON, Javier. [En Línea]. Venezuela. Disponible en: https://www.urbe.edu/info-consultas/web-profesor/12697883/articulos/Redes%20Informaticas/IPv4%20Vs%20IPv6.pdf

[4] CASTILLO, Yarisol. *Agotamiento de IPv4 en la región latinoamericana*. [En Línea]. Panamá. Disponible en: http://www.utp.ac.pa/documentos/2015/pdf/07-ACTUALIDAD_TECNOL._AGOTAMIENTO_26-28_0.pdf

[5] CCOYLLO, Ingrid. *Enrutamiento IPv6 - con el software Packet Tracer.* [En Línea]. Disponible en: https://informatica.ucm.es/data/cont/media/www/pag-66886/Presentacion%20Enrutamiento%20IPv6.pdf

[6]comparación, ventajas, problemas y una metodología para la transición de IPv4 a Ipv6 en las redes de comunicaciones. [En línea]. Bogotá. Disponible en: http://ciruelo.uninorte.edu.co/pdf/ingenieria_desarrollo/3_4/comparacion_ventajas_problemas_y_una_metodologia_para_la_transicion.pdf

[7] CORREA, Adelaida. CANDAMIL, Martha. *MECANISMOS DE TRANSICIÓN DE IPV4 A IPV6.* [En Línea]. Bogotá. Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/8797/MONOGRAFIA%20MECANISMOS%20DE%20TRANSICI%C3%93N%20DE%20IPV4%20A%20IPV6.pdf?sequence=1&isAllowed=y

[8] CORREA, Adelaida. Candamil, Martha. Mecanismo de transición Ipv4 a Ipv6. [En Línea]. Bogotá. Disponible en: https://repository.unilibre.edu.co/bitstream/handle/10901/8797/MONOGRAFIA%20MECANISMOS%20DE%20TRANSICI%C3%93N%20DE%20IPV4%20A%20IPV6.pdf?sequence=1

[9] *Direccionamiento ipv4,* [En Línea], Disponible en: https://juannava64.files.wordpress.com/2012/02/redes-direccionamiento-ipv4.pdf

[10] DOMINGUEZ, José. *Introducción a IPv6.* [En Línea]. Oregón. Disponible en: http://ws.edu.isoc.org/data/2004/1797176210448267ca02e17/IPv6.pdf

[11] FONSECA, Diana. *PLAN DE TRANSICIÓN DEL PROTOCOLO DE RED IPv4 A IPv6 BASADO EN LAS RECOMENDACIONES REALIZADAS POR EL MIN TIC COLOMBIA.* [En Línea]. Colombia. Disponible en: http://www.fusagasuga-cundinamarca.gov.co/Transparencia/MODELO%20INTEGRADO%20DE%20PLANEACION%20Y%20GESTION/Plan%20de%20Transicion%20del%20Protocolo.pdf

[12] Google IPv6, *Statistics* [En línea], Disponible en: https://www.google.com/intl/en/ipv6/statistics.html

[13] MONSERRAT Francisco. *Reciclaje de ataques IPv4 en Ipv6.* [En Línea]. Valencia. Disponible en: http://www.rediris.es/cert/doc/pres/jornadas-ipv6.pdf

[14] MORENO AGUDELO, José. *Transición de protocolo IPV4 A IPV6, para una Empresa del Estado, con Aplicación en una ciudad Intermedia.*

[15] PEREZ NAVA, Juan. HERRERA GUTIERREZ, Tecnologías y Mecanismos de Transición de Ipv4 a Ipv6. [En Línea]. México. Disponible en: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/2807/Tesis.pdf?sequence=1

[16] RAMIREZ PULIDO, Ferney. GUZMAN PANTOJA, Jaime. BELTRAN DIAZ, Jesús. Diseño De La Transición Del Protocolo Ipv4 Hacia Ipv6 En La Agencia Colombia Para La Reintegracion-Acr Con Base En Consideraciones De Seguridad En Implementación Ipv6 [en línea]. Bogotá. Disponible en: https://repository.ucatolica.edu.co/bitstream/10983/2803/1/IPV6.pdf

[17] *Seguridad y Privacidad de la Información.* [En Línea]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G19_Aseguramiento_protocolo.pdf

[18] SEGURA CRUZ, Edwin. *"METODOLOGIA PARA HACER UNA TRANSICION EN UNA RED IPV4 A IPV6"*. [En Línea]. Bogotá. Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/9245/SeguraEdwin2017.pdf?sequence=1

[19] Stallings, W. (2003). Fundamentos de Seguridad en Redes. Aplicaciones y Estándares (Segunda edición ed.) [En Línea]. Madrid, España: Pearson

[20] TAFFEMABERRY, Carlos. *Protocolo de Internet Versión 6 (ipv6).* [En Línea]. Disponible en: http://www1.frm.utn.edu.ar/teleinformatica/docs/IPv6.pdf

[21] TCP/IP Tutorial and Technical Overview. (diciembre de 2006). [En línea], Disponible en: http://www.redbooks.ibm.com/redbooks/pdfs/gg243376.pdf