DISEÑO Y DESARROLLO DE LA FASE DE PLANEACIÓN DEL PROYECTO DE ADOPCIÓN DE IPv6 EN LA INFRAESTRUCTURA TECNOLÓGICA Y DE COMUNICACIONES DE UNA ENTIDAD ADSCRITA AL MINISTERIO DE AGRICULTURA

HENRY ALBERTO DE LA HOZ NATERA

Trabajo de grado para optar el título
de Especialista en Telecomunicaciones

Director
Ingeniero Alvaro Escobar Escobar
Director especialización en seguridad informática
Director especialización en telecomunicaciones

UNIVERSIDAD PILOTO DE COLOMBIA
PROGRAMA DE POSTGRADOS
ESPECIALIZACIÓN EN TELECOMUNICACIONES
BOGOTÁ D.C.
2016

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del Director

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá D.C., agosto de 2016

AGRADECIMIENTOS

En primer lugar, agradezco profundamente a Dios por este nuevo logro. A mi esposa y a mi hija por ser quienes me acompañaron durante este proceso. A mis padres porque durante los años que tengo de vida me han brindado su apoyo incondicionalmente.

A mi familia en general que, gracias a su apoyo y consejos, he llegado a realizar una de mis grandes metas lo cual constituye la herencia más valiosa que pudiera recibir.

Asimismo, a la entidad y al equipo de trabajo del área de Infraestructura Tecnológica por su apoyo personal y humano.

Al Director de mi trabajo de grado, el Ing. Álvaro Escobar Escobar por su atención ante todas mis consultas y su permanente acompañamiento y orientación.

A la Universidad Piloto de Colombia por haberme dado la oportunidad de escalar un peldaño más en el campo del conocimiento.

CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

AAAA: registro que se utiliza en IPv6 para traducir nombres de hosts a direcciones IPv6[1].

ACCESS POINT: es un dispositivo de red que interconecta equipos de comunicación inalámbricos, para formar una red inalámbrica que interconecta dispositivos móviles o tarjetas de red inalámbricas[2].

BACKBONE: es una parte de la infraestructura de red informática que interconecta varios pedazos de red, proporcionando un camino para el intercambio de información entre las diferentes redes de área local o subredes[3].

BIT: siglas de Binary digit, (Dígito Binario) es un dígito del sistema de numeración binario[4].

BROADCAST: transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea[5].

DHCP**:** siglas de Dynamic Host Configuration Protocol, (Protocolo de Configuración Dinámica de Host), es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente[6].

DNS: siglas de Domain Name System, (Sistema de Nombres de Dominio), es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada[7].

EGP: siglas de Exterior Gateway Protocol, (Protocolo de Gateway Exterior), es un protocolo estándar usado para intercambiar información de enrutamiento entre sistemas autónomos[8].

---

[1] Disponible en Internet: https://www.hostingvox.com/knowledgebase.php?action=displayarticle&id=4
[2] Disponible en Internet: https://es.wikipedia.org/wiki/Punto_de_acceso_inal%C3%A1mbrico
[3] Disponible en Internet: http://www.slideboom.com/presentations/389164/GLOSARIO-DE-TERMINOS-REDES
[4] Disponible en Internet: https://es.wikipedia.org/wiki/Bit
[5] Disponible en Internet: http://rm-rf.es/broadcast-multicast-y-unicast/
[6] Disponible en Internet: https://www.ietf.org/rfc/rfc2131.txt
[7] Disponible en Internet: https://www.ietf.org/rfc/rfc1035.txt
[8] Disponible en Internet: https://tools.ietf.org/html/rfc827

FIREWALL: (ó Cortafuegos), es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas[9].

HTML: siglas de HyperText Markup Language, (Lenguaje de Marcado de Hipertexto), definido en el RFC 2854 de la IETF, hace referencia al lenguaje de marcado predominante para la elaboración de páginas web que se utiliza para describir y traducir la estructura y la información en forma de texto[10].

IANA: siglas de *Internet Assigned Numbers Authority*, es la entidad que supervisa la asignación global de direcciones IP[11].

ICMPv6: siglas de *Internet Control Message Protocol for IPv6*, (Protocolo de Mensajes de Control de Internet para IPV6), descrito en el RFC 4443 de la IETF, este protocolo es una nueva versión de ICMP y es una parte importante de la arquitectura IPv6 que debe estar completamente soportada por todas las implementaciones y nodos IPv6[12].

IDF: siglas de *Intermediate distribution frame* (Centro Intermedio de Distribución). Recinto de comunicación secundaria para un edificio que usa una topología de red en estrella[13].

IETF: siglas de *Internet Engineering Task Force*, (Grupo Especial sobre Ingeniería de Internet) es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad, etc[14].

IGP: siglas de Interior Gateway Protocol, (Protocolo de Gateway Interno) hace referencia a los protocolos usados dentro de un sistema autónomo[15].

IOS**:** siglas de Internetwork Operating System, es el software utilizado en la gran mayoría de routers y switches de Cisco Systems[16].

---

[9] Disponible en Internet: https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)
[10] Disponible en Internet: https://tools.ietf.org/html/rfc2854
[11] Disponible en Internet: http://www.iana.org/
[12] Disponible en Internet: https://tools.ietf.org/html/rfc4443
[13] Disponible en Internet: https://arodrigolopezgallegos1114.wordpress.com/2014/05/07/idf-y-mdf/
[14] Disponible en Internet: https://www.ietf.org/about/
[15] Disponible en Internet: https://es.wikipedia.org/wiki/IGP
[16] Disponible en Internet: https://es.wikipedia.org/wiki/Cisco_IOS

IPSEC: siglas de Internet Protocol Security, es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet, autenticando o cifrando cada paquete IP en un flujo de datos[17].

LACNIC: corresponde al Registro de Direcciones de Internet para América Latina y Caribe, es una organización no gubernamental internacional establecida en Uruguay en el año 2002. Es responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa, entre otros recursos para la región de América Latina y el Caribe[18].

LAN: siglas de Local Área Network, (Red de área local) es la interconexión de una o varias computadoras y periféricos[19].

LOOPBACK: es una interfaz de red virtual. Las direcciones del rango '127.0.0.0/8' son direcciones de loopback, de la cual la que se utiliza de forma mayoritaria es la '127.0.0.1' por ser la primera de dicho rango[20].

MDF: siglas de *Main Distribution Frame.* **(**Centro de Distribución Principal). es una estructura de distribución de señales para conectar equipos de redes y telecomunicaciones a los cables y equipos que corresponden al proveedor de servicios de telefonía, Internet, entre otros[21].

MPLS: siglas de *Multiprotocol Label Switching*, (Conmutacion Multiprotocolo mediante Etiquetas) es un mecanismo de transporte de datos estándar creado por la IETF. Opera entre la capa de enlace de datos y la capa de red del modelo OSI[22].

MRU: siglas de *Maximum Receive Unit*, (Unidad Máxima de Recepción), es la unidad que indica el tamaño máximo (en octetos) del campo de datos de una trama (en el nivel de enlace) que un determinado host es capaz de recibir en una red[23].

MTU: siglas de *Máximum Transfer Unit*, (Unidad Máxima de Transferencia) es un término que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un protocolo de comunicaciones[24].

---

[17] Disponible en Internet: https://seguridadenredesgjsa.wordpress.com/ipsec/
[18] Disponible en Internet: http://www.lacnic.net/web/lacnic/acerca-lacnic
[19] Disponible en Internet: https://redes-de-computadoras.wikispaces.com/Clasificaci%C3%B3n
[20] Disponible en Internet: https://es.wikipedia.org/wiki/Loopback
[21] Disponible en Internet: https://es.wikipedia.org/wiki/Main_distribution_frame
[22] Disponible en Internet: https://tools.ietf.org/html/rfc3031
[23] Disponible en Internet: https://es.wikipedia.org/wiki/Maximum_Receive_Unit
[24] Disponible en Internet: https://es.wikipedia.org/wiki/Unidad_m%C3%A1xima_de_transferencia

MULTICAST: (multidifusión), es el envío de la información en una red a múltiples destinos simultáneamente[25].

ND: siglas de *Neighbor Discovery*, (Descubrimiento de Vecinos) es un conjunto de mensajes y procesos que determinan las relaciones entre nodos vecinos[26].

NIBBLE: conjunto de cuatro dígitos binarios (bits)[27].

OSPFv3: siglas de Open Shortest Path First, definido por la IETF, es un protocolo de enrutamiento creado para soportar direccionamiento IPv6[28].

PVC: siglas de *Poly Vinyl Chloride*, (Poli Cloruro de Vinilo) es un polímero termoplástico que se presenta como un material blanco que comienza a reblandecer alrededor de los 80 °C y se descompone sobre los 140 °C[29].

QoS: siglas de *Quality of Service*, (Calidad de Servicio) son las tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado[30].

RACK: soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones[31].

RAM: siglas de *Random Access Memory*, (Memoria de Acceso Aleatorio) se utiliza como memoria de trabajo para el sistema operativo, los programas y la mayoría del software[32].

RFC: de las siglas en inglés *Request For Comments*, un documento que puede ser escrito por cualquier persona y que contiene una propuesta para una nueva tecnología, información acerca del uso de tecnologías y/o recursos existentes, propuestas para mejoras de tecnologías, proyectos experimentales y demás[33].

RIP: siglas de *Routing Information Protocol*, (Protocolo de Información de Enrutamiento), es un protocolo de puerta de enlace interna o IGP, utilizado por los routers para intercambiar información acerca de redes IP[34].

---

[25] Disponible en Internet: https://es.wikipedia.org/wiki/Multidifusi%C3%B3n
[26] Disponible en Internet: http://www.ipv6.es/es-ES/Glosario/Paginas/DEF.aspx
[27] Disponible en Internet: https://es.wikipedia.org/wiki/Nibble
[28] Disponible en Internet: https://tools.ietf.org/html/rfc5340
[29] Disponible en Internet: http://www.ecured.cu/Policloruro_de_vinilo
[30] Disponible en Internet: http://elastixtech.com/qos-calidad-de-servicio-para-voip/
[31] Disponible en Internet: https://es.wikipedia.org/wiki/Rack
[32] Disponible en Internet: http://ingeniatic.euitt.upm.es/index.php/tecnologias/item/512-memoria-ram
[33] Disponible en Internet: http://www.mikroways.net/2009/07/12/%C2%BFque-es-una-rfc/
[34] Disponible en Internet: https://tools.ietf.org/html/rfc2453

RIPng: siglas de *Routing Information Protocol Next Generation*, (Protocolo de Información de Enrutamiento de la siguiente generación), descrito en el RFC 2080 de la IETF, se refiere al protocolo RIP de la siguiente generación que tiene soporte para IPv6[35].

SWITCH: es el dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red y eliminando la conexión una vez finalizada esta[36].

TCP/IP: siglas de *Transmition Control Protocol/Internet Protocol*. (Protocolo de control de transmisión/Protocolo de Internet), es un conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre computadoras[37].

TIA/EIA-568-B: tres estándares que tratan el cableado comercial para productos y servicios de telecomunicaciones[38].

UDP: siglas de User Datagram Protocol, es un protocolo del nivel de transporte basado en el intercambio de datagramas[39].

ULA: es uno de los tres tipos de direcciones unicast soportados por IPv6. Las direcciones ULA son válidas y enrutables en el ámbito de la organización, pero no se permiten en Internet, muy similar al comportamiento que demuestran, en IPv4, los bloques de direcciones especificados en el RFC 1918[40].

UNICAST: es el envío de información desde un único emisor a un único receptor[41].

VLAN: siglas de *Virtual Local Área Network* (Red de Área Local Virtual) es un método de crear redes lógicamente independientes dentro de una misma red física[42].

---

[35] Disponible en Internet: https://tools.ietf.org/html/rfc2080
[36] Disponible en Internet: https://es.wikipedia.org/wiki/Conmutador_(dispositivo_de_red)
[37] Disponible en Internet: https://es.wikipedia.org/wiki/Familia_de_protocolos_de_Internet
[38] Disponible en Internet: https://es.wikipedia.org/wiki/TIA-568B
[39] Disponible en Internet: https://www.ietf.org/rfc/rfc768.txt
[40] Disponible en Internet: http://www.vptecnologia.com.ve/item/7-ipv6-ula-para-que-sirven
[41] Disponible en Internet: https://es.wikipedia.org/wiki/Unidifusi%C3%B3n
[42] Disponible en Internet: https://es.wikipedia.org/wiki/VLAN

VoIP: siglas de Voice over IP, (Voz sobre el Protocolo de Internet) es un grupo de recursos que hacen posible que la señal de voz viaje a través del Internet mediante el protocolo IP[43].

WAN: siglas de Wide Área Network, (Red de Área Amplia) es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proporcionando servicio a un país o un continente[44].

WIFI: es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica[45].

[43] Disponible en Internet: http://elastixtech.com/fundamentos-de-telefonia/voip-telefonia-ip/
[44] Disponible en Internet: http://redestipostopologias.blogspot.com.co/2009/03/tipos-de-redes.html
[45] Disponible en Internet: https://es.wikipedia.org/wiki/Wifi

INTRODUCCIÓN

Este proyecto de investigación presenta y explica los lineamientos que se deben tener en cuenta al momento de llevar a cabo la fase planeación para el despliegue y aseguramiento del protocolo IPv6 en la infraestructura tecnológica y de comunicaciones una entidad adscrita al ministerio de agricultura de Colombia. Apoyado en las recomendaciones y guías vigentes definidas por el Ministerio de las Tecnologías de Información y las Comunicaciones (en adelante MinTic) y su estrategia de “Gobierno en Línea” se pretende llevar un ciclo de desarrollo por fases en un ambiente controlado que permita consolidar el proceso de adopción de IPv6 con alta seguridad y un nivel de impacto altamente positivo en toda la organización.

Cabe resaltar que el desarrollo de todas las fases para la adopción del nuevo protocolo (planeación, implementación y pruebas) conlleva requisitos importantes de tiempo, inversión, recurso humano y compromiso desde áreas directivas como operativas. No obstante lo anterior, se aclara que el presente trabajo se desarrolla teniendo en cuenta únicamente la fase de planeación, la cual representa la etapa más crítica e importante del proceso y está enmarcada en las actividades, diagnósticos, diseños, y demás aspectos relevantes que definen y estructuran el desarrollo del proceso completo de adopción de IPv6 en la entidad, entre otras, el desarrollo de un análisis económico con miras a definir una propuesta de implementación que permita dimensionar el impacto que tendría para la entidad poder llevar a cabo las siguientes fases. Es importante además mencionar que, al ser una entidad pública del orden nacional, está obligada a regirse por la normatividad y legislación vigente en Colombia por lo cual posteriores fases del proyecto dependerán del presupuesto aprobado en la entidad. Adicionalmente, es la intención del presente trabajo documentar y evidenciar todas las consideraciones necesarias para que la planeación del proyecto en general siente las bases para las futuras actividades generadas en las fases de implementación y pruebas.

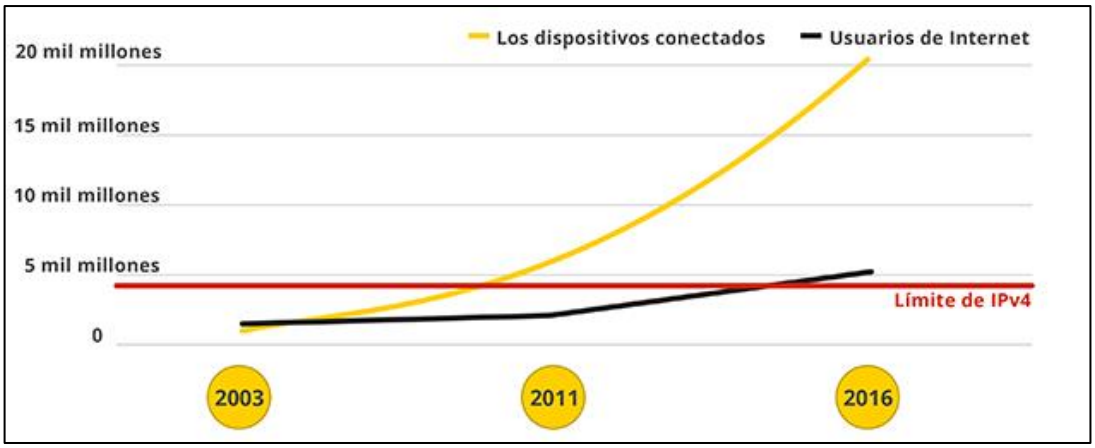
La importancia de un proyecto de implementación del mencionado protocolo radica en la posibilidad de crecimiento y evolución de las redes actuales, cuyas más recientes amenazas se han enfocado en el agotamiento de direcciones IP y aunque es común encontrar información acerca de las ventajas del protocolo IPv6 por sus evidentes características beneficiosas sobre IPv4, es válido notar que el foco de la transición no está en mejorar algunas características específicas sino en permitir el crecimiento de las redes antes que cualquier otra cosa.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES

El protocolo de internet versión 4 (IPv4) es el actual protocolo de capa 3 del modelo OSI usado en Internet y en la mayoría de las redes. IPv4 ha sobrevivido por más de 30 años y ha sido una parte integral de la evolución de internet. Fue originalmente descrito en el RFC 760 (enero de 1980) y el mismo declarado obsoleto por el RFC 791 (septiembre de 1981). En los primeros años, incluso con la llegada del *World Wide Web* a comienzos de los 90's, solo habían alrededor de 16 millones de usuarios en internet en todo el mundo comparado a los más de 3 billones del 2011[46] en adelante (ver figura 1). El actual número de dispositivos incrementa dramáticamente teniendo en cuenta que los usuarios de hoy día usualmente tienen múltiples dispositivos habilitados para internet como *smart phones*, *tablets* y *laptops*, superando los más de 20 billones de dispositivos conectados actualmente, tal y como se muestra en la figura 1.

Figura 1. Crecimiento de dispositivos y usuarios conectados



Fuente: google.com. Disponible en: https://www.google.com/intl/es/ipv6/index.html

De acuerdo con Niranjan Ravi, Muppidathi Saravanan A y Manoranjan Periyasamy, A finales de los 70s, una familia de protocolos experimentales fue desarrollada conocida como *Internet Stream Protocol* (ST) y después ST2. Originalmente

[46] Referencia: *Internet World Stats*, disponible en http://www.internetworldstats.com

definida en la *Internet Engineering Note* IEN-119 (1979), fue luego revisada en los RFC's 1190 y 1819. ST fue un protocolo de reserva de recursos experimental destinado a proveer calidad de servicio (QoS) para aplicaciones multimedia en tiempo real como video y voz. ST consistía de dos protocolos – ST (*Internet Stream Protocol*) y *Stream Control Message Protocol* (SCMP). ST2 no fue diseñado como un remplazo para IPv4, la idea era que aplicaciones multimedia pudieran usar ambos protocolos – el protocolo IPv4 para transferencia de paquetes tradicionales y ST2 para paquetes que llevaran datos en tiempo real. A pesar de que nunca fue reconocido como IPv5, cuando se encapsulaba en IP, ST usaba el protocolo IP numero 5 (RFC 1700). En otras palabras, aunque nunca fue implementado, la designación "IP versión 5" ya fue usada. El estándar actual para reservación de recursos es el protocolo de la capa de transporte RSVP (*Resource Reservation Protocol*), el cual puede ser usado para proporcionar la configuración del receptor iniciado sobre IPv4.[47]

La historia de internet además nos habla que durante años el protocolo IP versión 4 ha figurado, metafóricamente hablando, como el principal engrane en la robusta y compleja maquinaria que la compone, y ha propiciado el desarrollo y crecimiento de innovadores sistemas y tecnologías que han facilitado la vida del ser humano.

Sin embargo, los creadores de IPv4, a principio de los años 70, no predijeron en ningún momento, el gran éxito que este protocolo iba a tener en muy poco tiempo, en una gran multitud de campos, no solo científicos y de educación, sino también en innumerables facetas de la vida cotidiana.

A principios de los años noventa, el Grupo de Trabajo de Ingeniería de Internet (en adelante IETF[48]) centró su interés en el agotamiento de direcciones de red IPv4 y comenzó a buscar un reemplazo para este protocolo. Esta actividad produjo el desarrollo de lo que hoy se conoce como IPv6.

Crear mayores capacidades de direccionamiento fue la motivación inicial para el desarrollo de este nuevo protocolo. También se consideraron otros temas durante el desarrollo de IPv6, como manejo mejorado de paquetes, escalabilidad y longevidad mejoradas, mecanismos QoS (Calidad del Servicio), seguridad integrada, entre otros.

---

[47] NIRANJAN, Ravi, MUPPIDATHI Saravanan, y MANORANJAN, Periyasamy. "Implementation of IPv6/IPv4 Dual-Stack Transition Mechanism". Obtenido el 7 de marzo de 2016. Disponible en: http://www.ijircce.com/upload/2014/november/5_Implementation.pdf

[48] IETF (Internet Engineering Task Force)

Como se puede ver, IPv6 ha sido diseñado con escalabilidad para permitir años de crecimiento de la *internetwork*. Sin embargo, IPv6 se está implementando lentamente en redes selectas y en este proceso han surgido obstáculos evidentes por su poco conocimiento y experiencia. Debido a las mejores herramientas, tecnologías y administración de direcciones en los últimos años, IPv4 todavía se utiliza ampliamente y probablemente permanezca durante algún tiempo en el futuro. Sin embargo, IPv6 se está encaminando eventualmente a reemplazar a IPv4 como protocolo de Internet dominante.

Al conocer las dificultades u obstáculos que la transición a IPv6 conlleva es necesario considerar una planeación adecuada desde todo nivel, lo que hace importante tener la capacidad prever los posibles riesgos y factores que produzcan una interrupción de servicios y comunicaciones del instituto una vez se haya alcanzado la fase de implementación.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuáles son los factores a considerar en las fases de planeación e implementación del protocolo IPv6 en la infraestructura tecnológica y de comunicaciones de la entidad?

2. JUSTIFICACIÓN

El sistema global de direcciones de Internet (el medio por el cual se envían paquetes de información a la ubicación o al destinatario deseado a través de Internet) se está quedando sin direcciones. El protocolo de direcciones actual (IPv4) creó aproximadamente 4 mil millones de direcciones y, debido al enorme éxito de Internet, se espera que la fuente de direcciones restantes se agote próximamente a nivel global. De acuerdo a informes de la IANA (Internet Assigned Numbers Authority) sus bloques de direcciones /8 se agotaron en febrero de 2011, APNIC fue el primer RIR en quedarse sin espacio a los pocos meses de 2011, RIPE NCC agotó su espacio IPv4 en octubre de 2012 y LACNIC agotó su espacio IPv4 el 10 de junio de 2014.[49]

El nuevo protocolo de direcciones, IPv6, ofrece un espacio de direcciones que tiene una capacidad para 340 billones de billones de billones de direcciones, lo que hace que la cantidad de direcciones IPv4 parezca insignificante. Con este mayor espacio de direcciones, IPv6 ofrece una variedad de ventajas en términos de estabilidad, flexibilidad y simplicidad en la administración de redes. También es probable que la era IPv6 genere una nueva ola de innovación en las aplicaciones y las ofertas de servicios ya que, en muchos casos, termina con la necesidad de direcciones compartidas y el ocultamiento de red.

IPv6 se está implementando lentamente en redes y coexistirá con IPv4 hasta que se produzca una transición hacia IPv6 (una transición que probablemente demore varios años). Si bien el trabajo técnico relacionado con el protocolo, en gran medida, se ha completado, lo que resta es el uso. Lamentablemente, este proceso no se está realizando con la rapidez necesaria y puede tornarse en un gran desafío para el abordaje global integral ininterrumpido.

La entidad, perteneciente al sector público del orden nacional con personería jurídica, autonomía administrativa y patrimonio independiente. Además tiene jurisdicción en todo el territorio nacional, siendo su domicilio principal la ciudad de Bogotá, D.C., cuenta con 32 Gerencias Seccionales, una por departamento, y cada una de estas sedes se encuentran interconectadas mediante una red MPLS a través de un proveedor de telecomunicaciones con el datacenter ubicado en las oficinas de la gerencia general en Bogotá D.C. Toda su infraestructura tecnológica, de servicios y de comunicaciones actualmente está basada en IPv4.

---

[49] LACNIC. “Estado de IPv4 a fin de 2012”. Obtenido el 10 de mayo de 2016. Disponible en: http://portalipv6.lacnic.net/estado-de-ipv4-a-fin-de-2012-es/

En concordancia con las indicaciones de los entes que gestionan y administran los recursos de internet a nivel mundial y las disposiciones nacionales impartidas por el MinTic a través de la Dirección de Estándares y Arquitecturas de Tecnologías de la Información, desde el año 2014 se ha convertido en un tema indispensable y de gran importancia para las entidades públicas y privadas del país iniciar las actividades necesarias para la adopción del protocolo IPv6. En consecuencia, para cumplir con los objetivos de innovación tecnológica que exige el país, las entidades del sector publico debieron entrar en el proceso de transición del protocolo IPv4 hacia el nuevo protocolo IPv6 siguiendo las instrucciones descritas en la Circular 002 del 6 de julio de 2011 del Ministerio de Tecnologías de la Información y las Comunicaciones[50].

Adicionalmente, teniendo en cuenta las disposiciones del plan “Vive Digital” para la implementación de la estrategia GEL (Gobierno En Línea) el MinTic dispuso que las entidades debían cumplir al año 2015 con criterios específicos medidos mediante componentes que implican consideraciones que impactan las diferentes áreas temáticas y sirven de soporte a éstas, los componentes de la estrategia de GEL se derivan de la evolución de las “Fases de Gobierno en línea” contempladas en el Decreto 1151 de 2008. Dentro de estos componentes se encuentra el de “Elementos Transversales” el cual tiene como objetivo principal “Incorporar el Gobierno en línea como parte de la cultura y de la estrategia de innovación organizacional”, una de las actividades de este componente es la implementación de un sistema de gestión de TI con una participación del 15% dentro del componente, y la cual a su vez se subdivide en dos criterios a cumplir, La planeación del ajuste tecnológico (10%) y el protocolo de Internet IPv6 (5%), este último a su vez esta descrito por tres fases, la planeación (1%), implementación (3%) y monitoreo (1%).[51] De tal manera el presente trabajo está encaminado a realizar todas las actividades correspondientes al proceso de planeación que permitan dar cumplimiento a las metas establecidas por el MinTic.

Con la adopción del protocolo IPv6 la entidad tendrá más beneficios en cuanto a la mayor cantidad de direcciones para conectarse a internet, el fortalecimiento de la seguridad de la información, la mejora en el diseño y puesta en marcha de aplicaciones, mejora en el envío de conexiones de audio y vídeo por la red, entre otras. Sin embargo, un proyecto de implementación de este tipo no permite medir o dimensionar con facilidad los factores costo/beneficio para ser evaluados por la entidad, por lo tanto, se pretende identificar y justificar los costos económicos y de otro tipo que requiera llevar a cabo la implementación del proceso de adopción del protocolo IPv6.

---

[50] Disponible en http://www.MinTic.gov.co/portal/604/articles-5932_documento.pdf
[51] Manual 3.0 de la Estrategia Gobierno En Línea

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar y desarrollar las actividades de la fase de planeación del proyecto de adopción del protocolo IPv6 en la infraestructura tecnológica y de comunicaciones de la entidad.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar, diseñar y desarrollar el plan de diagnóstico del protocolo IPv4 a IPv6 en la red de la entidad.
- Elaborar y validar un inventario de activos de información de servicios tecnológicos.
- Identificar la topología actual de la red y su funcionamiento dentro de la organización.
- Evaluar el grado de afinidad del protocolo IPv6 a nivel de hardware y software con miras a preparar la nueva infraestructura de red.
- Validar el estado actual de los sistemas de información y de comunicaciones y evaluar la interacción entre ellos una vez adoptado el nuevo protocolo.
- Generar un análisis económico estructurado que permita definir una propuesta de implementación basada en la relación costo/beneficio para la entidad.

4. MARCO REFERENCIAL

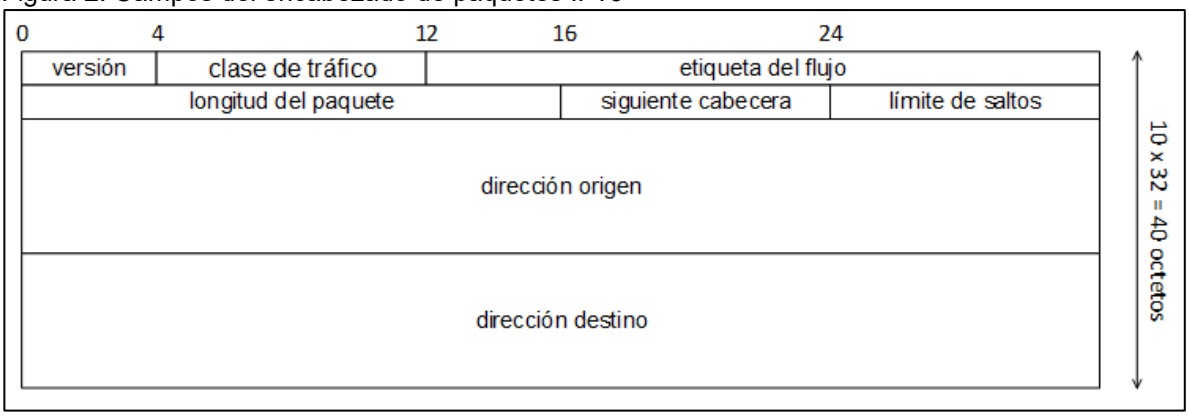
4.1 MARCO CONCEPTUAL

4.1.1 Cabecera IPv6. El origen de IPv6 data desde el 1991, cuando la IETF empezó a estudiar el problema de expandir el número de direcciones de Internet realizando un cambio en la cabecera del protocolo, lo que significaba una nueva versión de IP.

El protocolo IPv6 es un protocolo que permite aumentar el tamaño de direcciones IP de 32 a 128 bits, es decir 2^{128} posibles direcciones. Este aumento en el espacio de direcciones no solo proporciona mayor número de hosts, sino una jerarquía de direcciones mayor.

La cabecera IPv6, como se puede ver en la figura 2, elimina o hace opcionales varios de los campos de la cabecera IPv4, con el fin de obtener una cabecera de tamaño fijo, más simple y reduciendo el tiempo de procesamiento de los paquetes.[52]

Figura 2. Campos del encabezado de paquetes IPv6



Fuente: Ramón, M. (2001), Cabecera de IPv6. Obtenida el 18 de julio de 2016. Disponible en: http://www.ramonmillan.com/tutoriales/ipv6_parte1.php#cabeceraipv6

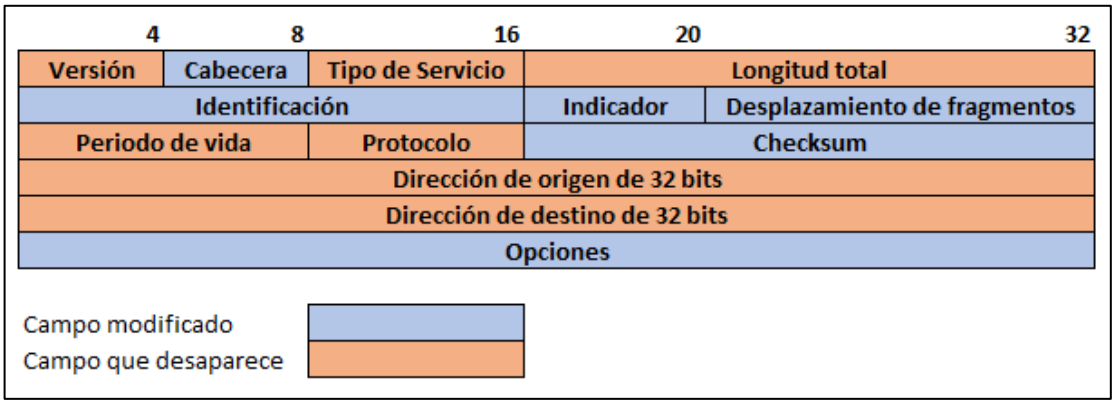
La cabecera básica de IPv6, tiene una longitud fija de 40 octetos y está compuesta de los siguientes campos:

[52] RAMOS, I. (2011), "IPv4-IPv6". Obtenida el 18 de julio de 2016. Disponible en: https://es.scribd.com/document/52418918/IPV4-IPV6

▪ Versión (4 bits): es el número de versión de IP, es decir 6.
▪ Clase de tráfico (8 bits): el valor de este campo especifica la clase de tráfico. Los valores de 0 - 7 están definidos para el tráfico de datos con control de la congestión, y de 8-15 para tráfico de vídeo y audio sin control de congestión.
▪ Etiqueta del flujo (20 bits): el estándar IPv6 define un flujo como una secuencia de paquetes enviados desde un origen específico a un destino. Un flujo se identifica únicamente por la combinación de una dirección fuente y una etiqueta de 20bits. De este modo, la fuente asigna la misma etiqueta a todos los paquetes que forman parte del mismo flujo.
▪ Longitud del paquete (16 bits): especifica el tamaño total del paquete, incluyendo la cabecera y los datos, en bytes. Es necesario porque también hay campos opcionales en la cabecera.
▪ Siguiente cabecera (8 bits): indica el tipo de cabecera que sigue a la cabecera fija de IPv6, por ejemplo, una cabecera TCP/UDP, ICMPv6 o una cabecera IPv6 opcional.
▪ Límite de saltos (8 bits): es el número de saltos máximo que le quedan al paquete. El límite de saltos es establecido a un valor máximo por el origen y reducido en 1 cada vez que un nodo encamina el paquete. Si el límite de saltos es reducido y toma el valor 0, el paquete es descartado.
▪ Dirección origen (128 bits): es la dirección del origen del paquete.
▪ Dirección destino (128 bits): es la dirección del destino del paquete.[53]

A continuación, en la figura 3 y 4, podemos observar como se ha reducido el tamaño de los 12 campos de la cabecera del protocolo IPv4 a 8 campos en IPv6

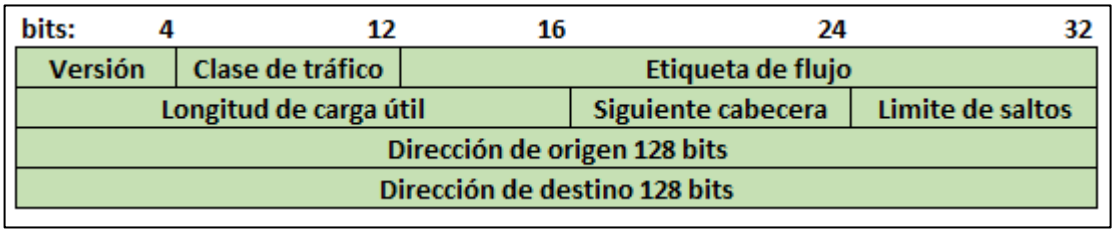
Figura 3. Formato de la cabecera del protocolo IPv4



Fuente: Elaboración propia

[53] MILLÁN, R. (2001), "El Protocolo IPv6". Obtenida el 18 de julio del 2016, disponible en http://www.ramonmillan.com/tutoriales/ipv6_parte1.php.

Figura 4. Formato de la cabecera del protocolo IPv6



Fuente: Elaboración propia

El motivo fundamental por el cual estos campos (tipo de servicio, indicadores, identificación y control de errores) son eliminados es la innecesaria redundancia, en IPv4 se está facilitando la misma información en diversas formas, como es el caso del campo control de errores.

En la figura 4 se puede observar que el campo desplazamiento de fragmentación de IPv4 ha sido eliminado, porque los paquetes ya no son fragmentados en los nodos intermedios, en IPv6 es un proceso que se produce extremo a extremo, El único campo realmente nuevo en la cabecera del protocolo IPv6 es la etiqueta de flujo.[54]

4.1.2 Descripción de IPv6. IPv6 es la nueva versión del protocolo IP que ha sido diseñado por el IETF para reemplazar en forma gradual a la versión actual de IPv4

(Ramírez y Cervantes, 2005[55]) nos presentan algunas de las características más importantes sobre IPV6:

- Ofrece un mayor espacio de direcciones. El tamaño de las direcciones IP
- cambian de 32 bits a 128 bits, con el fin de soportar mayores niveles de jerarquía
- de direccionamiento.
- Simplificación del formato de la cabecera IPv4 debido a que algunos campos se
- quitan o se hacen opcionales.
- Permite obtener paquetes IP eficientes y extensibles.
- Posibilidad de paquetes con una carga útil (datos) de más de 65.355 bytes.
- Calidad de servicio (QoS) y clase de servicio (CoS).

[54] MILLÁN, Ramón. op. cit. p.18
[55] RAMÍREZ, Sergio, y CERVANTES, María, (2005), “Introducción a IPV6”, Obtenida el 20 de Julio del 2011. Disponible en http://www.rau.edu.uy/ipv6/queesipv6.htm#01

• Seguridad en el núcleo del protocolo (IPsec).
• Capacidad de etiquetas de flujo que pueden ser usadas por un nodo origen para etiquetar paquetes pertenecientes a un flujo de tráfico particular.

4.1.3 Resolución de nombres en IPv6[56]. El Sistema de Nombres de Dominio (DNS) no puede ser fácilmente extendido para dar un soporte eficiente a las direcciones IPv6 debido a que las aplicaciones luego de ser consultadas retornan solamente direcciones IPv4 de 32 bits. Para dar un soporte adecuado a las direcciones IPv6 se debe definir lo siguiente:

• Un nuevo tipo de registro con el fin de relacionar un nombre de dominio con una dirección IPv6.
• Un nuevo dominio con el fin de brindar un soporte hacia las búsquedas basadas en la dirección IPv6.

La definición de un nuevo tipo de registro permite almacenar la dirección IPv6 de un host. En algunos casos un host tiene varias direcciones IPv6 por lo cual deberá tener más de un registro similar.

4.1.3.1 Tipos de registro. Existe un nuevo tipo de registro de recurso “AAAA” cuya función es almacenar una sola dirección IPv6, su equivalente en IPv4 es el registro “A”. En la figura 5, se presenta un ejemplo de un sitio web con los dos tipos de registros:

Figura 5. Sitio web asociado a diferentes tipos de registro

Tipo de registro	Formato
A	www.ica.gov.co A 200.0.28.3
AAAA	www.ica.gov.co AAAA 2001:DB8:ABCD:D21:1::2

Fuente: Elaboración propia

Ahora podemos decir que el proceso de resolución inversa del nombre de dominio IPV6 utiliza el tipo de registro de recurso “PTR” cuyo equivalente en IPv4 es el mismo.

[56] THOMSON, S. y HUITEMA, C. (1995), “Extensiones al DNS para dar soporte a IPv6”, Obtenida el 21 de Julio del 2016. Disponible en http://www.rfc-es.org/rfc/rfc1886-es.txt

Una dirección IPv6 se representa por una secuencia de *nibbles* separados por puntos con el sufijo ".IP6.INT". La secuencia de *nibbles* se codifican en orden inverso es decir primero el *nibble* de menor orden, seguido por el siguiente de menor orden, etc. Finalmente, cada *nibble* se representa por un dígito hexadecimal, en la figura 6 se puede apreciar un ejemplo:

Figura 6. Registro PTR

Tipo de registro	Formato
PTR	2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.8.1.c.0.y.y.y.y.e .f.f.3.ip6.int PTR www.ica.gov.co

Fuente: Cisco Systems, Inc., CISCO IOS IPv6 Configuration Guide, (2008), USA.

4.1.4 Principales protocolos en IPv6.

4.1.4.1 Protocolo ICMPv6[57]. El protocolo ICMPv6 es utilizado por los nodos IPv6 con el fin de informar sobre los errores encontrados durante el procesamiento de los paquetes y para realizar otras funciones relativas a la capa de internet como son los diagnósticos ("ping").

Los mensajes ICMPv6 se dividen en dos tipos:

- Mensajes de error: se identifican con un 0 en su campo "Tipo de mensaje" y sus valores van desde 0 a 127.
- Mensajes informativos: sus valores están entre 128 y 255.

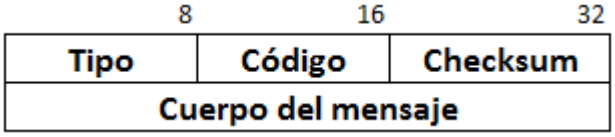
"Mediante ICMPv6, los hosts y los enrutadores que se comunican mediante IPv6 pueden informar sobre los errores que se presentan y enviar mensajes de eco simples."[58]

En la figura 7 se puede observar el formato de un mensaje ICMPv6:

[57] S. Deering, (1998), "ICMPv6 para IPv6". Obtenida el 22 de Julio del 2016. Disponible en http://www.ietf.org/rfc/rfc2463.txt

[58] MICROSOFT, (n.d), "Protocolo de mensajes de control de Internet para IPv6 (ICMPv6)". Obtenida el 22 de julio del 2016. Disponible en: http://technet.microsoft.com/es-es/library/cc757063%28WS.10%29.aspx

Figura 7. Formato de un mensaje ICMPv6



Fuente: Elaboración propia

4.1.4.2 Descubrimiento de escucha de multidifusión. Como su nombre lo indica la multidifusión consiste en enviar una serie de mensajes ICMPv6 a un solo destino, pero el procesamiento se produce en múltiples host.

De acuerdo con el concepto citado en el párrafo anterior podemos decir lo siguiente:

- El conjunto de host que atienden en una sola dirección de multidifusión se conoce como grupo de multidifusión.
- Los grupos de multidifusión son dinámicos.
- Un *host* puede unirse a un grupo de multidifusión mediante él envió de mensajes.
- Un *host* puede enviar tráfico a diferentes direcciones de grupo.

El objetivo de los mensajes MDL es poder intercambiar información acerca del estado entre los enrutadores IPv6 y los miembros de cada uno de los grupos de multidifusión.

4.1.4.3 Descubrimiento de vecinos (ND). El protocolo de descubrimiento de vecinos puede ser utilizado por un *host*, *router* o nodo y ofrece diferentes funciones:

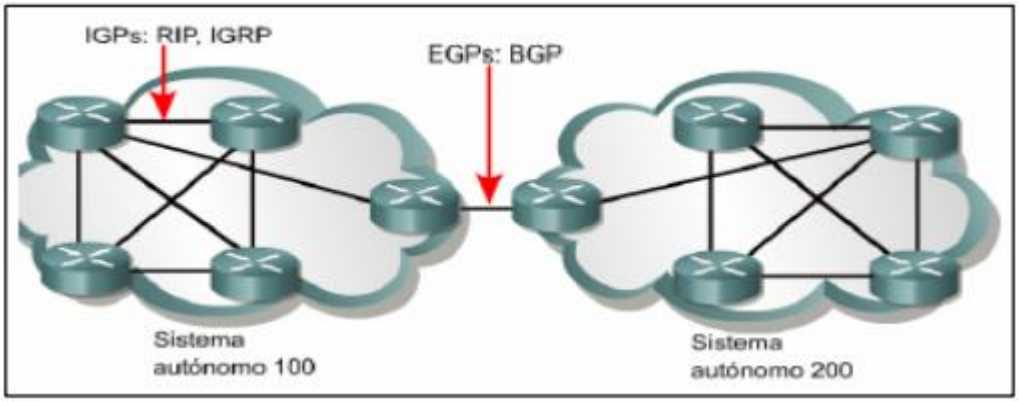
En un *host*:
- Permite descubrir enrutadores vecinos.
- Permite descubrir direcciones y otros parámetros de configuración.

En un *router*:
- Permite notificar su presencia mediante diferentes parámetros de configuración de host.
- Permite notificar a los hosts sobre la mejor dirección del siguiente salto.

En los nodos:
- Permite resolver la dirección IPv6 de un nodo vecino.
- Permite determinar si se pueden enviar y recibir paquetes IPv6 de un vecino.

4.1.5 Protocolos de enrutamiento.

Figura 8. Protocolos de enrutamiento



Fuente: Staky, "CCNA 1 and 2" Versión 3.1. Curriculum en formato pdf, (n.d), p. 218.

En la actualidad IPv6 adopta los mismos protocolos de enrutamiento que se utilizan en las redes IPv4 para interconectar sistemas autónomos (ver figura 8) a continuación se presentan estos:

1. IGP: Protocolo de enrutamiento de Gateway Interior.
Ejemplos: RIPng, OSPFv3.

2. EGP: Protocolo de enrutamiento de Gateway Exterior.
Ejemplo: BGP.

4.1.5.1 RIPng para IPv6[59]. Este protocolo está diseñado para que los *routers* puedan intercambiar información de rutas a través de una red basada en IPv6. RIPng es un protocolo de enrutamiento vector-distancia cuya finalidad es determinar mediante la métrica la dirección y la ruta más óptima de forma automática.

Cada *router* que implementa RIPng tiene una tabla de enrutamiento el cual posee una entrada para cada destino que se quiere alcanzar en todo el sistema de funcionamiento RIPng.

[59] MALKIN, G. y MINNEAR, R. (1997), "RIPng for IPv6", Obtenida el 24 de julio del 2016. Disponible en: http://www.ietf.org/rfc/rfc2080.txt

Cada entrada de la tabla de enrutamiento contiene la siguiente información:

- El prefijo IPv6 de destino.
- Una métrica que representa el número de saltos desde el *router* al destino.
- La dirección IPV6 del siguiente *router* y la ruta hacia el destino.
- Una bandera para indicar el cambio de ruta.
- Varios contadores asociados con la ruta.

4.1.5.2 OSPFv3 para IPv6. Éste es un protocolo de enrutamiento de estado de enlace desarrollado por la IETF en 1988, cuya función es responder rápidamente las actualizaciones o cambios que se producen en la red.

Staky nos presenta la siguiente definición: "Este tipo de protocolo permite enviar actualizaciones periódicas por rangos más prolongados por ejemplo de 20 minutos. Los algoritmos de estado de enlace utilizan sus bases de datos para crear entradas de tablas de enrutamiento que prefieran la ruta más corta"[60].

A continuación, se presenta una comparación acerca de las características de OSPFv3 y OSPFv2:

- OSPFv3 se amplia de OSPFv2 con el fin de proporcionar soporte para el enrutamiento IPV6.
- OSPFv3 permite obtener un mayor tamaño de direcciones IPV6.
- Para el proceso de enrutamiento se debe activar la configuración de OSPFv3 sobre una interfaz asociada.
- En OSPFv3 cada interfaz debe ser activada utilizando comandos sobre el modo de configuración de la interfaz.
- En IPV6 los usuarios pueden configurar varias direcciones sobre una interfaz. En OSPFv3 se incluyen todas las direcciones en una interfaz por defecto.
- A diferencia de OSPFv2 se puede ejecutar varias instancias de OSPFv3 en un solo enlace.[61]

4.1.5.3 BGP-4. La función de este protocolo es intercambiar información de enrutamiento entre sistemas autónomos de tal forma que garantiza la elección de una ruta libre de loops.

---

[60] STAKY, "CCNA 1 and 2". Versión 3.1 Curriculum en formato pdf, (n.d), p.219.

[61] Cisco Systems, Inc. (2003-211). "Implementing OSPF for IPv6", Obtenida el 24 de julio de 2016. Disponible en http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-ospf.html#wp1069815.

A continuación, se señalan algunas de las características de este protocolo:

- BGP es uno de los principales protocolos de publicación de rutas más utilizados por las compañías e ISP's en Internet.
- BGP toma decisiones de enrutamiento basadas en las políticas o reglas de una red.
- La relación entre *routers* BGP se mantiene con el envío de paquetes cada 60 segundos.

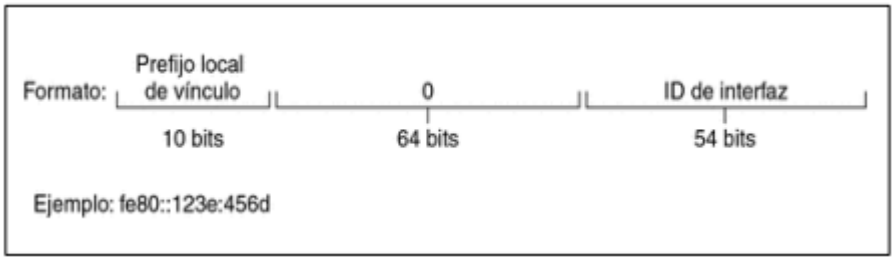
4.1.6 Direccionamiento IPv6. Las direcciones pasan de los 32 a 128 bits, es decir de 2^{32} direcciones (4.294.967.296) a 2^{128} direcciones (3.402823669 e38). Durante las investigaciones realizadas acerca del direccionamiento en IPv6, Ramos (2011, p.13) afirma que existen tres tipos de direcciones:

4.1.6.1 Direcciones *Unicast* o unidifusión. Este tipo de direcciones permite identificar una sola interfaz, es decir cuando un paquete es enviado a una dirección *unicast* éste será entregado solo a la interfaz identificada con dicha dirección.

A continuación, se describen los tipos de direcciones *unicast*:

1. ***Link Local* o Local de enlace**. Éste tipo de direcciones permite identificar interfaces en un mismo enlace de red local. Se utiliza en los procesos de descubrimiento de vecinos y siempre se configura de forma automática.

Figura 9. Partes de una dirección local de enlace



Fuente: ORACLE, (2010), Capitulo 3. "Introducción a IPv6", Obtenida el 24 de julio de 2016. Disponible en: http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-7/index.html

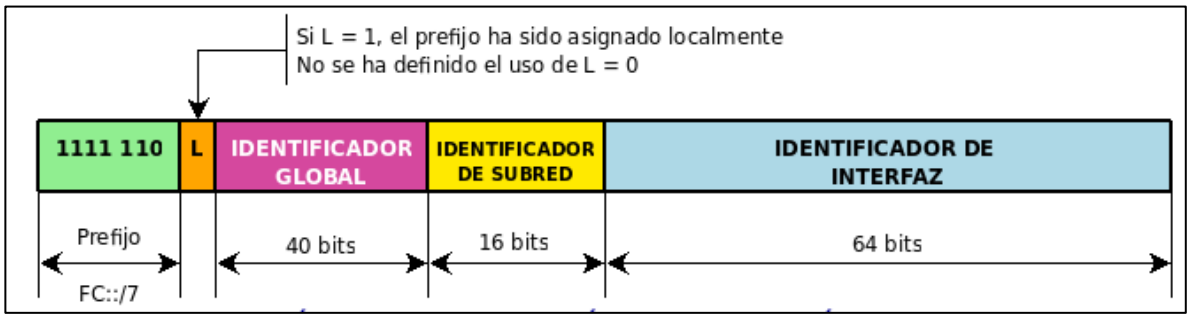
Como se puede observar en el ejemplo de la Figura 9 las direcciones Locales de enlace siempre comienzan por fe80.

- Prefijo local de vínculo: representa fe80::ID_Interfaz /10

• ID_Interfaz: dirección hexadecimal de la interfaz, que en general se deriva de la dirección física de 48 bits.

2. **Local de sitio o local única**. Éste tipo de direcciones permite identificar interfaces en un mismo sitio. El ámbito de una dirección local de sitio es el mismo sitio (conjunto de redes de la organización). Cuando se definió la dirección de enlace local se hizo lo propio con la llamada "Dirección de Sitio Local". Con el tiempo, ese último término fue sustituido por el de "Dirección Unicast Local Única" o simplemente "Dirección IPv6 Local". En inglés se suele usar el término ULA (*Unique Local Unicast Address*). Las partes que componen una dirección local de sitio se puede ver en la figura 10:

Figura 10. Partes de una dirección local de sitio



Fuente: "IPv6", (2011) Obtenida el 24 de julio de 2016. Disponible en: https://sites.google.com/site/tknikaipv6/2-direccionamiento/2-2-direccionamiento/2-2-5-direccion-unicast-local-unica

Las características de las Direcciones Unicast Locales Únicas son las siguientes:

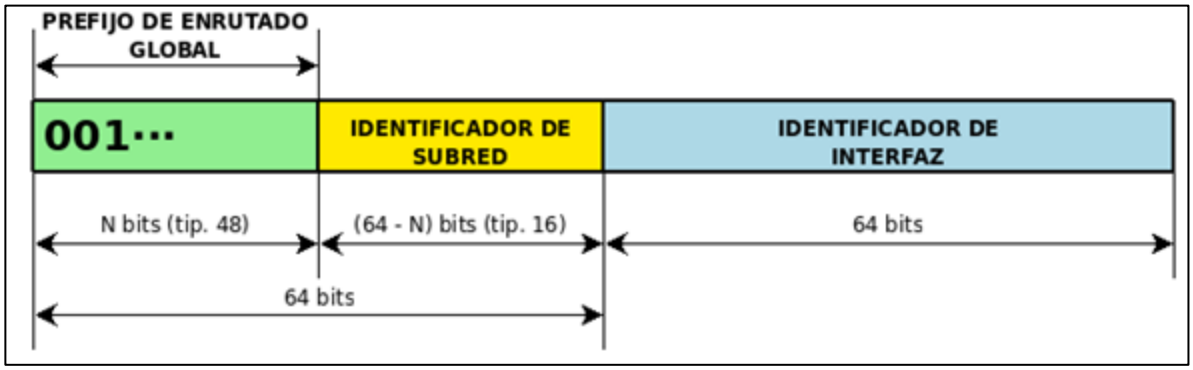
• Tienen un prefijo global único que facilita el filtrado en los límites de la red.
• Permiten la interconexión de redes privadas sin que haya riesgo de que surjan conflictos por direcciones duplicadas, lo cual implicaría la re-enumeración de una de las redes.
• No dependen de los ISP's.
• Se pueden usar en comunicaciones internas sin conexión a Internet.
• Si se enrutan accidentalmente a Internet, no surgen conflictos de direcciones
• Pueden ser utilizadas por las aplicaciones del mismo modo que utilizan las direcciones unicast globales.

Como se puede observar en la Figura 10, el bit L puesto a 1 indica que la administración del prefijo es local. Por ello, siempre que la administración sea local, el prefijo será FD::/8 (1111 1101). Y esto está relacionado con el siguiente bloque de 40 bits, el "Identificador Global". Cuando la administración es local, este Identificador Global se crea aplicando un algoritmo pseudo-aleatorio, que garantiza con una probabilidad altísima su exclusividad.

3. **Global**.[62] Éste tipo de direcciones permite identificar interfaces en el internet cuyo equivalente son las direcciones públicas en IPv4. Puesto que van a ser direcciones válidas a nivel global es lógico pensar que deben estar controladas como lo están las IP's públicas de IPv4, más adelante se puede comprobar que es así.

Todas las Direcciones Unicast Globales tienen 001 en sus tres bits de mayor peso, por lo que el prefijo es 2000::/3. Esto indica que si la dirección empieza tanto por 0010 (0x2) como por 0011(0x3), estaremos ante una dirección unicast global. En el RFC 4291 se define el formato de estas direcciones. La estructura de una dirección global se puede observar en la figura 11.

Figura 11. Estructura de la dirección Unicast Global



Fuente: "IPv6", (2011) Obtenida el 24 de julio de 2016. Disponible en: https://sites.google.com/site/tknikaipv6/2-direccionamiento/2-2-direccionamiento/2-2-3-direcciones-unicast-globales

Como se puede ver en la figura 11, los 128 bits de la dirección se descomponen en tres campos:

Prefijo de enrutado global (N bits). Éste prefijo limita el rango de direcciones asignado al sitio. Para redes de tamaño pequeño y medio suele constar de 48 bits y es gestionado por los servicios de registro internacionales (IANA) y los ISPs.

Identificador de subred ((64 – N) bits). El ID de Subred identifica un enlace dentro de un sitio. Puesto que normalmente N = 48 bits, quedan un total de 16 bits para hacer subredes en la organización. Es decir, una vez obtenido el prefijo de enrutado global, la organización puede descomponerse en 65.535 subredes.

[62] IPv6 @ Tknika. (2011). "Sitio Wiki del proyecto de IPv6 de Tknika". Obtenido el 25 de julio de 2016. Disponibile en: https://sites.google.com/site/tknikaipv6/

Lógicamente, la gestión de este identificador es responsabilidad del administrador local.

En caso de que la organización sea muy grande, puede solicitar un prefijo de enrutado global de menos de 48 bits, de modo que pueda disponer de más espacio para crear subredes.

Identificador de Interfaz (64 bits). El Identificador de Interfaz identifica una interfaz en una subred y debe ser único dentro de la misma. Este identificador se puede configurar de varias maneras:

- Configuración estática (Manual).
- Autoconfiguración (Identificador de Interfaz basado en EUI-64).
- Configuración dinámica (DHCPv6).
- Identificador de Interfaz Pseudo-Aleatorio.
- Identificador generado criptográficamente.

En el caso de la autoconfiguración EUI-64 (EUI = *Extended Unique Identifier*), se consigue un identificador de interfaz único que se basa en la dirección MAC de la propia interfaz (de ahí su exclusividad).

4.1.6.2 Direcciones *Anycast*. Éste tipo de direcciones permiten identificar un grupo de interfaces, es decir cuando un paquete es enviado a una dirección *anycast* este será entregado a cualquiera de las interfaces identificadas con dicha dirección.

4.1.6.3 Direcciones *Multicast*. Las cuales permiten identificar un grupo de interfaces, es decir cuando un paquete es enviado a una dirección *multicast* este será entregado a todas las interfaces identificadas por dicha dirección.

4.1.7 Representación de direcciones IPv6. Una dirección IPv6 tiene un tamaño de 128 bits y se divide en 8 campos de 16 bits, en donde cada bloque se convierte a un número hexadecimal de 4 dígitos o nibble separado por un signo de dos puntos.

Ejemplo: 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

A continuación, se presentan las formas de representar una dirección IPv6:

- Se puede eliminar los ceros iniciales de cada bloque de 16 bits, pero cada bloque debe tener al menos un dígito.

Por ejemplo: 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

Se puede representar como: 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

• Cuando una dirección contiene varios grupos de ceros se puede reemplazar por el símbolo “::”.

Por ejemplo: FE1A:4CB9:001B:0000:0000:12D0:005B:06B0

Se puede representar como: FE1A:4CB9:1B::12D0:5B:6B0

Nota: La compresión de ceros se puede utilizar una sola vez en una dirección dada.

• Cuando existe un escenario con nodos IPv4- IPv6 la dirección queda de la siguiente forma:

Ejemplo: 0000:0000:0000:0000:0000:0000:192.168.10.1

- Donde los ceros representan valores hexadecimales de 16 bits cada una.
- Los últimos bytes representan valores decimales de 8 bits cada una.

La dirección IP descrita en la parte superior se puede representar como:

::192.168.10.1

4.1.7.1 Prefijos IPv6. Un prefijo es una parte de la dirección que indica los bits que tienen valores fijos o los bits del identificador de red. Un prefijo de dirección IPv6 se representa como: **Dirección IPv6/Longitud de prefijo**.

Ejemplo: 21DA:D3:0:2F3B::/64

4.1.8 Ventajas y desventajas de IPv6.[63]

4.1.8.1 Ventajas del protocolo IPv6. Según el Autor Iván Ramos (2011, p.10) las desventajas del protocolo IPV6 son las siguientes:

• Permite obtener direcciones más largas debido a que el tamaño de una dirección cambia de 32 a 128 bits, con un espacio disponible tan grande que no puede llegar a agotarse en un futuro previsible.

[63] RAMOS, Ivan. Op. Cit. p. 17

• Contiene un formato de cabecera flexible, es decir que utiliza un nuevo formato de datagrama que a diferencia de IPv4 utiliza un formato con un número fijo de octetos, IPv6 utiliza un conjunto opcional de cabeceras.
• Permite la fragmentación *end-to-end*, es decir que a todos los enrutadores se les elimina la función de fragmentar los paquetes que llegan debido al MTU.
• Permite un soporte para la reserva de recursos debido a que IPv6 reemplaza la especificación del tipo de recursos de IPv4 utilizando un mecanismo que permite la reserva de los recursos de red. Este mecanismo tiene la capacidad de soportar aplicaciones de video en tiempo real, cuyo requerimiento es garantizar el ancho de banda.
• Permite la provisión de extensiones al protocolo, debido a que se produce un desplazamiento de un protocolo a otro permitiendo características adicionales. Este tipo de capacidad de extensión permite que el protocolo se adapte a los cambios en el hardware de la red o las nuevas aplicaciones.
• Permite un número de saltos, es decir cuando se cambia el tiempo de vida de un paquete IPv4 por el número de saltos en IPv6 se garantiza que el paquete no será eliminado sin que tenga la opción de llegar hasta el nodo de destino.

4.1.8.2 Desventajas del protocolo IPv6. Ramos (2011, p.10) afirma que los principales problemas que se presentan en IPV6 son los siguientes:

• El restablecimiento de la comunicación cuando un enlace se cae entre un par en enrutadores, de esta forma se afectan los siguientes factores:
- El Tamaño de los fragmentos de acuerdo al mínimo MRU.
- El Ancho de banda específico para esa comunicación.
- El Retardo aceptable en la transmisión.
• La transición de IPv4 a IPv6 debido a la tecnología actual y a la gran cantidad de nodos con soporte IPv4 que existen en el mundo.
• La tecnología de enrutamiento exige que se utilicen buenas estrategias, debido a que no se podría eliminar en un solo día toda la cantidad de enrutadores que funcionan con IPv4. Además, se deben crear nodos que soporten tanto IPv4 como IPv6 hasta cuando todos los nodos puedan llegar a comunicarse con la misma versión de IP.

4.1.9 Mecanismos de transición. Una de las premisas del diseño de IPv6, fue que pudiera realizarse una transición suave hacia la nueva versión del protocolo IP, sin que fuera necesario pasar de una versión a otra en forma abrupta. Con esta idea en mente, se diseñaron muchos mecanismos que pudieran ayudar a la convivencia entre ambas versiones.

Si bien en un comienzo se pensó que la adopción gradual de IPv6 crecería lo suficiente como para ir desplazando a IPv4 antes de su agotamiento, esto no

sucedió así, razón por la cual estos mecanismos de transición tienen hoy en día una relevancia incluso mayor.

Podemos hacer una clasificación general entre los mecanismos de transición de acuerdo al tipo de técnica que se utiliza:

• Dual stack
• Túneles
• Traducción

También es posible hacer una división entre los mecanismos de transición según estén basados en una infraestructura mayoritariamente IPv4 o IPv6: si bien en un comienzo teníamos redes IPv4 que iban incorporando el acceso a IPv6 gradualmente, a medida que el agotamiento de IPv4 se extiende, los proveedores comienzan a pensar en redes de acceso exclusivamente IPv6, con lo cual es necesario suministrar mecanismos que permitan continuar accediendo a aquellas redes que sólo poseen IPv4.

Existe una gran variedad de mecanismos de transición propuestos y muchos de ellos están actualmente en discusión en la IETF. Se describen a continuación los principales y a los que se considera más maduros.

NAT64/DNS64: Esta técnica permite tener una red sólo IPv6 y mediante una traducción poder mantener la conectividad con la Internet sólo IPv4. De esta forma, la complejidad de administración se simplifica al sólo tener que administrar una red IPv6-only. Las conexiones IPv6 son nativas, por lo que a medida que el despliegue de IPv6 crece en el mundo, el costo de esta solución no se incrementa.

464XLAT: Se basa en la técnica anterior, pero introduce una doble traducción para los casos en que se necesite utilizar una aplicación que no soporta IPv6. Esto soluciona algunos problemas de NAT64 y es una técnica muy adecuada para redes de celulares (móviles) ya que los sistemas Android ya la incorporan. También para montar datacenters IPv6-only.

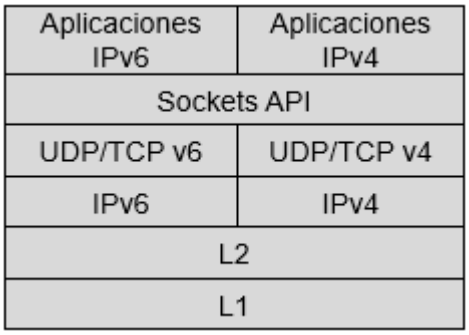
MAP-E y MAP-T: Son técnicas de transición similares a las anteriores pero que trabajan por compartición de puertos (A+P, ver RFC6346). MAP-T usa traducción para transportar el tráfico IPv4 mientras que MAP-E utiliza encapsulado (túneles).

4.1.9.1 Dual-Stack o doble pila (RFC 2893). En el esquema dual-stack, un nodo de red incorpora ambos protocolos (IPv4 e IPv6) apilados en paralelo (ver figura 3). Las aplicaciones IPv4 usan la pila IPv4, y las aplicaciones IPv6 usan la pila IPv6. Las decisiones de flujo de datos en el nodo están basadas campo “versión” de la cabecera IP para paquetes que son recibidos por capas inferiores – Un campo versión con valor “4” resulta en el paso de la unidad de dato del protocolo IP a la

capa IPv4 y con valor de “6” a la capa IPv6. Cuando se envían paquetes, el tipo de dirección de destino recibida de capas superiores determina la pila apropiada. Los tipos de direcciones típicamente viene de DNS lookups; la pila apropiada es escogida en respuesta a los tipos de registro DNS devueltos.

Muchos de los sistemas operativos comerciales ya proveen doble pila del protocolo IP. Por ejemplo, los sistemas operativos Microsoft Windows XP y Windows Server 2003 implementan la arquitectura en doble pila mostrada en la Figura 12, Windows Vista implementa lo que se denomina una pila (TCP/IP) de próxima generación que incorpora la arquitectura dual-stack, pero ambos IPv4 e IPv6 comparten en común las capas de transporte y framing, diferente a las capas de transporte mostradas en la figura 12. Consecuentemente, el mecanismo dual-stack está siendo ampliamente implementado como mecanismo de transición. Sin embargo, hay que tener en cuenta las pilas duales solo permiten comunicaciones entre aplicaciones de similar protocolo, es decir, IPv6 a IPv6 e IPv4 a IPv4.

Figura 12. Mecanismo de transición Dual-Stack en sistema final



Fuente: Handbook of IPv4 to IPv6 Transition. J. Amos

4.1.9.2 Tipo túnel. Este método permite transmitir paquetes IPv6 por medio de una infraestructura IPv4, es decir se encapsula el contenido del paquete IPv6 en un paquete IPv4.

Ramón Millán (2001, parte II) afirma que el nodo IPv6 que hace frontera con el túnel, toma el paquete IPv6, y lo pone en el campo de datos de un paquete IPv4. Este paquete IPv4 tiene como dirección de destino el nodo IPv6 en la parte final del túnel y es enviado al primer nodo IPv4 que conforma el túnel. Los nodos IPv4 del túnel encaminan el paquete, sin tener constancia de que el paquete IPv4 que están manejando contiene un paquete IPv6. Finalmente, cuando el paquete llega al extremo receptor IPv6 del túnel, este determina que el paquete IPv4 contiene un paquete IPv6 que debe ser extraído.

Los mecanismos de transición tipo túnel se dividen en 2 grupos:

• **Túneles manuales**: Un paquete IPv6 es encapsulado en un paquete IPv4 para ser encaminado sobre una infraestructura de enrutamiento IPv4, estos son los túneles punto a punto que necesitan ser configurados manualmente.

• **Túneles automáticos**: Los nodos IPv6 pueden utilizar diferentes tipos de direcciones compatibles con IPv4, IPv6 ó 6to4, el túnel automático es un túnel dinámico de paquetes IPv6 sobre una infraestructura de enrutamiento IPv4. La configuración de los túneles entre *routers* y host se pueden realizar de diferentes formas:

1. *Router* a *Router:* utiliza un mecanismo de túnel automático en donde los *routers* IPv6/IPv4 que están separados por una infraestructura IPv4 pueden encapsular paquetes IPv6 entre ellos mismos.
2. *Host* a *Router:* utiliza un mecanismo de túnel automático en donde un host IPv6/IPv4 puede encapsular paquetes IPv6 a un *router* intermedio IPv6/IPv4 que es accesible mediante una infraestructura de ruteo IPv4.
3. *Host* a *Host:* utiliza un mecanismo de túnel manual en donde los host IPv6/IPv4 que están interconectados por una infraestructura IPv4 pueden encapsular paquetes IPv6 entre ellos mismos.
4. *Router* a *Host:* utiliza un mecanismo de túnel manual en donde los routers IPv6/IPv4 pueden encapsular paquetes IPv6 a su destino final.

4.1.9.3 De traducción. "Estas técnicas permiten un ruteamiento transparente de la comunicación entre nodos que sólo poseen soporte a una versión del protocolo IP, o que utilizan Doble Pila. Pueden operar de diversas formas o en capas distintas, traduciendo cabeceras IPv4 en cabeceras IPv6 y viceversa, realizando conversiones de direcciones de API (Aplication Program Interface) de programación, o actuando en el intercambio de tráfico TCP a UDP."[64]

[64] UTPL. SOTO, Gissella (2015). "Transición de IPv4 a IPv6" Obtenido el 25 de julio de 2016. Disponible en: http://dspace.utpl.edu.ec/bitstream/123456789/12614/1/Soto_Velasco_Gissella_Patricia.pdf

4.2 MARCO INSTITUCIONAL

4.2.1 IPv6 en el sector gobierno colombiano. Desde hace más de tres décadas, las redes de telecomunicaciones han estado creciendo exponencialmente generando mayor demanda de servicios y oportunidades en la red mundial de internet; con el aumento de las tecnologías computacionales y de comunicaciones, ha aumentado el proceso de innovación tecnológica en los diversos dispositivos tanto alámbricos como inalámbricos, que comenzaron a incrementar la conectividad en muchas redes en el mundo y para ello han tenido que hacerlo con direcciones de internet (IP) y ciertos mecanismos complementario que permiten establecer conexiones para cada elementos conectado a la red, que en estos momentos entraron a una fase de agotamiento final, así mismo en el año 1992 la Internet IETF a partir de diversos grupos de trabajo definió el RFC 2460 (Especificaciones del Protocolo Internet Versión 6 (IPv6) que dio origen al nuevo protocolo IPv6 o IPng (Next Generation Internet Protocol).

Para atender esta necesidad inminente de innovación tecnológica en el país, el MinTic, mediante un instrumento publicado, pretende proyectar los lineamientos necesarios para diagnosticar, sensibilizar, desarrollar e implementar el protocolo IPv6 en las entidades del estado, con el propósito de adoptar el nuevo esquema de funcionamiento de manera paralela con el actual protocolo IPv4, de conformidad con la Circular 002 de Julio de 2011, garantizando que las infraestructuras de hardware, software y servicios continúen operando normalmente en las distintas instituciones del país.

Así mismo, para entrar en el proceso de adopción de este nuevo protocolo, entre las recomendaciones impartidas por el MinTic están entre otras, realizar un inventario de los activos de información, revisar su actual infraestructura de computación y de comunicaciones, validar todos los componentes de hardware y software de que se disponga, revisar los servicios que se prestan, los sistemas de información, revisión de estándares y políticas para conocer el impacto de adopción de la nueva versión del protocolo IP, a fin de facilitar las labores de planeación e implementación de IPv4 a IPv6, garantizando que las operaciones continúen funcionando normalmente dentro de las entidades del estado.

4.2.2 Acerca de la entidad. La institución, es una entidad Pública del Orden Nacional con personería jurídica, autonomía administrativa y patrimonio independiente, perteneciente al Sistema Nacional de Ciencia y Tecnología, adscrita al Ministerio de Agricultura y Desarrollo Rural.

Ésta tiene la jurisdicción en todo el territorio nacional, siendo su domicilio principal la ciudad de Bogotá, D.C., cuenta con 32 Gerencias Seccionales, una por departamento.

La entidad diseña y ejecuta estrategias para, prevenir, controlar y reducir riesgos sanitarios, biológicos y químicos para las especies animales y vegetales, que puedan afectar la producción agropecuaria, forestal, pesquera y acuícola de Colombia. Además, adelanta la investigación aplicada y la administración, investigación y ordenamiento de los recursos pesqueros y acuícolas, con el fin de proteger la salud de las personas, los animales y las plantas y asegurar las condiciones del comercio.

Sus acciones se orientan a lograr una producción agropecuaria competitiva, con el fin de aportar al logro de los objetivos de la Apuesta Exportadora de Colombia. Realiza inspección y control de productos agropecuarios, animales y vegetales en los pasos fronterizos, aeropuertos y puertos. Además, es responsable de las negociaciones de acuerdos sanitarios y fitosanitarios bilaterales o multilaterales que permiten la comercialización de los productos agropecuarios en el exterior y mediante los cuales se busca garantizar el crecimiento de las exportaciones.
De igual manera, el instituto tiene la responsabilidad de garantizar la calidad de los insumos agrícolas y las semillas que se usan en Colombia, al tiempo que reglamenta y controla el uso de organismos vivos modificados por ingeniería genética para el sector agropecuario.

La institución, actualmente se encuentra en un proceso de cambio e innovación tecnológica, cuya implementación final contribuirá al cumplimiento de los objetivos misionales y a la efectividad en la respuesta a los requerimientos y necesidades de los usuarios.

Teniendo en cuenta el constante desarrollo tecnológico al que el mundo se enfrenta, la entidad desea posicionarse en materia de tecnología e informática; con el fin de adquirir nuevas y mejores herramientas que permitan ejecutar los procesos de una manera más eficiente, brindando un servicio de calidad al usuario final. Esta necesidad de mejorar la comunicación entre la ENTIDAD – USUARIO y viceversa, requiere la intervención del campo tecnológico, lo cual es un punto de apoyo en el proceso de certificación de calidad.

5. DISEÑO METODOLÓGICO

5.1 TIPO DE INVESTIGACIÓN

Este trabajo de grado sigue los lineamientos del tipo de investigación de **Estudio Explicativo**.

5.2 HIPÓTESIS DE INVESTIGACIÓN

El desarrollo estructurado y sistemático de la etapa de planeación del proceso de adopción de IPv6 en la infraestructura tecnológica y de comunicaciones de la entidad adscrita al ministerio de agricultura repercute en el nivel de éxito del desarrollo de las fases de implementación y pruebas sin que existan interrupciones en los servicios y sistemas de información con los que cuenta la organización.

5.3 HIPÓTESIS NULA

El desarrollo estructurado y sistemático de la etapa de planeación del proceso de adopción de IPv6 en la infraestructura tecnológica y de comunicaciones de la entidad adscrita al ministerio de agricultura no influye en el nivel de éxito del desarrollo de las fases de implementación y pruebas sin que existan interrupciones en los servicios y sistemas de información con los que cuenta la organización.

5.4 VARIABLES

5.4.1 Variables independientes

- Planeación del proceso de adopción de IPv6
- Interrupciones en los servicios y sistemas de información

5.4.2 Variables dependientes

- Nivel de éxito del desarrollo de las fases de implementación y monitoreo

6. FASES PARA LA ADOPCIÓN DE IPv6

Teniendo en cuenta el contexto y alcance del presente proyecto de grado, se presenta a continuación la metodología que sería adoptada para llevar a cabo el proyecto de implementación en su totalidad en la entidad, destacando las actividades sugeridas para desarrollar en cada una de sus fases y los productos obtenidos como resultado de éstas.

6.1 FASE 1: PLANEACIÓN DE IPv6

La fase de planeación representa una etapa crítica e importante del proceso de transición por cuanto comienza con la definición y ejecución del plan de diagnóstico de la infraestructura de TI de la entidad. Las siguientes son las actividades a tener en cuenta en esta fase:

- Elaborar y validar el inventario de activos de Información de servicios tecnológicos y su interrelación entre ellos. Para esta actividad se requiere desarrollar y mantener el inventario de hardware y software, identificando claramente cuáles equipos soportan IPv6, cuales requieren actualizarse y cuáles no soportan el nuevo protocolo, dejando la respectiva documentación en constancia al momento de optar hacia IPv6.
- Analizar, diseñar y desarrollar el plan de diagnóstico del protocolo IPv4 a IPv6 en la red de la entidad.
- Identificar la topología actual de la red y su funcionamiento dentro de la organización.
- Evaluar el grado de afinamiento del protocolo IPv6 a nivel de hardware y software con miras a preparar la nueva infraestructura de red.
- Generar el plan detallado del proceso de transición de esta fase hacia IPv6.
- Planear la migración de los siguientes servicios tecnológicos: Servicio de Resolución de Nombres (DNS), Servicio de Asignación Dinámica de Direcciones IP (DHCP), Directorio Activo, Servicios WEB, Servidores de Monitoreo, Validación del Servicio de Correo Electrónico, Validación del Servicio de la Central Telefónica, Servicio de *Backups*, Servicio de Comunicaciones Unificadas e Integración entre Sistemas de Información; así mismo revisar los procedimientos de implementación de estos servicios y las aplicaciones identificadas en esta fase, con base en los estándares de la RFC de IPv6.
- Validar el estado actual de los sistemas de información, los sistemas de comunicaciones y evaluar la interacción entre ellos cuando se adopte el protocolo IPv6.

- Dentro del proceso de diagnóstico presentar cuales equipos de computación y de comunicaciones soportan IPv6 (IPv6-ready o IPv6-web), cuales requieren actualizarse y cuáles no se pueden implementar a IPv6.
- Identificar la configuración y los esquemas de seguridad de la red de comunicaciones y sistemas de información.
- Revisar las políticas de enrutamiento para IPv6 entre los segmentos de red internos, previa evaluación de los mismos.
- Para la construcción del plan de diagnóstico, que es el pilar fundamental de esta fase I, se requiere la realización de una validación previa de la infraestructura tecnológica que permita medir el grado de avance en la adopción del protocolo IPv6; dentro de dicha validación es necesario revisar el grado de compatibilidad del protocolo IPv6 con la infraestructura de la entidad de tal manera que la información recogida de esta tarea sea insumo para la acometida de la segunda fase que es la implementación de IPv6.
- Establecer el protocolo de pruebas para la validación de aplicativos, equipos de comunicaciones, plan de seguridad y coexistencia de los protocolos IPv4 e IPv6.
- Establecer los acuerdos de confidencialidad que sean necesarios sobre el tratamiento de la información ante terceros.
- Capacitar a funcionarios del área de TI de la entidad, de conformidad con los planes de capacitación establecidos, en el protocolo IPv6 y establecer la sensibilización a las personas de toda la organización a fin de dar a conocer el nivel de impacto del nuevo protocolo.

6.1.1 Productos de esta fase.

- Plan de trabajo para la adopción de IPv6
- Plan de diagnóstico que debe contener los siguientes componentes:
  - Inventario de TI (Hardware y software)
  - Informe de la infraestructura de red de comunicaciones
  - Recomendaciones para adquisición de elementos de comunicaciones, de computo o almacenamiento con el cumplimiento de IPv6
  - Plan de direccionamiento en IPv6
  - Plan de manejo de excepciones, en la que se definen las acciones necesarias en cada caso particular con aquellos elementos de hardware y software (aplicaciones y servicios) que sean incompatibles con IPv6
  - Informe de preparación (*readiness*) de los sistemas de comunicaciones, bases de datos y aplicaciones
- Documento que define los lineamientos al implementar la seguridad en IPv6 en concordancia con la política de seguridad de la entidad.
- Plan de capacitación en IPv6 a los funcionarios del área de TI de la entidad y plan de sensibilización al total de funcionarios de otras áreas.

6.2 FASE 2: IMPLEMENTACIÓN DE IPv6

De acuerdo a la planificación definida en la fase anterior, se realizará el despliegue de validaciones, configuraciones, actualizaciones, rediseños y todas las demás actividades necesarias para crear el ambiente de transición y coexistencia de IPv4 e IPv6 en la infraestructura tecnológica de la entidad. Entre otras estas son las actividades a tener en cuenta durante esta fase:

- Habilitar el direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo con el plan de diagnóstico de la primera Fase del proceso de transición de IPv4 a IPv6 y teniendo en cuenta el inventario de los activos de información realizado.
- Iniciar el proceso de transición usando la metodología *Dual-Stack*, permitiendo que coexistan los dos protocolos IPv4 e IPv6 y la transición en doble pila.
- Definir y poner en ejecución un piloto de pruebas, que incluya la simulación de la red de comunicaciones agregándole carga, servicios y usuarios finales que permitan detectar fallas y poder corregir configuraciones.
- Realizar el diseño de la nueva topología de red con base en los lineamientos del nuevo protocolo IPv6 en modo *Dual-Stack*.
- Implementar y validar la funcionalidad de los servicios y aplicaciones de la entidad sobre IPv6: DNS, DHCP, Directorio Activo, Servicios Web, Correo Electrónico, Telefonía, Servicios de Almacenamiento y *Backup*, VPN, Integración entre sistemas de información, etc.
- Con base en los lineamientos definidos en los RFCs de seguridad en IPv6, se activarán las políticas previamente establecidas para IPv4 en los equipos de seguridad y comunicaciones que posee la institución (Firewall, Servidores AAA, equipos perimetrales, entre otros).
- Informar y mantener un trabajo coordinado con el proveedor de servicios de internet para establecer la conectividad integral en IPv6 desde el interior de las redes LAN hacia las redes WAN a fin de garantizar que la entidad pueda generar tráfico IPv6 con normalidad.

6.2.1 Productos de esta fase.

- Informe del plan detallado de implementación del nuevo protocolo.
- Documentación con todas las configuraciones del nuevo protocolo realizadas en las plataformas de hardware, software y servicios que se han intervenido durante la fase.

- Informe de resultados de las pruebas realizadas a nivel de comunicaciones, de aplicaciones y sistemas de almacenamiento.

6.3 FASE 3: PRUEBAS

Con la finalidad de verificar que la implementación de IPv6 en la entidad es funcional y permite la continuidad operativa de los sistemas de información y de los servicios ofrecidos por la entidad, se realizaran las actividades relacionadas a continuación:

- Realizar un protocolo de pruebas y monitoreo de la funcionalidad de IPv6 en los sistemas de información, de almacenamiento, de comunicaciones y servicios tecnológicos de la entidad en un ambiente que permita empezar a generar tráfico IPv6 de la entidad hacia internet y viceversa.
- Probar y verificar la funcionalidad del nuevo protocolo frente a las políticas de seguridad perimetral, de servidores de computo, servidores de comunicaciones y equipos de comunicaciones con los que cuenta el instituto.
- Durante la etapa de pruebas se realizará una verificación y afinamiento de las configuraciones de hardware, software y servicios ofrecidos por la entidad, con base en la información resultante de la fase II.
- Elaborar un inventario final de los servicios, aplicaciones y sistemas de comunicaciones bajo el nuevo esquema de funcionamiento de IPv6.

6.3.1 Productos de esta fase.

- Documento con los cambios detallados de las configuraciones realizadas, previo al análisis de funcionalidad realizado en la fase II.
- Acta de cumplimiento a satisfacción de la entidad con respecto al funcionamiento de los servicios y aplicaciones que fueron intervenidos durante la fase II.
- Documento de inventario final de la infraestructura de TI sobre el nuevo protocolo de IPv6.

6.4 EL PASO A SEGUIR

Como se pudo observar, …el numeral 6.1 … hace referencia a la fase de planeación la cual en próximos capítulos será desarrollada con la finalidad de establecer estructuradamente como se llevará a cabo la implementación y pruebas del

proyecto correspondiente a las fases 2 y 3. Aunque se ha realizado un análisis integral de toda la infraestructura tecnológica que posee la institución, desde el nivel central hasta cada una de las seccionales en el país que la componen, en los siguientes capítulos se centraran en desarrollo de la planeación para la red del nivel central en la ciudad de Bogotá. Dentro de esta planeación se ha determinado realizar una implementación para la adopción del protocolo en **3 etapas** específicas para diversos componentes de la red central considerando las actividades y factores técnicos, económicos y humanos necesarios. …En el capítulo 7 … se explica detalladamente cada una de dichas etapas del proceso de implementación.

7. DESARROLLO DE LA FASE 1: PLANEACIÓN DE IPv6

Robbins, (2010) opina que “la planeación abarca la definición de las metas de una organización, el establecimiento de una estrategia general para lograr esas metas y el desarrollo de una jerarquía amplia de los planes para integrar y coordinar las actividades. Se relaciona, por lo tanto, con los fines (qué debe hacerse) así como también con los medios (cómo debe hacerse)”[65].

En ese sentido, con el visto bueno de la dirección del proyecto, la estrategia seleccionada dentro de lo planeado para lograr las metas deseables cuando se esté desarrollando la fase de implementación es llevar un despliegue del proceso por etapas delimitadas por los diferentes componentes de la red, con esto es posible evitar el sobredimensionamiento de actividades y el control de sus recursos asociados, además permite medir en corto y mediano plazo los resultados de cada meta trazada con miras a redefinir y optimizar las tareas planificadas en próximas etapas. A continuación, se explican los planes definidos y la dinámica que seguirá la fase de implementación en cada una de sus **3 etapas**.

7.1 PLANEACIÓN DE ETAPAS PARA LA IMPLEMENTACIÓN

7.1.1 Primera etapa (IPv6 en fronteras de red): Inicialmente se ha determinado desplegar el protocolo IPv6 en coexistencia con IPv4 en la entrada/salida a otras redes como internet, incluyendo la habilitación del stack IPv6 en servidores de aplicaciones web que actualmente ofrece la institución. Teniendo en cuenta que la entidad realiza anualmente contratación de proveedores de servicios de internet, se realizara un trabajo mancomunado con el proveedor de turno para las actualizaciones, configuraciones y habilitación de IPv6 en los equipos de borde (routers). Los elementos de red tenidos en cuenta para esta etapa y a los que se debe habilitar el Dual-Stack son:

- Firewall
- Router de borde
- Servidores Web

Las actividades programadas, el tiempo y recursos asociados en esta etapa se describen …en el anexo A … (cronograma de actividades). El tiempo estimado para puesta en marcha y evaluación es de **7 meses y 14 días**.

---

[65] ROBBINS, Stephen P. COULTER, Mary. “Administración”, 10ª edición. México: Pearson, 2010

7.1.2 Segunda etapa (IPv6 en la LAN del nivel central): Una vez superado el tiempo de maduración necesario en la primera etapa respecto a la disponibilidad de servicios y la generación de tráfico IPv6 hacia internet, se realizará el despliegue hacia la red LAN del edificio de oficinas nacionales, considerando todos los elementos de red requeridos para generar tráfico IPv6 en la red local. Similar a lo mencionado en el parágrafo anterior, las actividades programadas, el tiempo y recursos asociados en esta etapa se describen …en el anexo A … (cronograma de actividades fase de implementación). Para esta etapa se requiere la configuración y puesta en marcha del mecanismo dual-stack en los siguientes elementos de red:

- Switch Core
- Switches de acceso en cada piso
- Access Points
- Equipos de cómputo de usuarios
- Teléfonos IP

El tiempo estimado para puesta en marcha y evaluación es de **8 meses y 12 días**, esta cifra de tiempo se pudo obtener con base en lo establecido en el cronograma de las actividades definidas en cada etapa …véase anexo A ...

7.1.3 Tercera etapa (IPv6 en enlaces WAN con oficinas principales): Finalmente para lograr una cobertura casi total de la adopción del protocolo en la red de la institución, al igual que en la primera etapa, se requerirá al proveedor de conectividad y transporte de red desplegar las configuraciones necesarias en los gateways de cada oficina seccional en los diferentes departamentos del país (32 en total) de manera que dentro del enlace actual sobre la MPLS se tenga conectividad mediante IPv4 e IPv6. En esta etapa será necesario la habilitación de IPv6 en los siguientes equipos:

- Routers de seccionales (gateways)
- Router de datos del headquarter

Tiempo estimado para puesta en marcha y evaluación: 11 meses y 2 días. Dicho tiempo es el de mayor duración, sin embargo, es posible que se extienda un poco más, teniendo en cuenta la cantidad de nodos interconectados en el enlace. Similar a los anteriores tiempos estipulados, para su estimación se tuvo en cuenta lo descrito …en el anexo A …

No obstante lo anterior, para que el proceso por etapas se realice adecuadamente es importante poder conocer el estado y actualidad de la red de la entidad realizando un levantamiento de información y un diagnóstico de los activos tecnológicos frente

a IPv6, con lo cual se puede identificar el nivel de afinidad de los elementos de red con el nuevo protocolo, lo que influye en la estimación de recursos técnicos y económicos necesarios para llevar a cabo lo requerido. Para dicho diagnóstico fueron tenidos en cuenta la totalidad de los activos tecnológicos de la entidad, sin embargo, es impórtate recalcar que el enfoque dado en el desarrollo de la planeación corresponde lo evidenciado en el nivel central de la institución.

7.2 DIAGNOSTICO DE LA RED

Como resultado del proceso de recolección de información en el diagnóstico realizado a los activos de información (hardware y software) con los que cuenta la entidad, se presenta a continuación los aspectos relevantes caracterizados y validados por cada componente y las observaciones que se deben tener en cuenta para las futuras fases del proceso de adopción de IPv6.

7.2.1 Topología de red. Como se mencionó anteriormente, el instituto posee conectividad con todas sus sedes a nivel WAN a través de un proveedor de servicios de internet MPLS, cada seccional tiene además oficinas locales ubicadas en municipios aledaños en cada departamento del país que no hacen parte de la red WAN y que acceden a internet y a los servicios tecnológicos del instituto a través de conectividad con servicios banda ancha.

Referente al edificio de la oficina principal en la ciudad de Bogotá en donde está ubicado el *datacenter*, se cuenta con una red LAN con topología en estrella compuesta por las tres capas básicas de distribución, acceso y *core*, el edificio cuenta con 5 pisos cada uno con su cuarto de telecomunicaciones, su cableado horizontal en cobre, *backbone* vertical en fibra óptica y acceso inalámbrico a la red. La red esta segmentada en VLANs para las subredes de datos, dentro de las cuales están las diferentes dependencias, impresoras, VoIP, red inalámbrica y servidores. La anterior información se describirá con mayor detalle más adelante.

En el cuadro 1, se explican cuáles son los elementos principales por los que está conformada la red principal a nivel de equipos activos desde el *headquarter* hasta los enlaces establecidos con cada seccional.

Cuadro 1. Equipos activos en la red de oficina principal

Servicio	Dispositivo principal	Uso principal
Red de área local (LAN) alámbrica	*Switch*	Conexión de PC's, teléfonos, impresoras, servidores

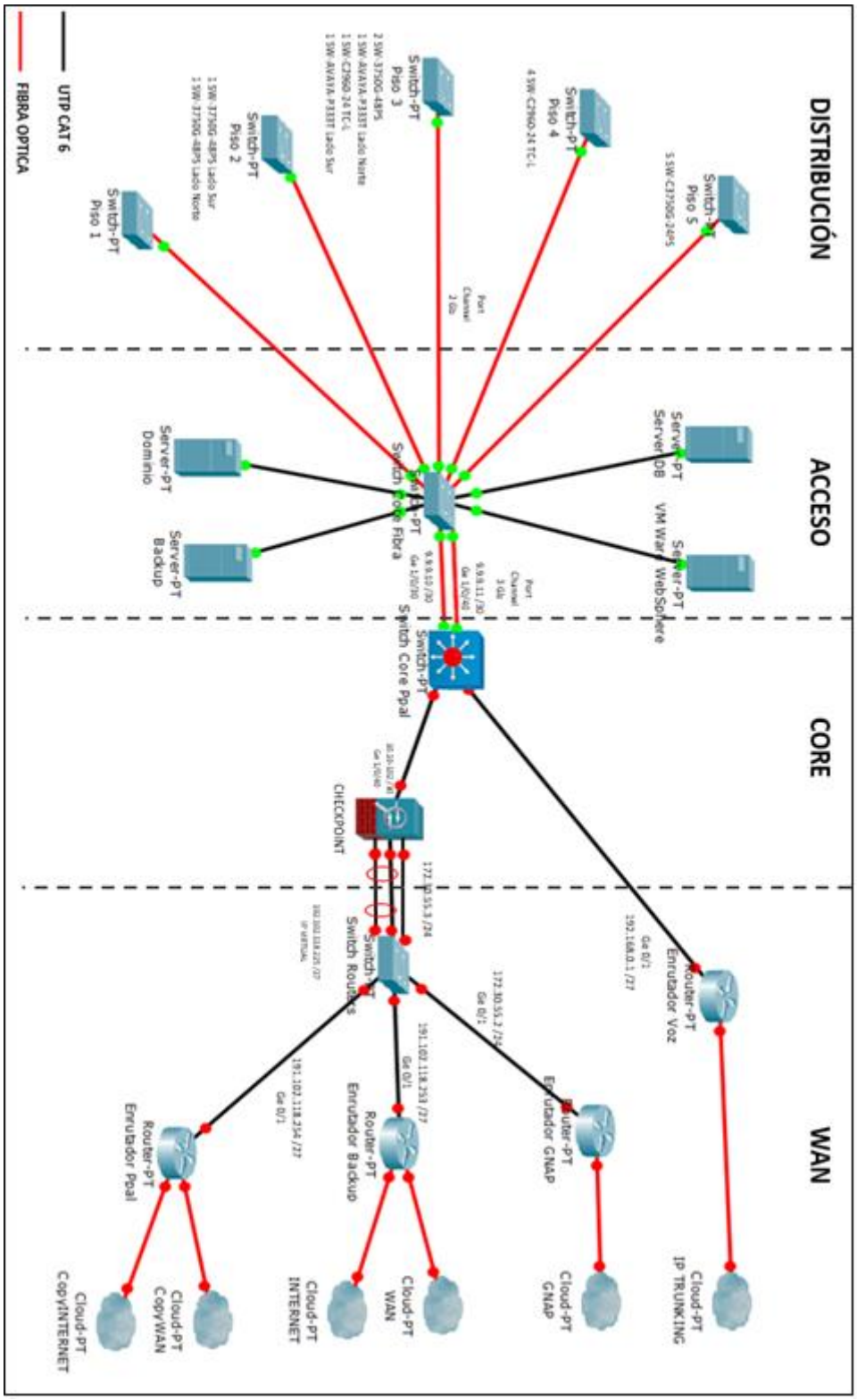
Cuadro 1 (Continuación)

Servicio	Dispositivo principal	Uso principal
Conectividad alámbrica segura en la LAN	Puntos de acceso alámbricos (APs)	Conexión de laptops
Conexión segura a internet	*Firewall*	Acceso seguro de entrada y salida a internet
Conexión a otras redes	*Router internet*	Proporciona acceso de entrada y salida a internet (ISP)
Conexión a oficinas remotas	*Router* de datos	Permite la extensión de la red LAN mediante MPLS
Fuente: Elaboración propia		

Adicionalmente toda la red a nivel nacional se encuentra administrada y controlada desde las oficinas principales a través de software especializado para el monitoreo de enlaces WAN, sin embargo, los eventos de incidentes o fallas detectadas en los nodos de cada seccional se reportan directamente al proveedor de conectividad quien es el encargado de brindar las acciones preventivas y correctivas necesarias.

El esquema general de la red central de la entidad se puede visualizar en la figura 13, también, en la figura 14 se muestra geográficamente los diferentes nodos en cada seccional que permiten el acceso a la red principal. Adicionalmente, en los cuadros 2 al 14 se describen los detalles técnicos de cada componente de la red principal.

Figura 13. Diseño de red del nivel central



Fuente: Elaboración propia

Figura 14. Mapa general de nodos interconectados a la red

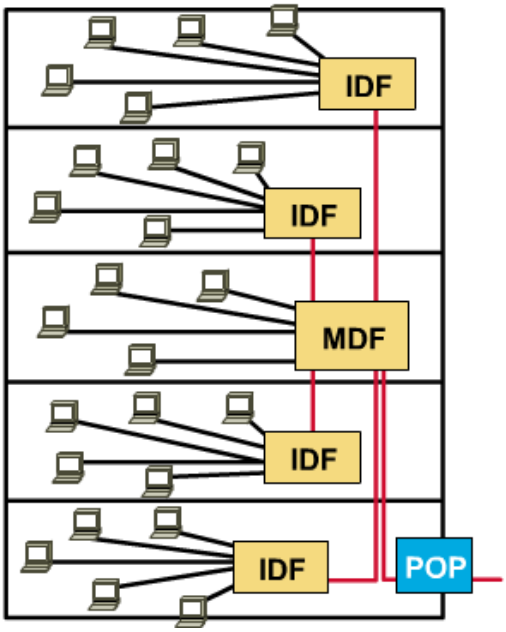
Fuente: Herramienta de monitoreo de canales de datos (SolarWinds)

Nota: Al tomar la imagen de la herramienta de monitoreo de canales, había nodos en estado *down* señalados con color rojo, los demás corresponden a los nodos en estado *up*.

7.2.1.1 Cableado estructurado. La finalidad de este análisis es determinar la situación actual de la red IPv4, conocer los tipos de medios de transmisión, la ubicación y características de los equipos, de tal manera es posible verificar si las instalaciones del instituto son adecuadas para el proceso de adopción de IPv6.

Red de la sede principal del instituto, donde está ubicada la gerencia general de la entidad y demás oficinas administrativas, se localiza en la la ciudad de Bogotá, el edificio cuenta con 5 pisos los cuales cuentan cada uno con un cuarto de equipos y centro de cableado secundario o IDF's, los cuales a su vez se enlazan a través del backbone de fibra óptica y UTP al centro de cableado principal o MDF ubicado en el datacenter en el tercer piso, en donde además se establece la conexión con el punto de presencia (POP) del proveedor de telecomunicaciones. En la figura 15 se puede visualizar dicha distribución de cableado:

Figura 15. Distribución de cableado en edificio principal



Fuente: http://www.ciberesquina.una.edu.ve/342_Redes/imagenes/tema10/a1pag15.bmp

7.2.1.2 Cableado horizontal. El cableado horizontal del edificio se extiende desde los IDF's de cada piso hasta los equipos del área de trabajo y los puntos acceso inalámbrico.

Los IDF's forman parte de la infraestructura de red de la institución y proveen servicios de voz y datos a cada piso, en general están compuestos por los siguientes elementos básicos:

- Racks abiertos y cerrados
- Gabinetes
- Patch panels

El cableado en las áreas de trabajo se despliega desde la terminación del cableado horizontal en la salida de datos de los IDF's hasta los equipos terminales de los usuarios. A continuación, se describen algunas características principales de los medios y demás elementos del área de trabajo:

- **Cable UTP.**

Cuadro 2. Características del cable UTP categoría 6

UTP categoría 6	Descripción
Características	Tipo de aislamiento: Polietileno. Para conexiones y aplicaciones IP. Conductor de cobre sólido de 0.57 mm Diámetro exterior 6.1 mm Impedancia: 100 Ω.
Aplicaciones	1.2 Gbps ATM, 622 Mbps ATM, 100 Base T, 100 Mbps TP-PMD, 100 BASE VG ANYLAN, 1000 Base T, Video digital, Video Banda Base y Banda Ancha
Normas aplicables	ANSI/TIA/EIA 568B.2-1, ANSI/ICEA S-102-700, ISO/IEC 11801 (2a edición, clase E), NEMA WC66, EN 50173-1, UL, NMX-I-248-NYCE-2005
Fuente: 3M. Disponible en: http://multimedia.3m.com/mws/media/361174O/categoria-6-utp.pdf	

- **Patch cords.**

Cuadro 3. Especificaciones técnicas de los *patch cords*

Característica	Descripción
Protección	Moldeada en sus extremos para liberación de tensión Respeto mejorado por el radio de curvatura
Marcaje	Marcaje en cubierta exterior indicando categoría 6 y tipo de cubierta
Cubierta	PVC
Longitudes	Estándar de 1, 2 y 3 metros
Construcción	4 pares calibre 24 AWG, multifilar (7/32)
Desempeño	Superior a los 250 Mhz
Normas	ISO/IEC 11801, EIA/TIA 568 B.2, EN 50173, UL y NMX-I-NYCE-248-2005
Fuente: 3M. Disponible en: http://multimedia.3m.com/mws/media/361174O/categoria-6-utp.pdf	

- **Conectores.**

Tipo: Clavija RJ-45 de par trenzado, Cat. 6.
Resistencia por aislamiento: > 10 M Ω.
Frecuencia: 100-250 Mhz.

Tipo: Conector hembra (*jack*) RJ45 tipo *Keystone* Cat. 6.
Contactos: 8 contactos a 90°. Colocados en *face plates* o paneles de parcheo.

7.2.1.3 Cableado vertical o *backbone*. El cableado vertical de la red del instituto se desarrolla desde el *Switch* principal ubicado en el MDF del datacenter en el tercer piso hacia cada uno de los *Switches* de los IDF's ubicados en los diferentes pisos de la UPS.

- M**DF**

Ubicación: El MDF de la red principal del instituto se encuentra en el tercer piso del edificio, y posee una conexión eléctrica a tierra y al POP ubicado en el primer piso del mismo.

Dimensiones: El cuarto tiene las siguientes dimensiones: 6 mts de largo x 4 mts de ancho dando un área total de 24 m^2.

Temperatura y humedad: La temperatura aproximada del cuarto varía entre 16 – 20°C y es controlada por medio de un sistema de climatización. La humedad relativa es del 60%.

Acceso a la habitación y equipos: El ingreso a la habitación se realiza a través de una puerta blindada de acero (2 mts de largo x 1,20 mts de ancho) la misma que cuenta con un sistema de control de acceso cuya finalidad es evitar el ingreso del personal no autorizado.

Acceso y mantenimiento del cableado: El tendido del cableado horizontal se encuentra por encima del cielo raso y por debajo del piso y está conectado a un punto central en el MDF el cual permite formar la topología en estrella.

- **Fibra Óptica**

Tipo: Multimodo
Numero de fibras: 8
Compatibilidad: 1GbE 50/125µm

Conectores:

Tipo: Multimodo
Tamaño de las fibras: 900 µm.
Compatibilidad: 1 GbE 50/125µm

Acceso y Mantenimiento de la Fibra Óptica: El acceso a los cables de fibra óptica para el mantenimiento se realiza directamente sobre los racks de datos, y por medio de ductos que permiten la interconexión del cableado desde el IDF hacia el MDF.

La distribución actual del cableado de la red del nivel central se encuentra establecida de manera correcta debido a las características mencionadas anteriormente. Según el análisis realizado se ha podido determinar que el cableado estructurado del edificio principal presenta los siguientes beneficios:

- **Confiabilidad en la red**: La red actual de la Universidad es capaz de cumplir todos los propósitos para lo cual ha sido diseñada.
- **Capacidad de crecimiento**: El diseño de la topología de red tiene la capacidad de permitir el aumento de nuevos sectores de red.
- **Fácil administración**: La ubicación estratégica de los equipos de red permite detectar fácilmente los errores y corregirlos de forma inmediata.
- **Mayor Seguridad**: El acceso al MDF y los IDF's se encuentra establecido por altas normas de seguridad.

Por todo lo anterior se puede afirmar que la distribución del cableado estructurado se encuentra lista para llevar a cabo el proceso de adopción de IPv6.

7.2.2 Características de los equipos de red. A continuación, se describen las características principales de cada uno de los equipos que forman parte de la red central del instituto sede Bogotá:

7.2.2.1 Servidores virtuales.

Cuadro 4. Características de algunos servidores Windows virtuales

Dirección IPv4	Nombre	Características principales
192.168.0.88	Bogot_web.19.entida.gov.co	**Procesador**: 4 cores **Memoria**: 40 Gb **Almacenamiento**: Disco 1 -> 40Gb, Disco 2 -> 100Gb **Sistema Operativo**: Windows server 2012 R2

Cuadro 4. (Continuación)

Dirección IPv4	Nombre	Características principales
192.168.0.87	Bogot_web.18.entidad.gov.co	**Procesador**: 4 cores **Memoria**: 32 Gb **Almacenamiento**: Disco 1 -> 200Gb, Disco 2 -> 500Gb **Sistema Operativo**: Windows server 2008 R2
192.168.0.86	Bogot_web.17.entidad.gov.co	**Procesador**: 4 cores **Memoria**: 32 Gb **Almacenamiento**: Disco 1 -> 60Gb, Disco 2 -> 100Gb **Sistema Operativo**: Windows server 2008 R2
192.168.9.2	BOGOT_WEB_ 02.ENTIDAD.GOV.CO	**Procesador**: 2 procesadores 8 cores **Memoria**: 32 Gb **Almacenamiento**: Disco 1 -> 840Gb **Sistema Operativo**: Windows server 2008 R2
192.168.8.12	BOGOT_WEB_ 12.ENTIDAD.GOV.CO	**Procesador**: 1 procesador 8 cores **Memoria**: 16 Gb **Almacenamiento**: Disco 1 -> 470Gb **Sistema Operativo**: Windows server 2008 R2
192.168.5.120	BOGOT_DES_ 05.ENTIDAD.GOV.CO	**Procesador**: 4 cores **Memoria**: 32 Gb **Almacenamiento**: Disco 1 -> 40Gb, Disco 2 -> 100Gb **Sistema Operativo**: Windows server 2012 R2
192.168.2.75	BOGOT_BD_75	**Procesador**: 4 cores **Memoria**: 16 Gb **Almacenamiento**: Disco 1 -> 250Gb, Disco 2 -> 60Gb, Disco 3 -> 50Gb **Sistema Operativo**: Linux Oracle
Fuente: Elaboración propia		

Cuadro 5. Características de algunos servidores Linux Virtuales

Dirección IPv4	Nombre	Características principales
192.168.8.33	Nodo_10	**Procesador**: 2 procesador 4 cores **Memoria**: 64Gb **Almacenamiento**: Disco 1 -> 300Gb, Disco 2 -> 300Gb **Sistema Operativo**: Linux redhat 6.5
192.168.8.30	Nodo_12	**Procesador**: 2 procesador 4 cores **Memoria**: 64 Gb **Almacenamiento**: Disco 1 -> 146Gb, Disco 2 -> 146Gb **Sistema Operativo**: Linux Redhat 6.5
Fuente: Elaboración propia		

Cuadro 6. Aplicaciones o servicios instalados en los servidores Windows

Nombre	Tipo de servidor	Dirección IPv4	Funcionalidad
BOGOT_DC_05	Virtual	192.168.1.6	Controlador de dominio
BOGOT_WEB_08	Virtual	192.168.1.9	Servidor Web
BOGOT_WEB_07	Virtual	192.168.1.12	Servidor Web
BOGOT_DC_14	Virtual	192.168.1.11	Controlador de dominio
APOLO_01	Físico	192.168.1.19	File Server
Monitoreo Vmware	Virtual	192.168.1.15	Gestión de monitoreo
BOGOT_HELP_02	Virtual	192.168.1.16	Aplicaciones mesa de ayuda /Web/cliente servidor
BOGOT_HELP_03	Virtual	192.168.1.17	Aplicaciones mesa de ayuda /Web/cliente servidor
MARTE_50	Físico	192.168.1.18	Aplicaciones facturación/cliente servidor
BOGOT_BCK_05	Físico	192.168.1.20	Aplicaciones dataprotector
BOGOT_FENICA_06	Virtual	192.168.1.21	Aplicaciones /cliente servidor
BOGOT_WEB_08	Virtual	192.168.1.22	Servidor Web
ABACOX_100	Virtual	192.168.1.25	Servidor Web
BOGOT_BD_88	Virtual	192.168.1.27	Servidor Base de Datos
BOGOT_S1S_02	Virtual	192.168.1.29	Servidor Web
BOGOT_BD_09	Virtual	192.168.1.47	Servidor Base de Datos
BOGOT_EPO_22	Virtual	192.168.1.48	Aplicación McAfee
BOGOT_WEB_05T	Virtual	192.168.1.61	Servidor Web
BOGOT_WEB_66	Virtual	192.168.1.62	Servidor Web
BOGOT_WEB_14	Virtual	192.168.1.63	Servidor Web
BOGOT_WEB_16	Virtual	192.168.1.64	Servidor Web
BOGOT_WEB_21	Virtual	192.168.1.65	Servidor Web
BOGOT_EPO_10	Virtual	192.168.1.69	Servidor Web
BOGOT_VCENTER_1	Virtual	192.168.1.71	Aplicación Vmware
BOGOT_WEB_18	Virtual	192.168.1.72	Servidor Web
BOGOT_WEB_16	Virtual	192.168.1.73	Servidor Web
BOGOT_SYNC_06	Virtual	192.168.1.76	Aplicación Office 365
BOGOT_HYB_05	Virtual	192.168.1.77	Aplicación Office 365
BOGOT_IMPR_03	Virtual	192.168.1.78	Aplicación de impresión
Bogot_bd_01_zfp	Virtual	192.168.1.80	Servidor Base de Datos
Bogot_web_3	Virtual	192.168.1.83	Servidor Web
MADR_WEB_11	Virtual	192.168.1.111	Servidor Web
MADR_APP_12	Virtual	192.168.1.112	Servidor Web
MADR_BD_13	Virtual	192.168.1.113	Servidor Base de Datos

Cuadro 6. (Continuación)

Nombre	Tipo de servidor	Dirección IPv4	Funcionalidad
BOGOT_BD_11	Virtual	192.168.0.106	Servidor Base de Datos
BOGOT_WEB_12	Virtual	192.168.0.114	Servidor Web
BOGOT_DES_08	Virtual	192.168.0.126	Servidor Web
BOGOT_WEB_09	Físico	192.168.5.4	Servidor Web
BOGOT-WEB_15	Físico	192.168.5.5	Servidor Web
BOGOT_WEB_13	Físico	192.168.5.6	Servidor Web
BOGOT_WEB_11	Físico	192.168.5.7	Servidor Web
BOGOT_FAX_05	Físico	192.168.5.8	Servidor Web
BOGOT_BCK_03	Físico	192.168.5.9	Aplicación backup usuario final
Fuente: Elaboración propia			

7.2.2.2 Firewall.

Cuadro 7. Características del firewall

Característica	Descripción
Marca	Check Point
Modelo	4800 Appliance
Número de usuarios administrativos	5 en simultaneo
Memoria (GB)	4
Máximo rendimiento (Mbps)	5800
Número máximo de conexiones	3.3 millones
Número máximo de conexiones / Segundo	70000
Puertos integrados	8 x 10/100/1000Base-T puertos RJ45
Número máximo de VLANS	256 por interfaz
Conectividad en red	Compatible con IPv4 e IPv6
Fuente: https://sc1.checkpoint.com/uc/pdf/datasheets/4800-appliance-datasheet.pdf	

7.2.2.3 Routers.

Cuadro 8. Características del router WAN/Internet principal

Característica	Descripción
Marca	Cisco
Modelo	3945E
Dimensiones	133.35 x 438.15 x 476.25 mm

Cuadro 8. (Continuación)

Característica	Descripción
Peso	27,2 Kg
Memoria DRAM	1 GB (instalada) / 2 GB Max. – DDR2 ECC
Memoria Flash	256 MB (instalada) / 4 GB Max.
Protocolos	IPv4, IPv6, static routes, OSPF, EIGRP, BGP, BGP Router Reflector, IS-IS, Multicast Internet Group Management Protocol (IGMPv3), Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPv4-to-IPv6 Multicast, MPLS, Layer 2 and Layer 3 VPN, IPSec, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Bidirectional Forwarding Detection (BFD), IEEE802.1ag, y IEEE802.3ah.
Protocolo de administración remota	SNMP, Remote Monitoring (RMON), syslog, NetFlow, y TR-069
Voltaje	AC 120/220 V (50/60 Hz).
Fuente: http://www.cisco.com/c/en/us/products/collateral/routers/3900-series-integrated-services-routers-isr/data_sheet_c78_553924.pdf	

Cuadro 9. Características del router de voz

Característica	Descripción
Marca	Cisco
Modelo	2951
Dimensiones	88.9 x 438.2 x 469.9 mm
Peso	15.5 Kg
Memoria DRAM	512 MB (instalada) / 2 GB Max. DDR2 ECC
Memoria Flash	256 MB (instalada) / 4 GB Max.
Protocolos	IPv4, IPv6, Static Routes, OSPF, EIGRP, BGP, BGP Router Reflector, IS-IS, IGMPv3, Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPSec, Generic Routing Encapsulation (GRE), Bi-Directional Forwarding Detection (BVD), IPv4-to-IPv6 Multicast, MPLS, L2TPv3, 802.1ag, 802.3ah, L2 y L3 VPN.
Gestión de tráfico	QoS, Class-Based Weighted Fair Queuing (CBWFQ), Weighted Random Early Detection (WRED), Hierarchical QoS, Policy-Based Routing (PBR), Performance Routing (PfR), y Network-Based Advanced Routing (NBAR).
Protocolo de administración remota	SNMP, Remote Monitoring (RMON), syslog, NetFlow, and TR-069
Voltaje	AC 120/220 V (50/60 Hz).
Fuente: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-4500-series-switches/product_data_sheet0900aecd801792b1.html	

7.2.2.4 Switches.

Cuadro 10. Características del switch CORE

Característica	Descripción
Marca	CISCO
Modelo	WS-C3750X
Numero de puertos	48
Protocolo de enrutamiento	Estatico, RIP-1, RI-2, RIPng, EIGRP, OSPF, OSPFv3, OSPFv6, BGPv4, IS-ISv4
Protocolo de administración remota	RMON, SNMPv3
Algoritmo de encriptación	SSH
Estándares	IEEE 802.1s/w/x/x-Rev/ae/D/p/Q. IEEE 802.3 IEEE 802.1ad//af/at/x/u/ab/z
Memoria Flash	64 MB (instalada) – 128 MB Max.
Interfaces	48 x 10Base-T/100Base-TX/1000BaseTX - RJ-45 1 x console - RJ-45 – management 4 x SFP (mini-GBIC)
Voltaje	100-240VAC, 50-60 Hz
Dimensiones	4.45 x 44.5 x 49.5 cm
Peso	7,6 Kg
Software	Cisco LAN Base, IP Base e IP Service Base
Fuente: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-x-series-switches/data_sheet_c78-584733.html	

Cuadro 11. Características switch principal de distribución (Servidores)

Característica	Descripción
Marca	CISCO
Modelo	WS-C3750G-12S
Numero de puertos	12 puertos SFP Gigabit Ethernet
Protocolo de enrutamiento	Estatico, RIP-1, RI-2, RIPng, EIGRP, OSPF, OSPFv6, BGPv4, IS-ISv4
Protocolo de administración remota	SNMPv1, v2c y v3. Telnet
Algoritmo de encriptación	SSH
Estándares	IEEE 802.1s/w/x/x-Rev/ae/D/p/Q. IEEE 802.3 IEEE 802.1ad//af/at/x/u/ab/z
Memoria Flash	16 MB
Interfaces	12 puertos Gigabit Ethernet SFP
Voltaje	100-240VAC, 0.6-1.2A, 50-60 Hz
Dimensiones	4.4 x 44.5 x 32.6 cm
Peso	4.6 Kg
Software	Cisco IP Base
Fuente: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series-switches/product_data_sheet0900aecd80371991.html	

Cuadro 12. Características switches de acceso

Característica	Descripción
Marca	Hewlett Packard
Modelo	A5120-48G
Numero de puertos	48 puertos 10/100/1000
Protocolo de administración remota	SNMP
Algoritmo de encriptación	SSL. SSHv2
Estándares	IEEE 802.1ad Q-in-Q, IEEE 802.1D MAC Bridges IEEE 802.1p Prioridad IEEE 802.1Q VLANs IEEE 802.1s Multiple Spanning Trees IEEE 802.1w Rapid Reconfiguration of Spanning Tree IEEE 802.1X PAE IEEE 802.3 Type 10BASE-T IEEE 802.3ab 1000BASE-T IEEE 802.3ad Link Aggregation Control Protocol (LACP) IEEE 802.3ae 10-Gigabit Ethernet IEEE 802.3af Power over Ethernet IEEE 802.3i 10BASE-T IEEE 802.3u 100BASE-X IEEE 802.3x Flow Control IEEE 802.3z 1000BASE-X
Memoria Flash	16 MB
Interfaces	44 RJ-45 autosensing 10/100/1000 ports (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); Media Type: Auto- MDIX; Duplex: 10BASE-T/ 100BASE-TX: half or full; 1000BASE-T: full only 4 dual-personality ports; autosensing 10/100/1000BASE-T or SFP Supports a maximum of 48 autosensing 10/100/1000 ports 1 RJ-45 serial console port
Voltaje	100 - 240 VAC - 50-60 Hz
Dimensiones	44 x 30x 4.37 cm
Peso	5 Kg
Fuente: https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA3-0725ENW.pdf	

7.2.2.5 Teléfonos IP.

Cuadro 13. Características de teléfonos IP cisco 7942G

Característica	Descripción
Tipo de producto	Teléfono VoIP
Protocolo VoIP	SCCP
Códecs de voz	G.711a, G.711µ, G.729a, G.729ab, G.722, and iLBC audio compression codecs are supported (see Q&A for details).
Visualizador	Display de 5” (12.5 cm), alta resolución (320 x 222), grafico monocromático a escala de grises de 4-bit.
Cantidad de puertos de red	2 x Ethernet 10/100Base-TX
Software compatible	Cisco Unified Communications Manager Versión 4.1(3)sr5b, 4.2(3)sr2b, 4.3(1), 5.1.1(b), 5.1(2), 6.0(1) y superiors. Cisco Unified Communications Express y SRST Version 4.1
Calidad de servicio	Soporta DSCP y estándares 802.1Q/p
Asignación de direcciones IP	Estáticas o por DHCP
Seguridad	Identidad positiva de dispositivo a través de certificados X.509v3, imágenes firmadas digitalmente, aprovisionamiento criptográficamente seguro, y la señalización de seguridad y los medios de comunicación seguro con AES-128. Criptografía no habilitada de forma predeterminada y sólo puede ser activado a través de un CUCM criptográficamente habilitado. También contiene un solicitante 802.1X y apoya EAPOL de paso a través
Soporte al lenguaje	Incorpora soporte a más de 30 idiomas
Dimensiones	20.32 x 26.67 x 15.24 cm
Peso	1.6 Kg
Fuente: http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-7942g/product_data_sheet0900aecd8069bb68.html	

Cuadro 14. Características de teléfonos IP cisco 7911

Característica	Descripción
Tipo de producto	Teléfono VoIP
Protocolo VoIP	SCCP
Códecs de voz	G.729a, G.729ab, G.711u, G711a
Visualizador	Pantalla de cristal líquido – monocromática
Cantidad de puertos de red	2 x Ethernet 10/100Base-TX
Software compatible	Cisco CallManager
Calidad de servicio	IEEE 802.1Q (VLAN), IEEE 802.1p
Asignación de direcciones IP	DHCP
Seguridad	AES de 128 bits
Soporte al lenguaje	Detección de actividad de voz (VAD)
Dimensiones	17.6 cm x15.2 cm x 20.3 cm
Peso	0,9 Kg
Fuente: http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-7911g/product_data_sheet0900aecd8039de52.html	

7.2.3 Equipos de cómputo e impresoras. Se realizó el inventario de equipos de cómputo de los usuarios a nivel nacional, soportado con la herramienta de colaboración Discovery, en el cual se identificaron 2902 equipos con variedad de sistemas operativos, en general se puede concluir que todos los equipos computacionales de usuarios activos que actualmente hacen parte del inventario tienen total compatibilidad con el protocolo IPv6. En la tabla 1 se relaciona un resumen de los datos verificados:

Tabla 1. Cantidad de equipos de cómputo por sistema operativo

Seccional	Sistema operativo (Windows)					
	Vista	Windows 7	Windows 8	Windows 8.1	XP	Total general
Amazonas		9	2		1	12
Antioquia	16	91	28	19	10	164
Arauca	11	32	16	9	5	73
Atlántico	9	16	13	16	1	55
Bogotá	90	421	64	169	25	769
Bolívar	11	33	19	9	4	76
Boyacá	12	35	20	10	6	83
Caldas	3	43	19	11	9	85
Caquetá	2	21	14	9	7	53
Casanare	4	15	23	9	1	52
Cauca		15	5	5	1	26
Cesar	10	19	28	12	7	76
Choco		6	4	2		12
Córdoba	3	48	23	14	4	92
Cundinamarca	45	102	21	36	39	243
Guainía		6	3			9
Guajira	7	6	3	6	1	23
Guaviare		6	6	3		15
Huila	1	20	9	9	3	42
La Guajira	1	6	5			12
Magdalena	1	23	23	14	1	62
Meta	14	50	23	13	7	107
Nariño	9	40	20	14	4	73
Norte de Santander	11	38	20	8	9	86
Oficinas nacionales	11	97	6	8	9	131
Putumayo	2	19	9	5		35
Quindío	4	21	12	5	6	48
Risaralda	2	24	13	2		41
San andres y providencia		4		1		5
Santander	6	36	23	6	12	83
Sucre	3	22	27	2	3	57
Tolima	2	23	18	11	1	55
Valle	6	26	16	18	1	67

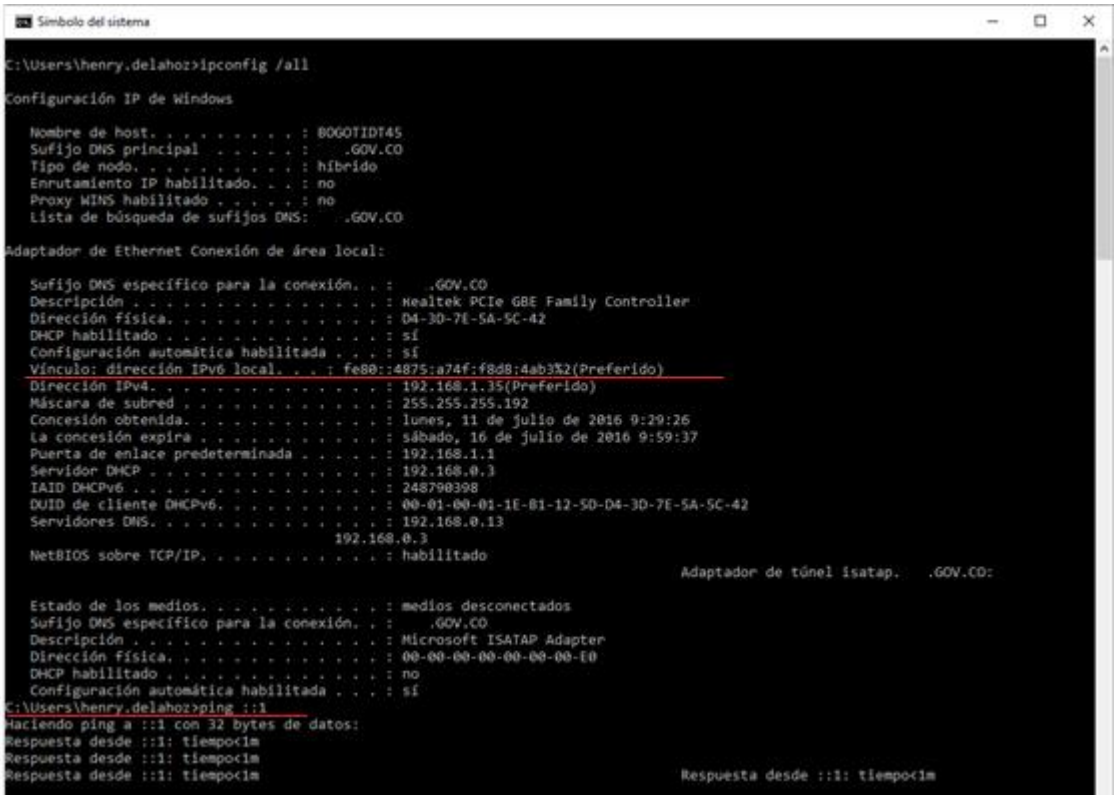
Tabla 1. (Continuación)

Seccional	Sistema operativo (Windows)					
	Vista	Windows 7	Windows 8	Windows 8.1	XP	Total general
Valle del cauca	2	15	11	2	6	36
Vaupés		4	3	1	1	9
Vichada		6	2	1		9
(en blanco)		5	2	3		10
Total general	**298**	**1403**	**553**	**462**	**185**	**2901**

Fuente: Elaboración propia

Cabe resaltar que los datos anteriormente relacionados están basados en consultas a la base de datos de la herramienta de colaboración y mesa de ayuda, lo que podría tener un margen de error teniendo en cuenta que algunas máquinas actualmente operativas podrían presentar falla en el agente de mesa de ayuda para la comunicación con el servidor. Sin embargo, una prueba sencilla que se puede hacer para la comprobación de IPv6 *Ready* en un equipo de cómputo es usando los comandos IPCONFIG /ALL y PING ::1 que corresponde a la dirección de *loopback* del equipo, como se observa en la figura 16.

Figura 16. Comprobación IPv6 Ready en Windows



Fuente: Elaboración propia

Adicional a los equipos de cómputo se pudo realizar la verificación de los diferentes modelos de impresoras que posee la entidad en las sedes de Cundinamarca, de las cuales se muestran en el cuadro 15 aquellas que resultaron no compatibles con el protocolo IPv6:

Cuadro 15. Impresoras verificadas no compatibles con IPv6

Marca/modelo	Sede	Dependencia	Ubicación	Versión IP	Compatible IPv6
Epson LX300+II	Aeropuerto	Sub. De Protección Fronteriza	CAT Piso 3	N/A	NO
Lexmark E330	LNDV	Medicina porcina	Laboratorio 2A	IPv4	NO
Lexmark E220	Oficinas Nacionales	Atención al Ciudadano	Piso 1 Lado Norte	IPv4	NO
Kodack 13200 Scanner	Oficinas Nacionales	Atención al Ciudadano	Piso 1 Lado Norte	IPv4	NO
HP Desjet 970CXI	Oficinas Nacionales	Planeación	piso 2 lado Sur	IPv4	NO
HP Desjet 970CXI	Oficinas Nacionales	Talento Humano	piso 3 Lado Sur	IPv4	NO
HP 1015 LaserJet	Oficinas Nacionales	Insumos Agrícolas	Piso 4 lado Norte	IPv4	NO
Epson LX300+II	Aeropuerto	Sub. De Protección Fronteriza	CAT Piso 3	N/A	NO
EPSON FX1170	TIBAITATÁ	ORNAMENTALES	SEDE PRINCIPAL - PISO 2	N/A	NO
LEXMARK E330	TIBAITATÁ	FRUTALES	SEDE PRINCIPAL - PISO 2	IPv4	NO
LEXMARK E330	TIBAITATÁ	COORDINACIÓN AGRÍCOLA	SEDE PRINCIPAL - PISO 1	IPv4	NO
LEXMARK E330	LNDV	Medicina porcina	Laboratorio 2A	IPv4	NO
LEXMARK T642	LNDV	Responsables laboratorios	Bloque administrativo	IPv4	NO
Lexmark T640	LNDV	recepción de muestras	recepción de muestras	IPv4	NO
LEXMARK E330	LNDV	Medicina porcina	Laboratorio 2A	IPv4	NO
Lexmark T644	LNDV	Brucelosis	Laboratorio 2A	IPv4	NO
Fuente: Elaboración propia					

Además, algunas de estas impresoras permiten el soporte al nuevo protocolo, pero condicionadas a la inclusión de un accesorio o modulo adicional, son estas las relacionadas en el cuadro 16:

Cuadro 16. Impresoras verificadas compatibles con IPv6 con accesorio

Marca/modelo	Sede	Dependencia	Ubicación	Versión IP	Compatible IPv6
Lexmark T644	Oficinas Nacionales	Financiera	piso 5 lado Norte	IPv4	SI (CON ACCESORIO)
Lexmark T644	Oficinas Nacionales	Insumos Veterinarios	Piso 3 lado Norte	IPv4	SI (CON ACCESORIO)
Lexmark T644	Oficinas Nacionales	OTI	Piso 3 lado Norte	IPv4	SI (CON ACCESORIO)
Lexmark T640	Oficinas Nacionales	Vigilancia	Piso 3 lado Norte	IPv4	SI (CON ACCESORIO)
Lexmark T640	Oficinas Nacionales	Cuarentena Vegetal	Piso 3 lado Norte	IPv4	SI (CON ACCESORIO)
Lexmark T644	Oficinas Nacionales	Insumos Agrícolas	Piso 4 lado Norte	IPv4	SI (CON ACCESORIO)
Lexmark T644	Oficinas Nacionales	TH Bienestar y capacitación	piso 2 lado Sur	IPv4	SI (CON ACCESORIO)
Lexmark T644	Oficinas Nacionales	Jurídica	piso 2 lado Norte	IPv4	SI (CON ACCESORIO)
HP-LaserJet M3035 MFP	Oficinas Nacionales	Servicios Generales	Piso 1 lado Sur	IPv4	SI (CON ACCESORIO SOLO WINDOWS)
HP LaserJet P1660DN	Oficinas Nacionales	Atención al Ciudadano	Piso 1 Lado Norte	IPv4	SI (CON ACCESORIO)
Lexmark T644	Oficinas Nacionales	Financiera	Piso 1 lado Sur	IPv4	SI (CON ACCESORIO)
HP-LaserJet 2200d	Oficinas Nacionales	Planeación	piso 2 lado Sur	IPv4	SI (CON ACCESORIO)
HP-LaserJet 40115m	Oficinas Nacionales	Sub Sanidad Animal	piso 2 lado Norte	IPv4	SI (CON ACCESORIO)
HP-LaserJet M3035 MFP	Oficinas Nacionales	Sub Regulación Fitosanitaria	piso 2 lado Norte	IPv4	SI (CON ACCESORIO SOLO WINDOWS)
HP-LaserJet M3035 MFP	Oficinas Nacionales	Insumos Agrícolas	Piso 4 lado Norte	IPv4	SI (CON ACCESORIO SOLO WINDOWS)
Lexmark T644	Oficinas Nacionales	Insumos Agrícolas	Piso 4 lado Norte	IPv4	SI (CON ACCESORIO)
HP Office jet Pro8100	Oficinas Nacionales	D. Técnica de Sanidad Vegetal	Piso 4 lado Norte	IPv4	SI (CON ACCESORIO)
HP LaserJet P1660DN	Oficinas Nacionales	Contractual	piso 5 lado Norte	IPv4	SI (CON ACCESORIO)
Lexmark T644	Oficinas Nacionales	D. Técnica de Sanidad Animal	piso 5 lado Norte	IPv4	SI (CON ACCESORIO)
Lexmark T642	Oficinas Nacionales	Contractual	piso 5 lado Norte	IPv4	SI (CON ACCESORIO)
HP LaserJet P3035	Aeropuerto	Sub. De Protección Fronteriza	CAT Piso 3	IPv4	SI (CON ACCESORIO SOLO WINDOWS)
HP LaserJet P3035	Aeropuerto	Sub. De Protección Fronteriza	CAT Piso 3	IPv4	SI (CON ACCESORIO SOLO WINDOWS)
HP LaserJet P3035	Aeropuerto	Sub. De Protección Fronteriza	CAT Piso 3	IPv4	SI (CON ACCESORIO SOLO WINDOWS)
HP M3035 MFP	TIBAITATÁ	CONTABILIDAD	SEDE PRINCIPAL - PISO 2	IPv4	SI (CON ACCESORIO SOLO WINDOWS)
LEXMARK T640	TIBAITATÁ	PECUARIA	SEDE PRINCIPAL - PISO 1	IPv4	SI (CON ACCESORIO)

Cuadro 16. (Continuación)

Marca/modelo	Sede	Dependencia	Ubicación	Versión IP	Compatible IPv6
HP M3035 MFP	TIBAITATÁ	LABORATORIO NACIONAL DE DIAGNOSTICO FITOSANITARIO	LABORATORIO LNDF	IPv4	SI (CON ACCESORIO SOLO WINDOWS)
LEXMARK T640	TIBAITATÁ	INSUMOS PECUARIOS	SEDE PRINCIPAL - PISO 2	IPv4	SI (CON ACCESORIO)
HP LaserJet M3035 MFP	LNDV			IPv4	SI (CON ACCESORIO SOLO WINDOWS)
Lexmark T642	LNDV	Responsables laboratorios	Bloque administrativo	IPv4	SI (CON ACCESORIO)
HP LaserJet M3035 MFP	LNDV	Responsables laboratorios	Bloque administrativo	IPv4	SI (CON ACCESORIO SOLO WINDOWS)
Lexmark t640	LNDV	recepción de muestras	recepción de muestras	IPv4	SI (CON ACCESORIO)
Lexmark T644	LNDV	Brucelosis	Laboratorio 2A	IPv4	SI (CON ACCESORIO)
HP LaserJet M3035 MFP	LNDV			IPv4	SI (CON ACCESORIO)
HP LaserJet M3035 MFP	LNDV	Responsables laboratorios	Bloque administrativo	IPv4	SI (CON ACCESORIO)
Fuente: Elaboración propia					

7.2.4 Equipos de comunicaciones. Una vez caracterizados y verificados técnicamente los diferentes modelos de equipos de comunicaciones (*Switches*, plantas telefónicas, *Access Points*, Teléfonos y demás) con los que cuenta la entidad, se pudo determinar que algunos de estos actualmente no cumplen con las condiciones técnicas requeridas para soportar el protocolo IPv6 ni permiten el despliegue de alguna actualización de firmware para tal fin, son éstos los equipos detectados relacionados en el cuadro 17:

Cuadro 17. Equipos de comunicaciones no compatibles con IPv6

Equipo	Marca	Modelo	Sistema Operativo	Rol	Versión IP	Compatible	Actualizable
Switch	Avaya			Horizontal Piso 1	IPv4	NO	NO
Switch	Cisco	WS-C2960-24TC-L	12.2(44)SE6	Horizontal Piso 2	IPv4	NO	NO
Switch	Avaya			Horizontal Piso 3	IPv4	NO	NO
Switch	Avaya	P330	3.0.5	TIBAITATÁ	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Aeropuerto Dorado	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Barranquilla	IPv4	NO	NO
Planta Telefónica	Panasonic	NCP500	N/A	Planta Cartagena	IPv4	NO	NO

Cuadro 17. (Continuación)

Equipo	Marca	Modelo	Sistema Operativo	Rol	Versión IP	Compatible	Actualizable
Planta Telefónica	Panasonic	NCP500	N/A	Planta Duitama	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Bucaramanga	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Cerete	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Cúcuta	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Florencia	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Ibagué	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Bogotá Identifica	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Manizales	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Medellín	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Cordoba	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Neiva	IPv4	NO	NO
Planta Telefónica	Panasonic	NCP500	N/A	Planta Pasto	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Pereira	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Puerto Asis	IPv4	NO	NO
Planta Telefónica	Panasonic	TDA 100	N/A	Planta Armenia	IPv4	NO	NO
Planta Telefónica	Panasonic	NCP500	N/A	Planta Riohacha	IPv4	NO	NO
Planta Telefónica	Panasonic	NCP500	N/A	Planta Sincelejo	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Valle del Cauca	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Valledupar	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Villavicencio	IPv4	NO	NO
Planta Telefónica	Panasonic	TDE 100	N/A	Planta Yopal	IPv4	NO	NO
Planta Telefónica	Panasonic	NCP1000	N/A	Planta Bogotá Ceisa	IPv4	NO	NO
Teléfono	Cisco	7940	N/A	Telefonía IP	IPv4	NO	NO
Teléfono	Panasonic	NT366	N/A	Telefonía IP	IPv4	NO	NO
Teléfono	Panasonic	NT346	N/A	Telefonía IP	IPv4	NO	NO
Videoconferencia	Aethra	X5 y X3	Vega X5 Series 3 12.1.10	Bogotá Oficina Nacionales Gerencia	IPv4	NO	NO
Videoconferencia	Aethra	X5 y X3	Vega X5 Series 3 12.1.10	Bogotá Oficina Nacionales Sub. Administrativa	IPv4	NO	NO

Cuadro 17. (Continuación)

Equipo	Marca	Modelo	Sistema Operativo	Rol	Versión IP	Compatible	Actualizable
Enrutador Inalámbrico	Trendnet	Trednet TEW-452brp	N/A	Inalámbrico Ibagué	IPv4	NO	NO
Enrutador Inalámbrico	Trendnet	Trednet TEW-452brp	N/A	Inalámbrico Meta	IPv4	NO	NO
Enrutador Inalámbrico	Trendnet	Trednet TEW-452brp	N/A	Inalámbrico Guajira	IPv4	NO	NO
Enrutador Inalámbrico	Trendnet	Trednet TEW-452brp	N/A	Inalámbrico Sincelejo	IPv4	NO	NO
Enrutador Inalámbrico	Trendnet	Trendnet tew-450apb	N/A	Inalámbrico LNDV	IPv4	NO	NO
Enrutador Inalámbrico	Encore	ENHWI-2AN3	N/A	Inalámbrico Arauca	IPv4	NO	NO
Enrutador Inalámbrico	Dlink	DLINK DI524	N/A	Inalámbrico Armenia	IPv4	NO	NO
Access Point	Tp-Link	TL-WA901ND	N/A	Inalámbrico Cúcuta	IPv4	NO	NO
Enrutador Inalámbrico	LinkSys	WRT300N-V1	N/A	Inalámbrico LANIP	IPv4	NO	NO
Enrutador Inalámbrico	Trendnet	TEW-452BRP	N/A	Inalámbrico Barranquilla	IPv4	NO	NO
Enrutador Inalámbrico	D-Link	DIR-610	N/A	Inalámbrico Valle del Cauca	IPv4	NO	NO
Access Point	Tp-Link	TL-WA801ND	N/A	Inalámbrico LNDV	IPv4	NO	NO
Access Point	Tp-Link	TL-WA901ND	N/A	Inalámbrico LNDV	IPv4	NO	NO
Enrutador Inalámbrico	LinkSys	WAP4400N	N/A	Inalámbrico LNDV	IPv4	NO	NO
Enrutador Inalámbrico	LinkSys	Cisco WRT320N	N/A	Inalámbrico LNDV	IPv4	NO	NO
Access Point	Tp-Link	TL-WA901ND	N/A	Inalámbrico identifica	IPv4	NO	NO
Access Point	Tp-Link	TL-WA901ND	N/A	Inalámbrico Fundación	IPv4	NO	NO
Access Point	Tp-Link	TL-WR841N	N/A	Inalámbrico Yopal	IPv4	NO	NO
Access Point	linksys	Cisco wrt120n	N/A	Inalámbrico Barranquilla Puerto	IPv4	NO	NO
Access Point	Kozáni	K-1500NR	N/A	Inalámbrico San Jose De Guaviare	IPv4	NO	NO
Access Point	Kozáni	K-1500NR	N/A	Inalámbrico Palmira	IPv4	NO	NO

Fuente: Elaboración propia

Todos los demás equipos no señalados en la tabla anterior, de acuerdo a las verificaciones realizadas, cumplen efectivamente con el soporte al nuevo protocolo.

Por lo tanto, respecto a los equipos no compatibles, es necesario que por parte de la dirección del proyecto y las instancias administrativas y gerenciales de la entidad se realice un análisis de factibilidad económica que permita considerar una renovación tecnológica para atender la problemática de incompatibilidad y obsolescencia actual frente al protocolo IPv6, más adelante se analizan los costos económicos asociados a este tipo de requerimientos.

7.2.5 Aplicaciones de negocio. La metodología utilizada inicialmente fue realizar la consulta a las personas directamente responsables y administradores de las diferentes aplicaciones quienes diligenciaron el formato enviado con la información solicitada, las siguientes fueron las aplicaciones referenciadas:

- Contratos
- CMS Portal Corporativo
- INSTINET
- SINAD
- SIGMA
- SISFITO
- SPS - Sistema programación seguimiento
- ABACOX
- DATAPROTECTOR

De acuerdo a lo verificado únicamente la aplicación que, con base a lo confirmado con el proveedor, resultó incompatible con el protocolo IPv6 y no actualizable fue **EQUITRAC** para la administración de colas de impresión.

Como resultado de dicha consulta se obtuvo que la mayoría de aplicaciones anteriormente mencionadas son compatibles o soportan el protocolo IPv6 para su funcionamiento, sin embargo con el objetivo de que esta afirmación esté soportada técnicamente es necesario generar un entorno de verificación mediante laboratorios prueba para analizar el comportamiento de las aplicaciones en coexistencia de los dos protocolos de red (IPv4/IPv6) y desplegar además un protocolo de pruebas de funcionalidad a cada componente de dichas aplicaciones, para lo anterior, se llevó a cabo el montaje virtual de un laboratorio de pruebas preliminar con la aplicación SISFITO, los detalles y resultados de este ambiente de pruebas se explican …en el anexo B … (Acta de reunión 003 de 2016).

7.2.6 Servidores. De acuerdo a la información suministrada por el ingeniero de la oficina de tecnologías de información encargado de la administración de servidores, se puede confirmar que todos los sistemas operativos (Windows y Linux), tanto

físicos como virtuales, soportan el protocolo IPv6. Las versiones de los sistemas operativos y roles de cada servidor se señalan en el cuadro 18:

Cuadro 18. Compatibilidad de IPv6 en servidores

Compatible con IPv6	Sistema operativo								
	GNU/Linux				Windows				
Rol	Debian 6	Debian 8	Oracle	Redhat 6.5	2000 server	2003 server	2008 server	2012 server R2	Total general
Aplicación Backup usuario final							1		1
Aplicación de Impresión								1	1
Aplicación McAfee								1	1
Aplicación Office 365								2	2
Aplicación VMWare								1	1
Aplicaciones /cliente servidor							1		1
Aplicaciones Dataprotector							1		1
Aplicaciones facturación/cliente servidor					1				1
Aplicaciones mesa de ayuda /Web/cliente servidor							2		2
Clúster Nodo 1 (Oracle)				1					1
Clúster Nodo 2 (Oracle)				1					1
Controlador de dominio								2	2
Controlador de dominio secundario							14		14
File Server						1			1
Gestión de Monitoreo								1	1
Servidor Base de Datos							3	2	5
Servidor de Aplicaciones (SIGMA)	1								1
Servidor de Aplicaciones		1							1
Servidor de Aplicaciones Pruebas		1							1
Servidor de Base de aplicaciones nube		1							1

Cuadro 18. (Continuación)

Compatible con IPv6	Sistema operativo								
	GNU/Linux				Windows				
	Debian 6	Debian 8	Oracle	Redhat 6.5	2000 server	2003 server	2008 server	2012 server R2	Total general
Servidor de Base de aplicaciones sipco - dspace		1							1
Servidor de base de datos (Oracle)				1					1
Servidor de Base de datos Maria DB		1							1
Servidor de Base de datos Pruebas (Oracle)			1						1
Servidor Web						3	15	5	23
Total general	**1**	**5**	**1**	**3**	**1**	**4**	**37**	**15**	**67**
Fuente: Elaboración propia									

7.2.7 Observaciones generales del diagnóstico IPv6. Es importante destacar que del diagnóstico realizado inicialmente se puede considerar que la infraestructura tecnológica y sistemas de la entidad se encuentra en un **86%** de compatibilidad con el protocolo IPv6 y el diferencial para garantizar el soporte total del protocolo en todos los equipos, sistemas, servicios y demás depende en gran medida de la inversión de nueva infraestructura y renovación tecnológica necesaria para garantizar un ambiente en doble pila (IPv4/IPv6) estable.

Nota: El porcentaje anteriormente mencionado se pudo definir como resultado de lo mostrado en el cuadro 19.

Cuadro 19. Estimación del nivel de compatibilidad con IPv6

Tipo de elemento	(a)	(b)	(c)	(d)
Equipos de computo	2901	0	0%	100%
Periféricos	208	41	20%	80%
Equipos de comunicaciones	144	56	39%	61%
Software	11	1	9%	91%
Servidores	67	0	0%	100%
Total	**3331**	**98**	**14%***	**86%***
Fuente: Elaboración propia				

***** Resultado del promedio de los porcentajes por cada tipo de elemento diagnosticados.

Donde:

(a) Cantidad de elementos diagnosticados.
(b) Cantidad de elementos no compatibles con IPv6.
(c) Porcentaje de elementos diagnosticados no compatibles con IPv6.
(d) Porcentaje de elementos diagnosticados compatibles con IPv6.

7.3 RIESGOS DEL PROYECTO

Durante el desarrollo del proyecto es posible que exista una serie de aspectos que ponen en riesgo el proceso de migración hacia el protocolo IPv6, en ese sentido la intención de identificar estos riesgos es poder tener previstas las acciones que se podrían completar para tratar de minimizarlos o mitigarlos, en los cuadros 20, 21 y 22, se presentan los riesgos más importantes:

Cuadro 20. Matriz de riesgos identificados

Número	Riesgos asociados al proyecto de transición
1	Desconocimiento de la tecnología por parte de los stakeholders
2	Nula o inadecuada planeación
3	Incumplimiento en el proceso de implementación
4	Información técnica incompleta, desactualizada, obsoleta o inexistente
5	Resistencia y falta de empoderamiento para la gestión de cambios
6	Demoras en los procesos de contratación
7	Presupuesto insuficiente para el acompañamiento, maduración de proyecto y adquisiciones
Fuente: Elaboración propia	

A pesar de que IPv6 nos abre las puertas a nuevas posibilidades en el desarrollo de redes y sistemas de información, gracias a sus ya mencionadas ventajas que tiene sobre IPv4, es también relevante poder conocer y entender los riesgos que pueden estar asociados a su adopción, en el cuadro 21 se describen algunos de estos:

Cuadro 21. Riesgos identificados al adoptar IPv6

Número	Riesgos de adoptar IPv6
1	Incompatibilidad IPv4/IPv6 en tecnologías de hardware, software y plataformas TIC
2	Falta de soporte efectivo a la nueva tecnología IPv6
3	Amenazas de seguridad de la información
4	Ausencia / Fallas en la implementación de herramientas de monitorización de red
5	Pérdida de información
6	Proceso de curva de aprendizaje y experiencia
7	Proceso de maduración de la tecnología
8	Problemas de funcionamiento de sistemas operativos
9	Entornos TIC sin IPv6 Ready
10	Aplicaciones hechas a la medida sin soporte
Fuente: Elaboración propia	

El uso de IPv6 en las empresas aumenta de forma progresiva en el mundo, por lo tanto, la no implementación de IPv6 puede producir lo relacionado en el cuadro 22:

Cuadro 22. Riesgos de no adoptar IPv6

Número	Riesgos de no adoptar IPv6
1	Incumplimiento de políticas / directrices del estado colombiano e internacionales
2	Obsolescencia tecnológica
3	Aumento de la brecha de conectividad y servicios digitales
4	Agotamiento / No disponibilidad de direcciones IPv4
5	Incompatibilidad y no operatividad tecnológica
6	Indisponibilidad en la prestación de servicios al ciudadano y continuidad de negocio
7	Incremento en los costos de soporte y mantenimiento de tecnologías obsoletas
8	Incremento de costos por adoptar IPv6 en forma tardía
Fuente: Elaboración propia	

En la actualidad el uso de IPv6 no es muy representativo masivamente, pero su adopción en las redes va en aumento, por este motivo es imposible postergar la implementación de IPv6 por mucho más tiempo, ya que puede generar diferentes desventajas para el desarrollo de Internet.

Todos los días tenemos nuevas redes gracias a la expansión de las empresas, la convergencia de tecnologías y al surgimiento de nuevos negocios, el crecimiento de las redes 4G y el uso del Internet en dispositivos electrónicos son ejemplos de aplicaciones que contribuyen al crecimiento de la red.

7.4 PLAN DE CONTINGENCIA ANTE RIESGOS

El plan de contingencia permite evaluar y prevenir los riesgos, con la finalidad de garantizar una adecuada ejecución y funcionamiento del proyecto, asegurando un servicio continuo con una calidad apropiada. A continuación, se presenta en el cuadro 23 las acciones que se deben realizar para tratar de prevenir los riesgos descritos en el cuadro 21.

Cuadro 23. Acciones para minimizar o mitigar riesgos

Número	Acciones
1	Utilizar la documentación del software desarrollado y del manejo de los equipos.
2	Generación de protocolos o estándares de mantenimiento y soporte previo y continua al despliegue
3	Mantener actualizadas y alineadas las políticas de seguridad ante el nuevo protocolo
4	Adquirir o desarrollar las herramientas de software para el mantenimiento y monitoreo de la red apropiadas para todos los protocolos de la red
5	Respaldo de toda la información crítica de la entidad en dispositivos de almacenamiento confiables como discos duros, cd’s, etc.
6	Generar bases de conocimiento ante los eventos presentados que afecten la calidad de la red de comunicaciones y servicios
7	Definir los tiempos adecuados para las pruebas y seguimientos a los cambios realizados en la infraestructura en función del protocolo IPv6
8	Descargar todas las actualizaciones y complementos para el manejo adecuado de sistemas operativos en ambiente IPv6.
9	Garantizar que con el despliegue del protocolo se mantengan ambientes interoperables entre cada uno de sus componentes tecnológicos

Cuadro 23. (Continuación)

Número	Acciones
10	Validar los códigos de desarrollo y documentación generados o buscar alternativas a esas soluciones que sean compatibles.
Fuente: Elaboración propia	

7.5 DEFINICIÓN DEL PLAN DE TRABAJO

El proyecto tiene como meta final la implementación y transición del protocolo IPv4 a IPv6 dependiendo del nivel de compatibilidad y adaptación que posean los equipos, servicios tecnológicos, aplicaciones y demás sistemas de la entidad. Como paso inicial, siguiendo las recomendaciones del MinTic y las buenas prácticas de implementación del nuevo protocolo[66], se pretende realizar un despliegue mediante el mecanismo *de Dual-Stack* para garantizar la continuidad de los servicios y para poder monitorear y evaluar con datos precisos el comportamiento de IPv6 en la red del instituto y en las aplicaciones web ofrecidos hacia internet inicialmente. con base en lo anterior, y de acuerdo a la estrategia definida, se busca lograr finalmente una cobertura casi total en la red institucional para el proceso de transición, incluyendo equipos cliente, servidores, aplicaciones, telefonía, equipos activos, etc.

Teniendo en cuenta que la entidad se extiende con oficinas regionales por todo el país interconectadas la gran mayoría a través de una LAN extendida (MPLS), como primera medida se definió que el proceso de adopción de IPv6 inicia en el nivel central (*headquarter*) en la ciudad de Bogotá, en donde está ubicado el *datacenter* de la oficina de tecnologías de información, en el cual se enfocara el despliegue del protocolo inicialmente generando ambientes de prueba para validar compatibilidad de aplicaciones de negocio, verificación de disponibilidad de servicios, mecanismos de verificación de afinidad con políticas de seguridad, entre otros. Luego de los preliminares se realizará la habilitación del “camino” hacia las aplicaciones accesibles desde internet mediante IPv6, teniendo en cuenta todas las configuraciones de red y políticas de seguridad pertinentes, con lo cual se podrá generar el tráfico inicial en producción bajo dicho protocolo.

Un componente importante del proceso, es la solicitud de un pool de direcciones IPv6 al RIR correspondiente a nuestra zona geográfica (LACNIC), dicho procedimiento está contemplado realizarse una vez se surta con éxito y resultados

[66] IPv6 BEST PRACTICES Disponible en http://www.ipv6forum.com/dl/presentations/IPv6%20Best%20Practices%20eBook%202.pdf

un laboratorio de pruebas efectuadas sobre algunas de nuestras aplicaciones. Lo anterior, va a permitir a la entidad contar con un direccionamiento publico propio que lograra mantener las configuraciones a nivel de red para salida a internet independientemente del proveedor (ISP) que se tenga, teniendo en cuenta que anualmente se realizan procesos licitatorios para la contratación de éste.

A continuación, se presentan los análisis realizados sobre los factores más relevantes a tener en cuenta para el proceso de adopción del protocolo IPv6 en la red del instituto:

7.5.1 Análisis del factor técnico. En relación al recurso técnico necesario para abordar el proceso de adopción del nuevo protocolo, se evalúan a continuación los posibles escenarios que podrían darse al momento de la implementación, adicionalmente se describe todo lo relacionado con numeración y direccionamiento IPv6.

7.5.1.1 Escenarios de Transición a IPv6. El proceso de transición de IPv4 a IPv6 no es una tarea fácil, por este motivo se debe mantener una comunicación entre la versión actual y el protocolo IPv6, ya que tarde o temprano se deberá llevar a cabo un cambio completo de IPv4 a IPv6 sin la necesidad de afectar los servicios y aplicaciones de la red actual.

El objetivo de la transición no es remplazar los servicios IPv4 existentes, lo único que se trata de hacer es buscar diferentes escenarios para la adopción del protocolo y futura migración, ya que las instituciones modernas necesitan implementar lo último en tecnología con el fin de obtener mecanismos estables para que se puedan transmitir los datos y demás aplicaciones tanto en IPv4 como en IPv6.

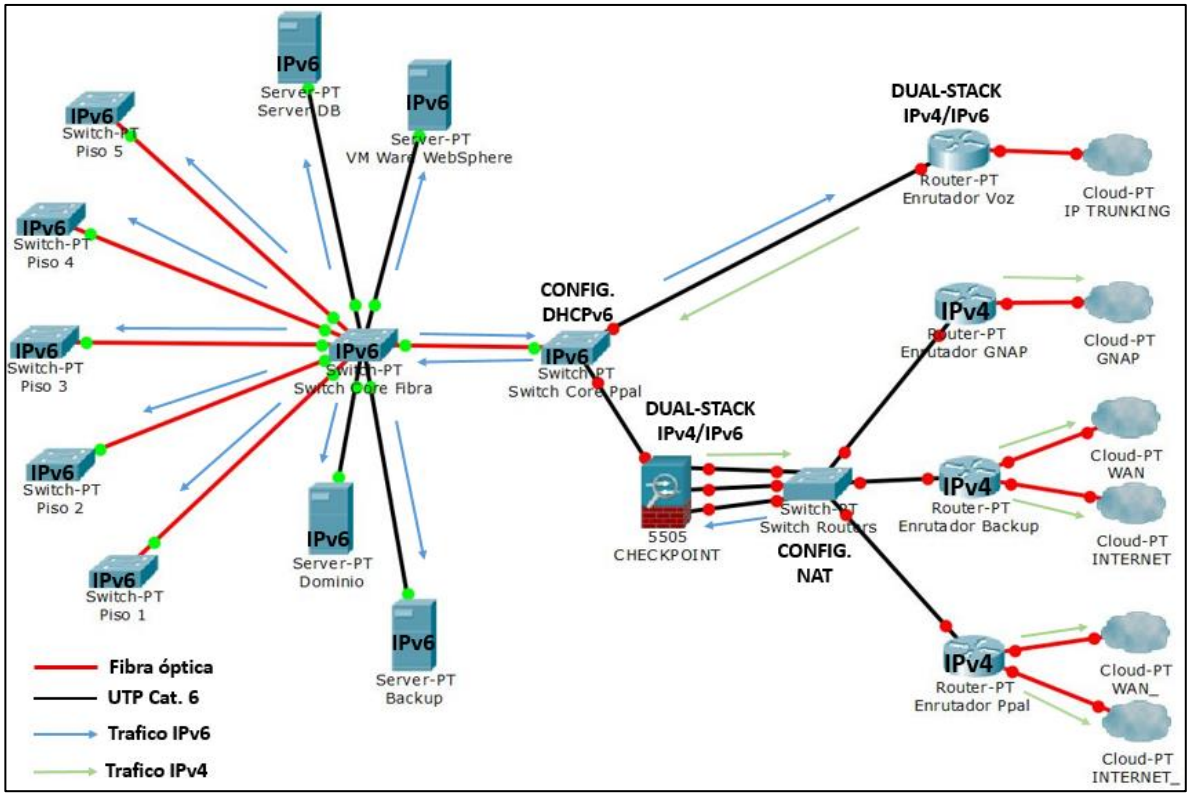
Como parte de las etapas descritas en …el numeral 7.1 …, a continuación, se presenta una descripción de los posibles escenarios para la adopción de IPv6 en la red del nivel central.

7.5.1.1.1 Primer escenario: Mantener IPv4 en fronteras e IPv6 en red local. El esquema que se propone permite activar la configuración IPv6 por medio de DHCPv6 en todos los equipos de red que se encuentran conectados al Switch principal hasta la conexión con el Firewall.

En el firewall Check Point y en el router de voz se establece una configuración del mecanismo Dual-Stack para permitir la comunicación de la red local de IPv6 a IPv4, además debe existir una configuración de NAT para permitir la “traducción” de las direcciones IPv4/IPv6.

Un ejemplo grafico de este esquema se puede ver en la figura 17:

Figura 17. IPv6 en la red local e IPv4 hacia internet



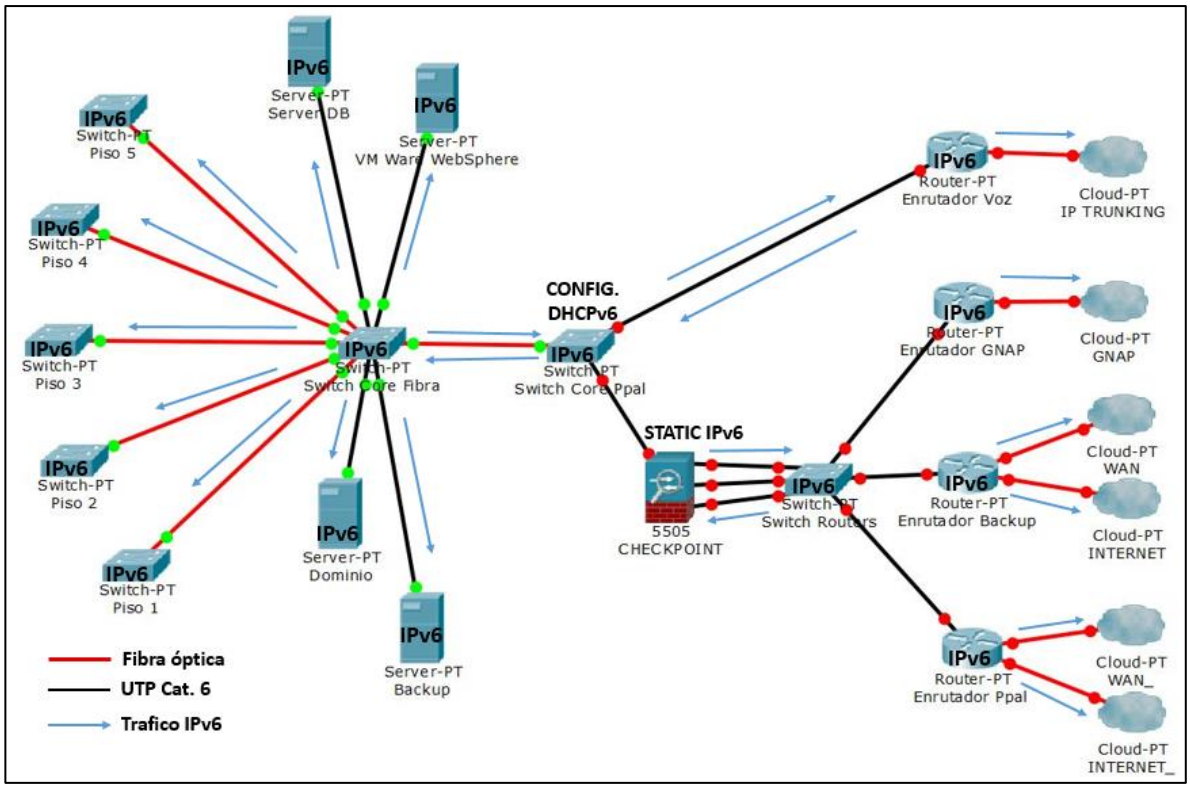
Fuente: Elaboración propia

7.5.1.1.2 Segundo escenario: IPv6 en fronteras e IPv6 en red local. El esquema que se propone es similar al primer escenario en donde tenemos que activar la configuración IPv6 por medio de DHCPv6 en todos los equipos de red que se encuentran conectados al Switch principal y a servidores hasta la conexión con el Firewall.

En este escenario estamos asumiendo que hacia afuera de los nodos de frontera (internet y otras redes) ya se encuentra funcionando completamente en IPv6, debido a esto para acceder al Internet desde nuestra red local, lo único que tenemos que hacer es configurar el Firewall utilizando un direccionamiento estático para IPv6.

En la figura 18, se presenta el diagrama del segundo escenario para la adopción del protocolo IPv6:

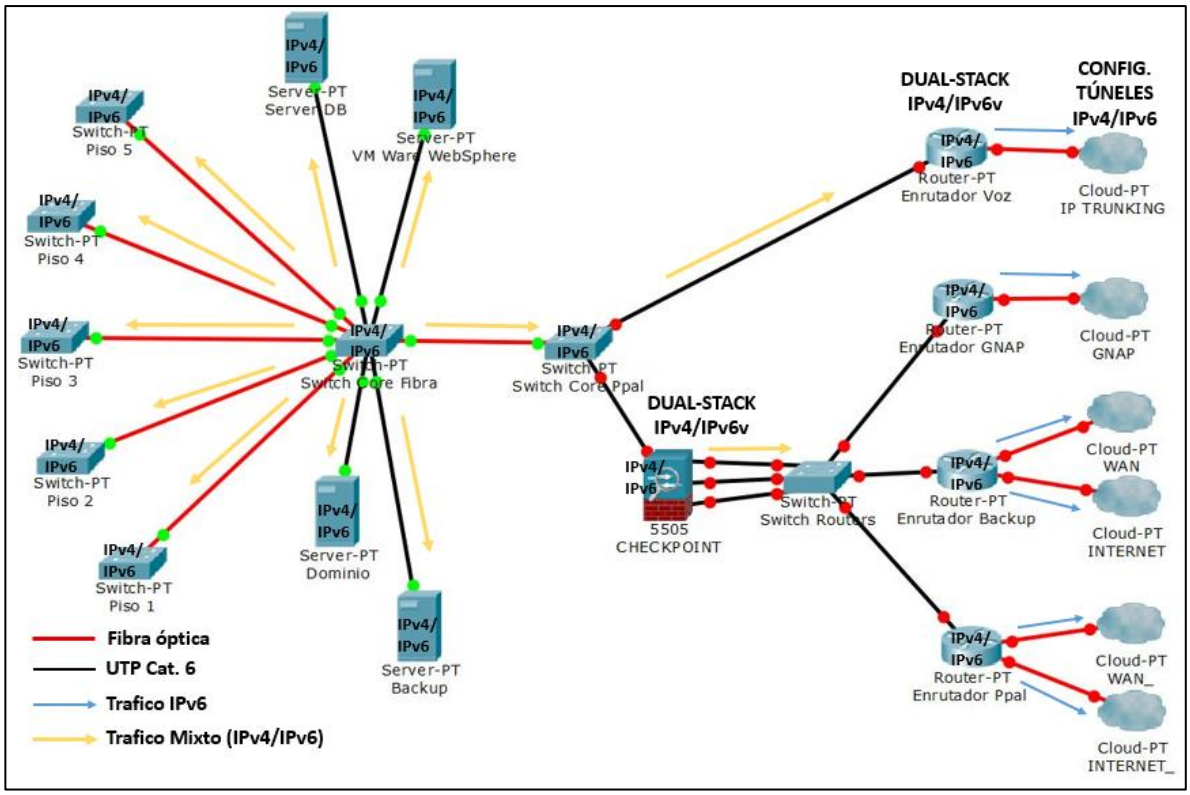
Figura 18. IPv6 en LAN y en salida a Internet y otras redes



Fuente: Elaboración propia

7.5.1.1.3 Tercer escenario: IPv6 en fronteras y mantener IPv4 e IPv6 en la LAN. Como último escenario planteado, se establecen las configuraciones en el Switch principal y en los servidores para que se genere tráfico de red mediante ambos protocolos en la red local, es decir, una configuración interna en doble pila (Dual-Stack), y por otro lado garantizar que el tráfico generado hacia internet sea sobre el protocolo IPv6, sin embargo el escenario también estaría habilitado para generar tráfico IPv4, para lo cual es necesario habilitar y configurar el protocolo en los routers de borde administrados por el proveedor de servicios de telecomunicaciones, además de otros mecanismos de transporte de datos como *tunelling* o traducción. Un ejemplo del diagrama de este escenario se puede observar en la figura 19:

Figura 19. Dual-Stack en la red LAN y salida a internet con túneles IPv4/IPv6



Fuente: Elaboración propia

7.5.1.2 Direccionamiento IPv6 en la red del instituto. Con base en las recomendaciones y guías para la adopción de IPv6 elaboradas por el MinTic para las entidades públicas, se requiere realizar una solicitud formal de recursos IP ante LACNIC, específicamente un prefijo IPv6 /48 mínimo para dar cobertura a todas las necesidades de la institución en ese sentido, lo cual por supuesto conlleva incurrir en destinación de recursos económicos inmediatos sin ningún tipo de retorno de inversión (ROI)[67] o beneficios fácilmente visibles. Por lo anterior, a manera de ejercicio práctico y con la finalidad de estipular un plan de direccionamiento en IPv6 para la red central de la entidad, se utiliza el siguiente prefijo supuesto para realizar asignaciones a equipos activos, servidores y equipos de usuarios:

2001:DB8:ABCD:: /48

[67] ROI, Return Of Investment. Obtenido el 15 de agosto de 2016. Disponible en http://www.gerencie.com/roi.html

Para la configuración de las direcciones IPv6 de cada equipo de usuario se utiliza el mecanismo de autoconfiguración por DHCP existente en IPv6, a excepción de los equipos de red como Switch, Router, Firewall en donde se realizó la asignación de direcciones IPv6 de forma manual para simplificar su configuración y administración.

A continuación, en la tabla 2, se describe el diseño básico del direccionamiento en IPv6 para los elementos de red en el nivel central (Oficinas Nacionales) del instituto teniendo en cuenta el *subneting* planteado por cada unidad administrativa:

Tabla 2. Subneting en IPv6 para red de nivel central

# Sitio	Nombre Sitio	# Sub-sitio	Nombre Sub-sitio	Prefijo	Sitio	Sub-Sitio	Subnet
1	Bogotá D.C.	1	Oficinas Nacionales	2001:DB8:ABCD:: /48	2001:DB8:ABCD:1000:: /56	2001:DB8:ABCD:1010:: /64	**Routers WAN** 2001:DB8:ABCD:1010:1000:: /72
							Routers Voz 2001:DB8:ABCD:1010:1100:: /72
							CORE 2001:DB8:ABCD:1010:1200:: /72
							Servidores 2001:DB8:ABCD:1010:1300:: /72
							Wireless 2001:DB8:ABCD:1010:1400:: /72
							Switch Piso 1 2001:DB8:ABCD:1010:1500:: /72
							Switch Piso 2 SUR 2001:DB8:ABCD:1010:1600:: /72
							Switch Piso 2 NORTE 2001:DB8:ABCD:1010:1700:: /72
							Switch Piso 3 SUR 2001:DB8:ABCD:1010:1800:: /72
							Switch Piso 3 NORTE 2001:DB8:ABCD:1010:1900:: /72
							Switch Piso 4 2001:DB8:ABCD:1010:1A00:: /72
							Switch Piso 5 2001:DB8:ABCD:1010:1B00:: /72

Fuente: Elaboración propia

Adicionalmente, por cada subred reservada se tiene disponible la cantidad de IPs para hosts mostradas en el cuadro 24, para el caso de las unidades administrativas en cada uno de los pisos del edificio se planea utilizar el protocolo DHCPv6:

Cuadro 24. Cantidad de IPs disponibles para host

Descripción	IPv6 de Host
IP inicial	2001:DB8:ABCD:1010:0000:0000:0000:0001 /72
IP final	2001:DB8:ABCD:1010:ffff:ffff:ffff:ffff /72
Cantidad disponible por subred	16.384
Fuente: Elaboración propia	

7.5.2 Análisis del factor económico. Dentro del proceso de adopción de protocolo IPv6 uno de los temas fundamentales son los costos de implementación debido a que la inversión necesaria se fundamenta en la obtención de bienes o servicios que formaran parte de la infraestructura actual o de una nueva.

Según Gartner, "se estima que el costo de convertir el entorno de una empresa de TI de IPv4 a IPv6 ronda el 6% del presupuesto anual total del departamento de TI de la empresa. Los costos fijos luego de realizada la conversión ascenderán aproximadamente el 1% del presupuesto de TI en los años siguientes, en comparación a los costos incurridos por la empresa si se hubiera mantenido la versión IPv4".[68] Para la entidad, a pesar de no ser una empresa de TI, estas cifras se traducen en un incremento del presupuesto destinado para el área de tecnologías de información que incluso supera esos porcentajes, teniendo en cuenta que la tendencia de los requerimientos necesarios y los factores analizados es una mayor demanda de recursos económicos importantes asignados.

Por otra parte, el análisis realizado en este factor consiste en evaluar los siguientes elementos:

[68] Budgeting for IPv6 migration. VAN DIJK, Sandra. (2011). Obtenido el 27 de Julio de 2016 Disponible en: http://www.computerworld.com.au/article/394612/ipv6_guide_part_2_budgeting_ipv6_migration/

- Numeración
- Software
- Hardware
- RR.HH.
- Capacitación

7.5.2.1 Costos para numeración IP. De acuerdo con las guías definidas por el MinTic, un requisito fundamental para que la entidad adopte adecuadamente el protocolo IPv6 es la solicitud y adquisición de un pool de direcciones IPv6 ante el Registro de Direcciones de Internet para América Latina y Caribe (LACNIC), con lo cual será posible que la entidad sea públicamente visible en internet con su propia numeración IP. En la tabla 3, se describe el costo de la asignación de recursos según LACNIC para entidades del sector gobierno:

Tabla 3. Costos de numeración IPv6

Descripción	Cantidad	Costo por asignación
Bloque de direcciones IPv6 /48	1	$ 7´310.000,00
Renovación anual	1	$ 1’750.000,00
Fuente: LACNIC. Disponible en: http://www.lacnic.net/web/lacnic/tabla-de-precios		

7.5.2.2 Costos de software. La oficina de tecnologías de información del instituto cuenta con software comercial (sistemas operativos, bases de datos, etc.) adquirido por contratos licitatorios y software a la medida creado internamente por los diferentes equipos de desarrollo del área. En el cuadro 25, se relacionan los principales sistemas comerciales y aplicaciones web en funcionamiento tanto en servidores como en máquinas cliente:

Cuadro 25. Análisis de costos de software

Software	Observación	Costo al implementar IPv6
GNU/Linux Debian 6 y 8	Estas distribuciones de software libre soportan IPv6 y se encuentran instaladas en algunos servidores, lo único que se debe realizar es descargar las actualizaciones buscando en Internet y almacenarlos en medios magnéticos.	$0

Cuadro 25. (Continuación)

Software	Observación	Costo al implementar IPv6
GNU/Linux Red Hat 6.5	Esta distribución de software libre soporta IPv6 y está instalada en el servidor de base de datos, lo único que se debe realizar es descargar las actualizaciones buscando en Internet y almacenarlos en medios magnéticos.	$0
Microsoft Windows Server 2000, 2003, 2008 y 2012	Sistemas operativos de los servidores físicos y virtuales totalmente compatibles con IPv6, únicamente se requiere configuración de red.	$0
Oracle	Este software es compatible con IPv6, lo único requerido son configuraciones específicas que pueden obtenerse de internet.	$0
Microsoft Windows XP, Vista, 7, 8 y 10	Estos S.O's de Microsoft soportan IPv6 y se encuentran instalados en las máquinas de los usuarios de la red, lo único que se debe hacer es activar el protocolo IPv6. La activación no tiene costo.	$0
SIGMA	Aplicación web desarrollada internamente para generar guías sanitarias de movilización animal. Técnicamente comprobado que es independiente de la capa de red.	$0
SISFITO	Técnicamente comprobado que es independiente de la capa de red.	$0
Intranet	Basado en servidor Microsoft SharePoint y CMS. No se requiere ninguna adaptación al protocolo IPv6	$0
Total		$0
Fuente: Elaboración propia		

7.5.2.3 Costos de hardware. De acuerdo a lo relacionado en el diagnóstico de la infraestructura …en el numeral 7.2 … es necesario tener en cuenta que, para garantizar una total cobertura del despliegue del protocolo en el nivel central de la institución (oficinas nacionales), es importante tener en cuenta el remplazo del hardware relacionado en el cuadro 26:

Cuadro 26. Análisis de costos de hardware

Equipo	Marca	Modelo	Observación	Costo al implementar IPv6[69]
Impresora	Lexmark	E220	Ubicada en atención al ciudadano Piso 1 Lado Norte	$8’000.000,00
	Kodak	13200 scanner	Ubicada en atención al ciudadano Piso 1 Lado Norte	$2´400.000,00
	HP	Deskjet 970CXI	Ubicada en Planeación Piso 2 lado sur	$6´890.000,00
Switch	Avaya	P330	Distribución horizontal pisos 1 y 3	$3´000.000,00
	Cisco	WS-C2960-24TC-L	Distribución horizontal piso 2	$4´000.000,00
Planta telefónica	Panasonic	TDE-100	Planta telefónica del programa “Identifica” en Bogotá	$15’000.000,00
Teléfono	Cisco	7940	Telefonía IP de oficinas nacionales	$1’300.000,00
	Panasonic	NT366	Telefonía IP de oficinas nacionales	$800.000,00
Total				**$41’390.000,00**
Fuente: Elaboración propia				

7.5.2.4 Costos de RR.HH. Uno de los puntos importantes para establecer la adopción del protocolo IPv6 en la infraestructura tecnológica y de comunicaciones del instituto son los costos de contratación de nuevo personal profesional y especializado, cuya mano de obra no será incluida para la implementación física y lógica del protocolo, debido a que la entidad cuenta con el personal calificado en el área de tecnologías de información para realizar estas labores bajo la dirección del jefe de la OTI para presentar calidad en los procesos de implementación.

Ahora bien, para determinar los costos asociados por recurso humano es válido enunciar el costo en horas-hombre al llevar a cabo la implementación por los

[69] Valores de referencia en el mercado al año 2016.

ingenieros que componen la oficina de tecnologías en el área de infraestructura y redes de la siguiente manera:

A (Cantidad de horas laboradas en un día por trabajador) = 8
B (Cantidad de días laborados en un mes por trabajador) = 22
C (Total horas por trabajador (A x B)) = 176

D (Cantidad de trabajadores en el área) = 8

E (Cantidad total horas-hombre (C x D)) = 1408

F (Salario promedio en pesos colombianos) = $4.515.000

Al verificar la cantidad de horas-hombre empleadas de 1408 horas divididas entre 8 trabajadores, se puede concluir que:

Costo hora-hombre (F/C) = $4.515.000/176 = **$25.653**

La planeación realizada para la implementación del proyecto sugiere una inversión de tiempo considerable. Como se indicó en capítulos anteriores, la implementación del protocolo IPv6 en la infraestructura de red y comunicaciones es un proceso lento y dispendioso, sin embargo y con base en lo anterior es posible estimar el costo estimado para este rubro de acuerdo a las horas-hombre requeridas para cada una de las etapas de implementación y que están discriminadas …en el anexo A … (cronograma de implementación) de la siguiente manera:

T1 = Tiempo estimado primera etapa = 7,5 meses (1.320 horas-hombre)

T2 = Tiempo estimado segunda etapa = 6,13 meses (1.078 horas-hombre)

T3 = Tiempo estimado tercera etapa = 8,06 meses (1.419 horas-hombre)

Tiempo total (T1 + T2 + T3) = 3817 horas-hombre

Costo total del RR.HH. estimado = $25.653 x 3817 = **$97’917.501,00**

Nota: En el cálculo de la cantidad de meses empleados en cada etapa se tiene en cuenta el calendario de días laborales y horas-hombre de 176 horas al mes.

7.5.2.5 Costos de capacitación. Otro de los aspectos relevantes para tener en cuenta en cuanto a la inversión económica que se requiere para la implementación del proyecto en la institución son las pruebas de funcionamiento y capacitación del personal técnico. Las pruebas de funcionamiento están contempladas en la fase 3 del proyecto, sin embargo, se deben hacer laboratorios de pruebas durante la fase

de implementación para poder validar funcionalidad del software tanto comercial como propio de la entidad, un ejemplo de estos laboratorios se puede observar …en el anexo B …, como se mencionó en secciones anteriores.

Para la capacitación en IPv6 es deseable que las personas involucradas puedan acceder a cursos, seminarios o certificaciones de nivel básico para abordar el proceso de implementación adecuadamente, algunos de estos serían gratuitos y no representarían inversión económica para la entidad, sin embargo, para el caso de requerir certificaciones el personal técnico con el apoyo deseable de la entidad debe incurrir en el coste de estas ya sea virtualmente o en academias autorizadas en Colombia, teniendo en cuenta la normatividad de contratación pública por prestación de servicios en Colombia.

Se relacionan en la tabla 4, los costos estimados para lo relacionado con ejecución de periodos de prueba y capacitaciones:

Tabla 4. Análisis de costos para capacitación y pruebas

Descripción	Unidad	Cantidad	Costo por unidad	Valor
Pruebas de funcionamiento	Horas	2190	$4.862,00*	$10’645.833,00
Capacitación personal técnico para manejo de IPv6	Horas	60	$61.680,00**	$3’712.00,00
	Total			**14’357.833,00**
Fuente: Elaboración propia				

* Calculo basado en el costo por hora mensual de un profesional contratista de la OTI con ingreso básico de $3,500.000 pesos colombianos
** Calculo basado en la certificación “IPv6 Forum Course & Certified Network Engineer (Silver)”. Disponible en: http://www.academiaipv6.org/index.php/cursos/silver-course-engineer

7.5.2.6 Inversión final. Es muy importante considerar un porcentaje adicional del 20% para los gastos de imprevistos debido a que en algunos casos puede ser necesario la contratación de un agente externo como proveedores o contratistas para el asesoramiento en configuraciones técnicas y procesos complejos, además se debe tomar en cuenta que los costos de software, hardware y capacitación son valores aproximados y en cualquier momento puede ser necesario una modificación cuando se esté llevando a cabo el proceso de transición hacia IPv6.

En la tabla 5 se describen dichos costos en pesos colombianos:

Tabla 5. Costos asociados a la implementación de IPv6

Costo asociado	Valor
Costos de Numeración	$ 7’310.000,00
Costos de Software	$ 0,00
Costos de Hardware	$ 41’390.000,00
Costos de RR.HH.	$ 97’917.501,00
Costos de Capacitación	$ 14’357.833,00
Imprevistos (20%)	$ 32’195.067,00
Costo total de implementación	**$ 193’170.401,00**
Fuente: Elaboración propia	

Teniendo en cuenta lo anterior, es necesario indicar que el recurso económico necesario para llevar a cabo el proyecto depende en su totalidad de las decisiones del ordenador del gasto de la entidad y las áreas financieras y contractuales que disponen directamente de los presupuestos y planes de compra que se presentan por las demás unidades administrativas de la institución, en este caso la oficina de tecnologías de información es la encargada de solicitar los registros presupuestales que incluyan anualmente los rubros estipulados para el desarrollo del proyecto en cada una de sus etapas.

7.5.3 Análisis del factor humano. El capital humano es el recurso primordial de cuyas habilidades, formación y experiencia depende asegurar la creación y sostenimiento de las ventajas competitivas de la empresa. Por ello, el análisis de los recursos humanos se convierte en una función trascendental, evaluando su estructura y cualificación para contribuir a la consecución de los objetivos y estrategias de la empresa[70].

En ese sentido, la oficina de tecnologías de información (OTI) de la institución está compuesta por diversos grupos de profesionales y especialistas en la rama de tecnologías de información y telecomunicaciones, dentro de estos se encuentra el

[70] COLOMER, Eduardo. “El análisis de empresas: Análisis de recursos humanos” (2012) Disponible en: http://www.mirelasolucion.es/blog/analisis-empresas-recursos-humanos/

grupo de “Infraestructura Tecnológica y Redes” integrado por profesionales en ingeniería y especialistas encargados del despliegue, soporte y mantenimiento de todo lo relacionado con la red y comunicaciones del instituto, todos ellos bajo la supervisión del jefe de la OTI. El anterior grupo mencionado, será el encargado del desarrollo, pruebas y seguimiento del proyecto de adopción de IPv6. Sin embargo, de acuerdo a un sondeo a través de un test de 15 preguntas realizado sobre conocimientos generales del protocolo IPv6 …véase anexo C … se pudo comprobar que, aunque ellos no cuentan con experiencia en proyectos relacionados con el tema, sí poseen los conocimientos básicos requeridos, las capacidades y la disposición para llevar a cabo el proyecto adecuadamente desde todos sus ángulos. El cuadro 27 corresponde a la descripción del equipo de trabajo con sus respectivos roles definidos para el proyecto:

Cuadro 27. Roles del equipo humano del proyecto

Cantidad de personas	Rol en el proyecto	Profesión	Cargo/Área
1	Director del proyecto	Ingeniero de Sistemas / Especialista en Telecomunicaciones	Jefe de la oficina de tecnologías de información
2	Conectividad y documentación	Ingeniera electrónica e Ingeniero de sistemas	Oficina de tecnologías de información
3	Servidores, *firewall*, aplicaciones de negocio y servicios	Ingenieros de sistemas	Oficina de tecnologías de información
2	Telefonía sobre IP	Ingeniera electrónica	Oficina de tecnologías de información
2	Gestión de seguridad y auditoria	Ingenieros de sistemas / Especialistas en auditoría	Oficina de tecnologías de información
Fuente: Elaboración propia			

8. CONCLUSIONES

Durante el desarrollo de este proyecto de grado se logró analizar, diseñar y realizar un plan de implementación para la adopción de IPv6 tomando como información referencial la red central del instituto, se plantearon algunos escenarios posibles de implementación para abordar desde la planeación, para esto se determinó utilizar el mecanismo de transición Dual-Stack, el cual permite conectar las distintas unidades administrativas y ofrecer servicios web a internet mediante el protocolo IPv6, sin la necesidad de utilizar mecanismos de transición complejos.

La transición hacia IPv6 debe realizarse de manera gradual, por este motivo es necesario establecer un periodo de transición y coexistencia entre los dos protocolos con el fin de reducir el impacto sobre el funcionamiento de la red.

Una vez culminado el proceso de transición de IPv4 a IPv6, la entidad no tendrá que preocuparse por el agotamiento de las direcciones IP pues se garantizará que la infraestructura de TI, debe seguir en línea ofreciendo a los usuarios múltiples oportunidades de seguir conectados y apuntar a los nuevos mercados que surgen alrededor de IPv6.

El análisis de los factores más relevantes en la fase de planeación (factor técnico, económico y humano) permitieron identificar y dimensionar aspectos clave respecto a la factibilidad de las siguientes fases de implementación y pruebas.

De acuerdo con el análisis del factor económico el costo más representativo, después del costo asociado al RR.HH., para la inversión requerida por parte de la entidad corresponde a los elementos de hardware de la infraestructura de red que deben ser renovados para garantizar una cobertura total en la adopción del protocolo, tanto en el nivel central como en las diferentes seccionales del instituto.

Para la implementación del mecanismo de transición Dual-Stack es necesario habilitar el servicio DNS con la finalidad de resolver nombres y direcciones para los dos protocolos, en el caso de IPv6 se requiere responder a consultas de registros tipo AAAA (Quad - A).

Con la adopción del protocolo IPv6 se podrá seguir construyendo soluciones tecnológicas más confiables, permitiendo que la seguridad de las aplicaciones mejore con su adopción y que la red de comunicaciones y los sistemas de

información de la entidad se beneficie gradualmente de acuerdo a los lineamientos establecidos en la circular 002 del 2011 del MinTic, que pretende impulsar su aplicabilidad, en un ambiente de planificación, ejecución y operación con un mínimo de criticidad posible para todos los entes gubernamentales del país.

9. RECOMENDACIONES

Para una implementación mejor controlada y adecuada a las necesidades, es recomendable en las etapas iniciales realizar la configuración de IPv6 solo en los nodos y elementos de la red que lo requieran, y no hacer un despliegue a todo simultáneamente, ya que existen muchos servicios y dispositivos que continuaran trabajando sobre la pila IPv4, por lo cual la mejor opción es utilizar el método de transición Dual-Stack.

El protocolo IPv6 tiene asociado un gran componente teórico que requiere una gran cantidad de conocimiento, por este motivo el personal técnico del área de tecnologías de la entidad debe tomarse el tiempo necesario para capacitarse y realizar un estudio completo en el tema, en lo posible poder tomar cursos y certificaciones que les permitan tener un alto nivel de compresión al momento de desarrollar las soluciones para IPv6.

Con el objetivo de generar ambientes de pruebas y validaciones técnicas y funcionales mediante laboratorios ya sea virtuales o con equipos físicos, sin que esto implique la obligatoriedad de la adquisición de recursos de numeración IPv6 ante LACNIC, se recomienda solicitar a futuros proveedores de conectividad un pool de direcciones IPv6 a través de los pliegos de contratación que se definan.

Habilitar las capacidades del protocolo IPv6 solo en los componentes de la red que lo requieran y de igual manera “apagar” IPv6 donde no se esté usando, teniendo en cuenta que posiblemente un número determinado de programas o elementos físicos ya han sido configurados para trabajar con IPv6, y otros tantos ya tienen el protocolo encendido de forma automática por defecto. Es preferible comprobar una, dos y tres veces el entorno de la red para asegurarse que IPv6 sólo está disponible cuando realmente está siendo usado.

Toda la fase de implementación debe ir alineada con las políticas de seguridad definidas en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) que actualmente está en desarrollo en la entidad, con la finalidad de garantizar un alto nivel de confiabilidad en las practicas desarrolladas a lo largo del despliegue del protocolo IPv6 en la red.

BIBLIOGRAFÍA

Páginas Web

CHAPTER 37 Configuring IPV6 ACLs, s/f, http://www.cisco.com/en/US/docs/switches/metro/me3400/software/release/12.2_50_se/configuration/guide/swv6acl.pdf.

CHAPTER 38 Configuring IPV6 ACLs, s/f, http://www.cisco.com/en/US/docs/switches/lan/catalyst3750x_3560x/software/release/12.2_55_se/configuration/guide/swv6acl.pdf

CHAPTER 13 Configuring VLAN ACLs, s/f http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_vlanacls.pdf

CCNA Security, 2009, http://es.scribd.com/doc/65202776/CCNA-Security-Espanol Características de IPv6, 2011, http://www.redesymas.org/2011/06/caracteristicas-principales-de-ipv6.html

Configuración Routing / resumen comandos, s/f, http://www.6deploy.org/workshops/20100927_bogota_colombia/DIA3-3-routing-Help_Commands_Cisco.pdf

IPv6 Access Lists on IOS, Junio 2010, http://packetlife.net/blog/2010/jun/30/ipv6-access-lists-acl-ios/

Las empresas no están listas para IPV6, s/f, http://www.ipv6.mx/index.php/informacion/noticias/1-latest-news/106-enterprisenotreadyipv6

Listas de Control de Acceso VLAN, s/f, http://es.scribd.com/doc/58116973/12/Listas-de-Control-de-Acceso-VLAN.

Migramos la red a IPv6, s/f, http://quepagina.es/internet/migramos-la-red-a-ipv6.html

Que es una Red Backbone, s/f, http://wifiw.com/1625/que-es-una-red-backbone.html#ixzz1ZpJf3p1e

Uso de IPv6 situación actual y perspectivas del futuro, Internet Society, s/f, http://www.internetsociety.org/sites/default/files/ipv6-way-forward-es.pdf.

Router Cisco: Configuración básica, s/f,
http://es.kioskea.net/faq/2759-router-cisco-configuracion-basica

AHUATZIN, Gerardo, Desarrollo de un esquema de traducción de direcciones IPV6-IPV4-IPV6, s/f,
http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo3.pdf

CASTRO, Gabriel, Introducción de IPV6 en Telecom Argentina, 2010,
http://lacnic.net/documentos/presentaciones/lacnicxiv/TelecomArgentinaIPv6.pdf

CEDIA, Curso IPv6, enero 2010,
http://dspace.cedia.org.ec/bitstream/123456789/44/2/cedia%20ipv6%20curso.pdf

CISCO, CCNA Security 1.0 Implementación de seguridad en redes, s/f,
http://es.scribd.com/doc/34759326/Ccna-Security-Ins

CISCO, Deploying IPv6 in Campus Networks, febrero 2012,
http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/CampIPv6.html#wp390438.

CISCO, Adding an IPv6 Access List, s/f,
http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/acl_ipv6.html#wpxref69804.

CISCO, Configuring IPv6 ACLs, s/f,
http://www.cisco.com/en/US/docs/switches/blades/3110/software/release/12.2_40_ex2/configuration/guide/swv6acl.html

CISCO, CCNA ICND2 Guía Oficial para el examen de Certificación Segunda edición, España, 2008, http://es.scribd.com/doc/79514092/17/Creacion-de-VLANs-y-asignacion-de-VLANs-de-acceso-a-una-interfaz.

CISCO, Cisco Self-Study: Implementing Cisco IPv6 Networks (IPv6), 2003,
http://www.ciscopress.com/articles/article.asp?p=31948&seqNum=4

CISCO, DHCPv6 Using the Prefix Delegation Feature Configuration Example, 2011,
http://www.cisco.com/en/US/tech/tk872/technologies_configuration_example09186a0080b8a116.shtml

CISCO, Implementing Traffic Filters and Firewalls for IPv6 Security, 2011,
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-sec_trfltr_fw.html#wp1073622.

CISCO, Implementing IPv6: Addressing, Routing, and Dual Stacking, 2011,
https://learningnetwork.cisco.com/thread/31918

CISCO, IPv6 NAT-PT, 2011, https://supportforums.cisco.com/thread/2092027

CISCO, IPv6 IPv4 Network Interconnection NAT-PT, 2011, https://supportforums.cisco.com/thread/2131296

CISCO, Understanding Simple Network Management Protocol (SNMP) Traps, 10 de Octubre de 2006, http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094aa5.shtml

COMPUTER NETWORKING, How to configure routing with IPv6 step by step guides, 2011, http://computernetworkingnotes.com/ipv6-features-concepts-and-configurations/routing-with-ipv6.html

COMPUTER WORLD, Como migrar a IPv6, 2011, http://www.networkworld.es/Como-migrar-a-IPv6/seccion-atualidad/noticia-111664

EGIDO, Fernando, Como realizar la migración a IPV6 en seis sencillos pasos, s/f, http://www.muycomputerpro.com/2011/04/26/migracion-ipv6-seis-pasos/

ECURED, Calidad de servicio, 12 de septiembre de 2012, http://www.ecured.cu/index.php/Calidad_de_servicio.

GAGLIANO, Roque, Planificando IPv6, s/f, http://lacnic.net/documentos/lacnicxii/presentaciones/Planificacion.pdf

GUERRERO, Alejandro, Tutorial Voz IP Packet Tracer, Julio 2011, http://www.wcruzy.pe/ri/ptvozip.pdf

LACNIC, FAQ sobre IPV6, s/f, http://portalipv6.lacnic.net/es/ipv6/novedades/preguntas-frecuentes-faq

LACNIC, IPV6 en el Ambiente Académico, s/f, http://portalipv6.lacnic.net/es/ipv6/ipv6-en/ambiente-acad-mico-0

MICROSOFT, Descubrimiento de Vecinos (ND), n.d, http://technet.microsoft.com/es-es/library/cc778019%28v=ws.10%29.

MILLAN, Ramón, El protocolo IPV6, 2001, http://www.ramonmillan.com/tutoriales/ipv6_parte1.php

MILLAN, Ramón, SNMPv3 (Simple Network Management Protocol versión 3), 2003, http://www.ramonmillan.com/tutoriales/snmpv3.php

ORACLE, Capítulo 3 Introducción a IPv6 (Descripción general), s/f, http://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-7/index.html

PALET, Jordi, Manual para la transición de IPv4 a IPv6, 2011, http://www.baquia.com/posts/2011-03-21-manual-para-la-transicion-de-ipv4-a-ipv6

RAMIREZ, Sergio, Introducción al IPV6, 2005, http://www.rau.edu.uy/ipv6/queesipv6.htm

SANTAMARIA, Pilar, "Si una empresa no migra a IPv6 su web no podrá estar accesible, 2012", s/f, http://www.muycomputerpro.com/2012/06/05/santamaria-cisco-empresa-migra-ipv6-web-accesible/

SKIBBZ, Configure a static IPv6 address on a network, 2012, http://skibbz.com/step-by-step-guide-on-how-to-configure-a-static-ipv6-address-on-a-network-device-interface-and-implementation-of-ospf-routing-protocol/

STONESOFT, Diez consejos para implementar IPV6 de forma segura, s/f, http://www.muycomputerpro.com/2012/07/03/consejos-implementar-ipv6-segura/

VERISIGN, Lanzamiento mundial del IPv6, s/f, http://www.verisigninc.com/es_LA/why-verisign/innovation-initiatives/ipv6/index.xhtml

IPv6 PARA TODOS. Guía de uso y aplicación para diversos entornos. 1ra ed. – Buenos Aires: Asociación Civil Argentinos en Internet, 2009. http://www.ipv6tf.org/pdf/ipv6paratodos.pdf

IPv6 BEST PRACTICES. Disponible en: http://www.ipv6forum.com/dl/presentations/IPv6%20Best%20Practices%20eBook%202.pdf

MECANISMOS DE TRANSICIÓN. Disponible en: http://portalipv6.lacnic.net/mecanismos-de-transicion/

LACNIC, Estado de IPv4 a fin de 2012. Disponible en: http://portalipv6.lacnic.net/estado-de-ipv4-a-fin-de-2012-es/

ANEXOS

Anexo A. Cronograma del plan de implementación de IPv6.

	Modo de	Nombre de tarea	Duración	Comienzo	Fin
1					
2		**Plan de implementacion para adopción de IPv6 en la red del ICA**	**937 días**	**lun 1/02/16**	**mar 3/09/19**
3		**1. Estrategia**	**282 días**	**lun 1/02/16**	**mar 28/02/17**
4		Documentar la formulación básica del proyecto	21 días	lun 1/02/16	lun 29/02/16
5		Definir la metodología de trabajo	15 días	mar 1/03/16	lun 21/03/16
6		Reunión exploratoria con equipo de trabajo del ICA y MinTic	1 día	mar 3/05/16	mar 3/05/16
7		Realizar laboratorios de pruebas iniciales sobre aplicaciones de negocio	36 días	mié 1/06/16	mié 20/07/16
8		Ajustar lo requerido de acuerdo a pruebas iniciales para garantizar operatividad de aplicaciones sobre IPv6	82 días	lun 25/07/16	mar 15/11/16
9		Pruebas con Pool de direcciones IPv6 del proveedor del servicio de conectividad	30 días	mié 18/01/17	mar 28/02/17
10		**2. Adquisición de pool de direcciones IPv6 ante LACNIC**	**62 días**	**mié 1/03/17**	**jue 25/05/17**
11		**2.1 Establecer necesidades de adoptar una direccion IPv6**	11 días	mié 1/03/17	mié 15/03/17
12		**2.2 Presentar solicitud de recursos ante LACNIC de acuerdo a requisitos**	**51 días**	**jue 16/03/17**	**jue 25/05/17**
13		Definir propuesta detallada de planes de enrutamiento, incluyendo protocolos a usar	29 días	jue 16/03/17	mar 25/04/17
14		Definir propuesta de asignacion de recursos en la red (plan de direccionamiento)	8 días	mié 26/04/17	vie 5/05/17
15		Generar descripcion detallada de la topologia de red	8 días	lun 8/05/17	mié 17/05/17
16		**2.3 Recepción de recursos IPv6 para la red del ICA**	6 días	jue 18/05/17	jue 25/05/17
17		**Primera etapa (IPv6 en fronteras de red - salida a internet y servidores web)**	**163 días**	**jue 1/06/17**	**lun 15/01/18**
18		**3. Asignación de direcciones IPv6**	**25 días**	**jue 1/06/17**	**mié 5/07/17**
19		3.1 Identificar y adecuar nodos principales en la red central del ICA	15 días	jue 1/06/17	mié 21/06/17
20		3.2 Definición de tablas de enrutamiento y direcciones IPv6 estaticas para cada nodo principal	10 días	jue 22/06/17	mié 5/07/17
21		**4. Actualización de nodos para funcionamiento con IPv4/IPv6**			
22		4.1 Verificación y descarga de OS's de cada equipo de red	15 días	lun 10/07/17	vie 28/07/17
23		4.2 Actualización y pruebas de funcionamiento firewall	15 días	mar 1/08/17	lun 21/08/17
24		**5. Implementación del mecanismo de transición**	**104 días**	**mié 23/08/17**	**lun 15/01/18**
25		5.1 Revisión de los mecanismos de transición	10 días	mié 23/08/17	mar 5/09/17
26		5.2 Implementación del mecanismo Dual-Stack	20 días	jue 7/09/17	mié 4/10/17
27		5.3 Pruebas técnicas y funcionales	51 días	lun 6/11/17	lun 15/01/18
28		**Segunda etapa (IPv6 en red LAN de headquarter - Oficinas nacionales)**			
29		**6. Asignación de direcciones IPv6**	**26 días**	**mar 16/01/18**	**mar 20/02/18**
30		6.1 Identificar y adecuar nodos principales en la red central del ICA	15 días	mar 16/01/18	lun 5/02/18
31		6.2 Definición de configuraciones y direccionamiento IPv6 para cada nodo	10 días	mié 7/02/18	mar 20/02/18
32		**7. Actualización de nodos para funcionamiento con IPv4/IPv6**	**30 días**	**jue 1/03/18**	**mié 11/04/18**
33		7.1 Verificación y descarga de O.S's de cada equipo de red	15 días	jue 1/03/18	mié 21/03/18
34		7.2 Actualización y pruebas de funcionamiento de firewall	15 días	jue 22/03/18	mié 11/04/18
35		**8. Implementación del mecanismo de transición**	**120 días**	**lun 16/04/18**	**vie 28/09/18**
36		8.1 Implementación del mecanismo Dual-Stack	10 días	lun 16/04/18	vie 27/04/18
37		8.2 Habilitar servicios IPv6 necesarios (DHCP, DNS, WEB, MAIL, entre otros)	20 días	jue 26/04/18	mié 23/05/18
38		8.3 Pruebas técnicas y funcionales	90 días	lun 28/05/18	vie 28/09/18
39		**Tercera etapa (IPv6 en enlaces WAN con oficinas principales (Antioquia, Santander, Tolima, Bolivar y Cesar))**	**242 días**	**lun 1/10/18**	**mar 3/09/19**
40		**9. Asignación de direcciones IPv6**	**35 días**	**lun 1/10/18**	**vie 16/11/18**
41		9.1 Identificar y adecuar nodos conectados a la red MPLS de oficinas seccionales	25 días	lun 1/10/18	vie 2/11/18
43		**10. Actualización de nodos para funcionamiento con IPv4/IPv6**	**60 días**	**lun 5/11/18**	**vie 25/01/19**
44		10.1 Verificación y descarga de O.S's de cada equipo de red	30 días	lun 5/11/18	vie 14/12/18
45		10.2 Actualización y pruebas de funcionamiento	30 días	lun 17/12/18	vie 25/01/19
46		**11. Implementación del mecanismo de transición**	**152 días**	**lun 4/02/19**	**mar 3/09/19**
47		11.2 Implementación del mecanismo Dual-Stack por cada nodo de oficina	60 días	lun 4/02/19	vie 26/04/19
48		11.3 Pruebas técnicas y funcionales	90 días	mié 1/05/19	mar 3/09/19

DIAGRAMA DE GANTT

DIAGRAMA DE GANTT

Anexo B. Acta del laboratorio de validación IPv6 en aplicaciones (SISFITO)

ACTA – No 003 de 2016	

Motivo Reunión	**Quien cita**	
Laboratorio de verificación IPv6 en aplicaciones (Sisfito)	OTI	
Objetivo	**Fecha:**	21/06/2016
Efectuar las pruebas necesarias para validar la afinidad de aplicaciones de negocio con el protocolo IPv6	**Lugar:**	OTI
	Hora:	9:00 a.m. a 12:00 m.
	Notas por:	Henry De la Hoz
	Próxima Reunión:	**26/07/2012**

AGENDA
Se llevó a cabo el laboratorio de pruebas en un ambiente controlado con las siguientes características: • Máquina virtual Windows Server 2012 64bits (DHCP) • Máquina virtual Windows Server 2012 64bits (DNS + AD) • Máquina virtual Debian Linux 64bits (SISFITO, Maria DB – Apache - PHP) Una vez preparado el setup, se siguió el procedimiento previamente planeado para la realización de las pruebas (asignación automática de IPs, comunicación cliente-servidor, resolución de nombre, acceso a aplicación por IPv6, pruebas de funcionalidad). Para esta ocasión se puso a prueba la aplicación SISFITO con una copia de la base de datos, para probar el comportamiento de la aplicación en ambiente IPv6, inicialmente, se debía verificar la parametrización los componentes de la aplicación, de lo cual quedo configurado con dual-stack el servidor web apache y el motor de base de datos MARIA DB, sin embargo, quedó pendiente para una próxima sesión de pruebas verificar la funcionalidad de la aplicación. A continuación, se pueden observar las evidencias de lo realizado: Servidor 1: Se realizaron las configuraciones para habilitar el servidor con dual-stack (IPv4/IPv6) IPv4: 10.10.21.2 IPv6: 2001:db8:abcd:3f00::2/64

Controlador de Dominio **pruebas.com**:

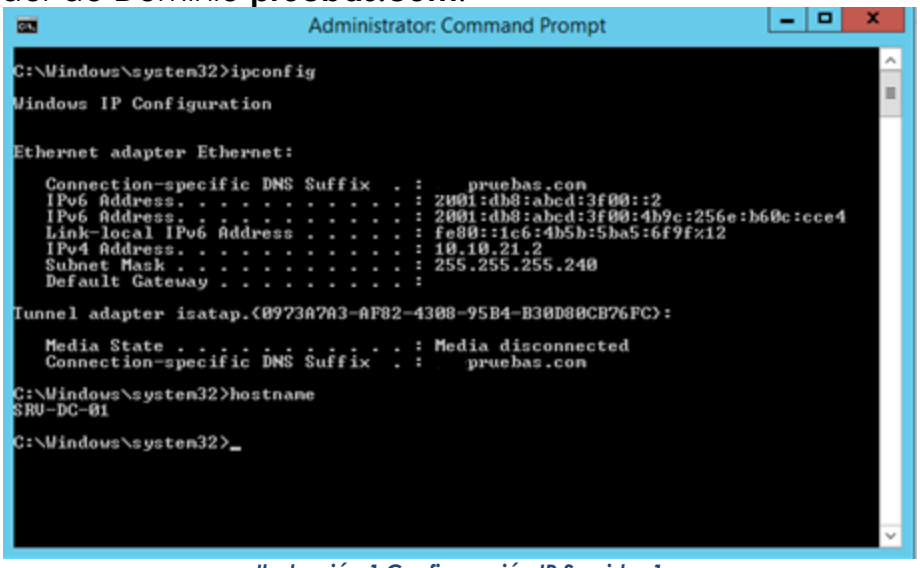


Ilustración 1 Configuración IP Servidor 1

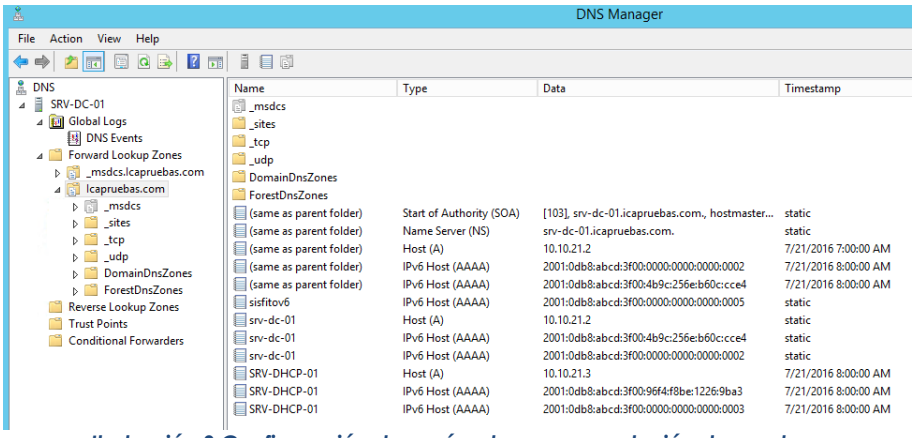


Ilustración 2 Configuración de parámetros para resolución de nombres

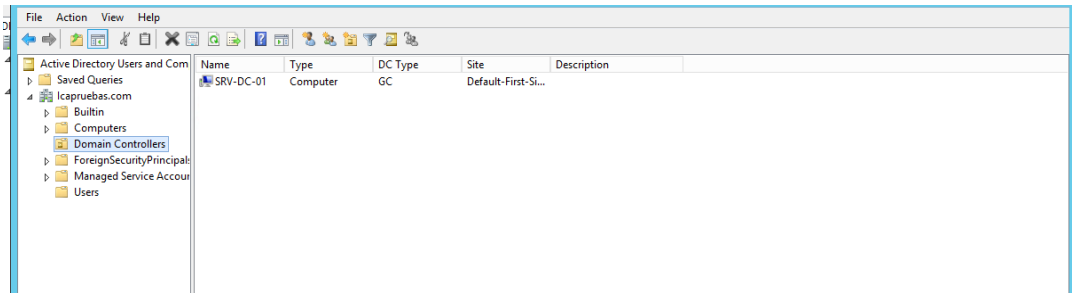


Ilustración 3 Controlador de dominio

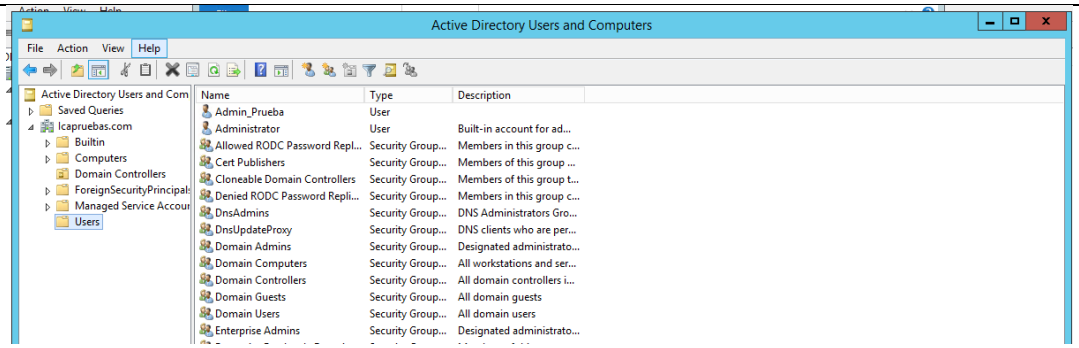


Ilustración 4 Usuarios y grupos del dominio

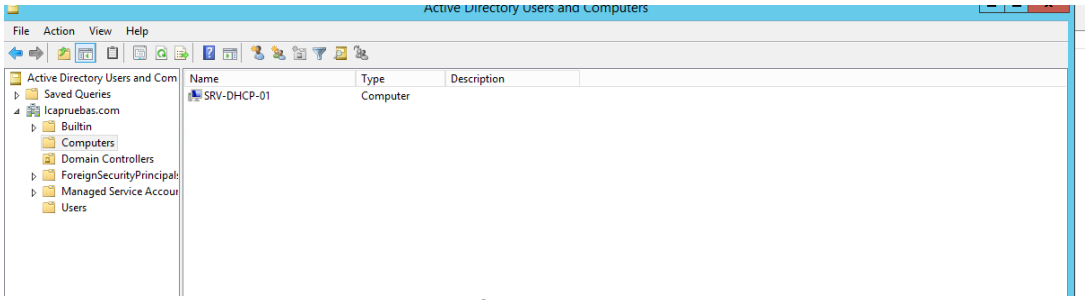


Ilustración 5 Servidor DHCPv6

Servidor 2: Se realizaron las configuraciones para habilitar el servidor con dual-stack (IPv4/IPv6)

IPv4: 10.10.21.3
IPv6: 2001:db8:abcd:3f00::3/64

DHCP **pruebas.com**:

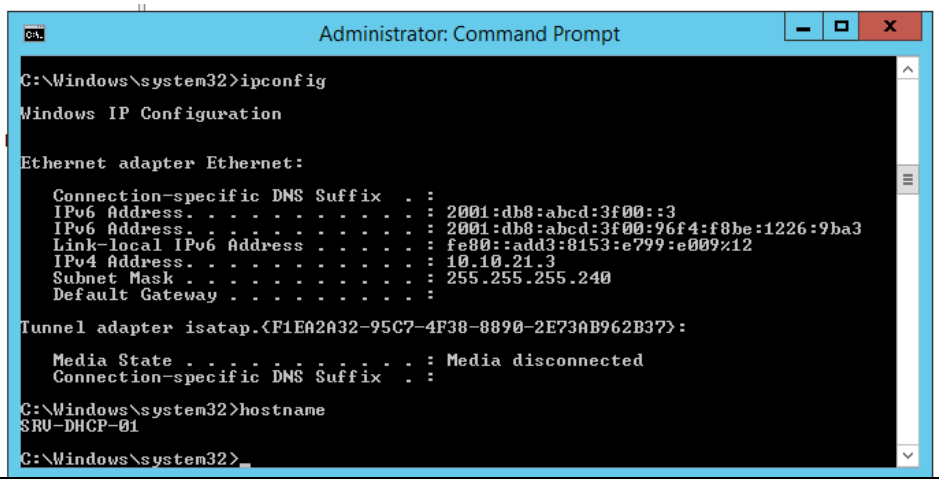


Ilustración 6 Ilustración 1 Configuración IP Servidor 2

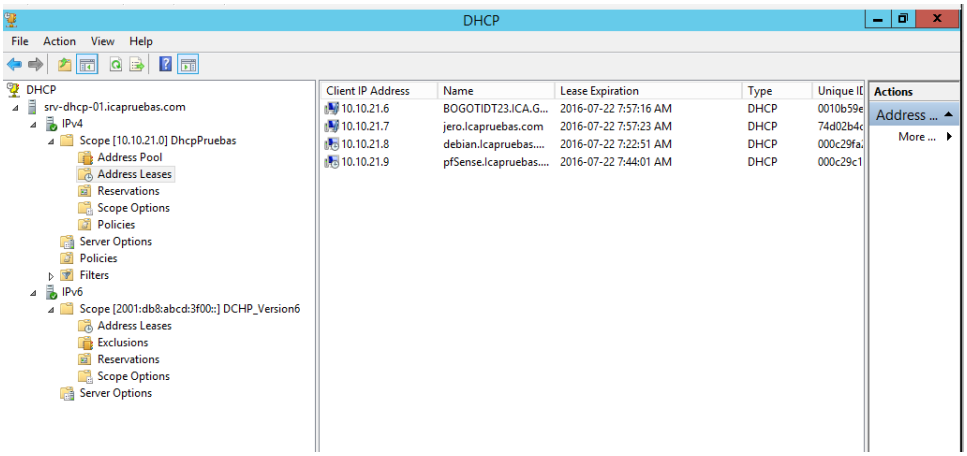


Ilustración 7 Listado de máquinas con IPs versión 4 asignadas

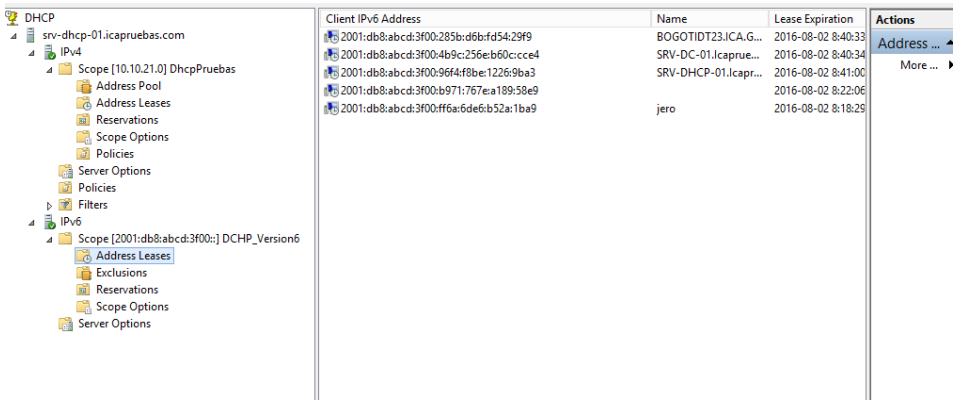


Ilustración 8 Ilustración 7 Listado de máquinas con IPs versión 6 asignadas

Servidor 3: Se realizaron las configuraciones del Apache y Maria DB requeridas para que la aplicación SISFITO fuera accesible mediante el stack IPv6.

IPv4: 10.10.21.7
IPv6: 2001:db8:abcd:3f00::5/64

Apache con app **SISFITO**:

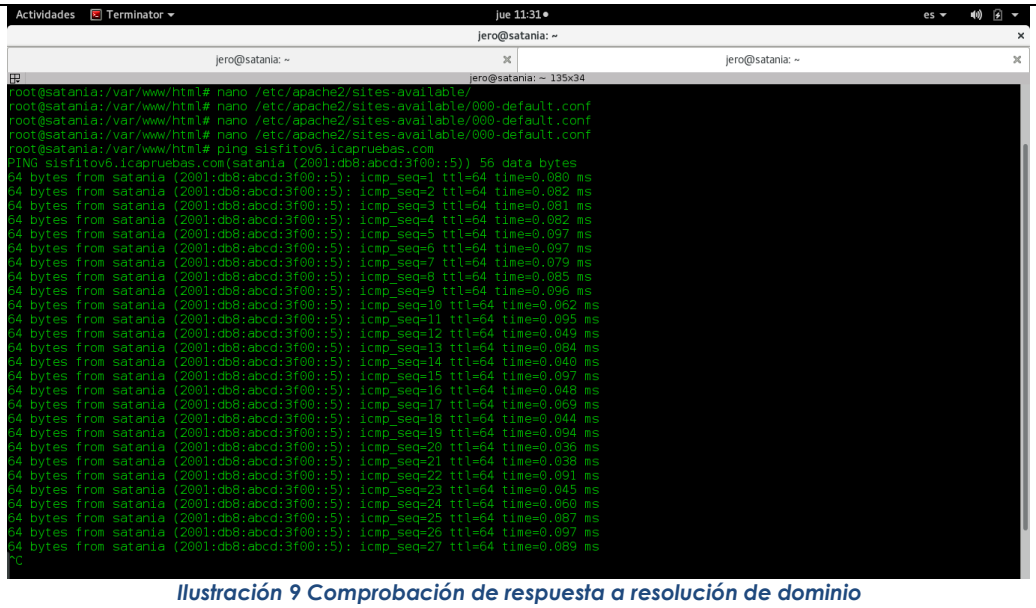


Ilustración 9 Comprobación de respuesta a resolución de dominio

Se realizó la parametrización pertinente al servidor Apache para que respondiera a solicitudes a través de IPv6.

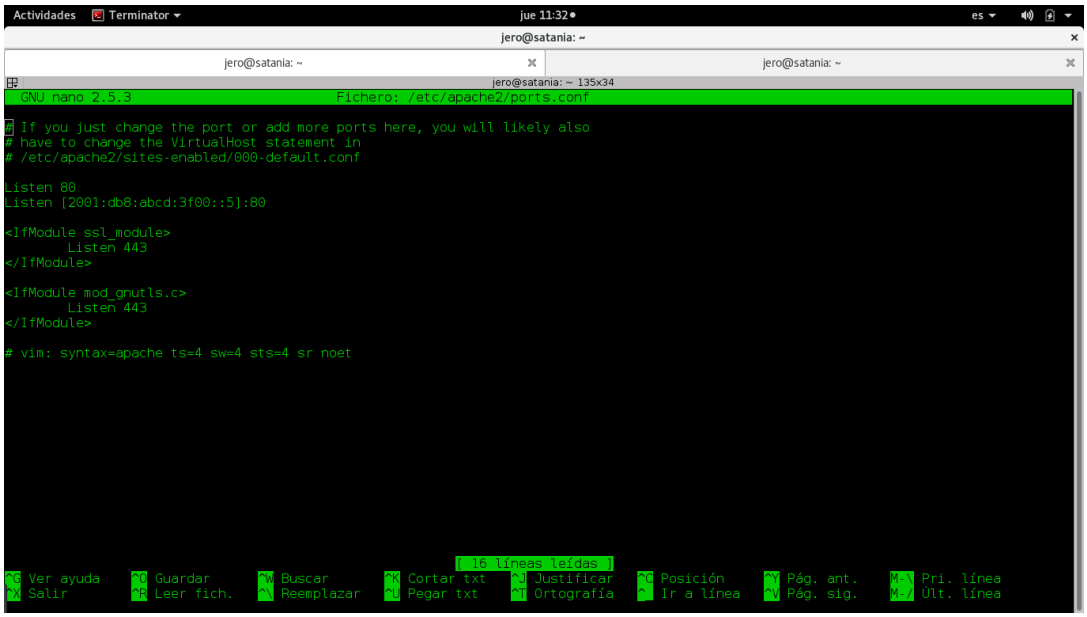


Ilustración 10 Configuración Apache2

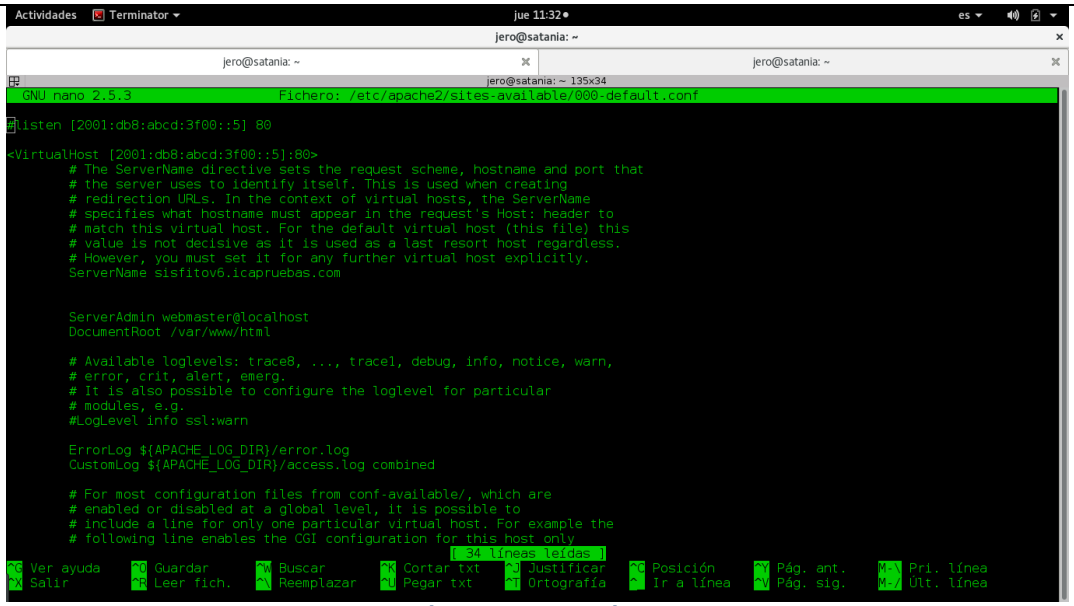


Ilustración 11 Configuración Apache2

Prueba de acceso mediante IPv6:

Al realizar solicitud bajo protocolo http y con un ping a la IPv6 de la maquina con el servicio web (2001:db8:abcd:3f00::5/sisfito/web) se obtuvo respuesta satisfactoria como se puede ver a continuación:

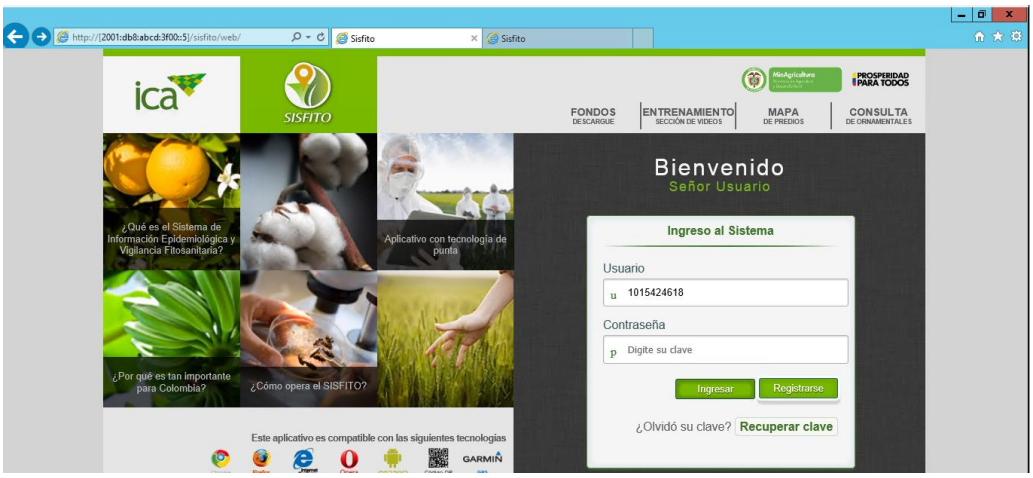


Ilustración 12 Respuesta del servicio solicitado alcanzado mediante la IPv6

El mismo resultado se obtuvo al realizar la solicitud mediante URL o nombre de dominio (http://sisfitov6.epruebas.com/sisfito/web/):

Ilustración 13 Respuesta del servicio solicitado alcanzado mediante nombre de dominio

APROBACIÓN DE LOS DECISIONES TOMADAS POR PARTE DE LOS ASISTENTES:

Nombre	Firma
Hector Odilio Cristancho	
Jorge Enrique Rojas	
Dimelza Carolina Rozo	
Henry Alberto De la Hoz	

Anexo C. Cuestionario de conocimientos básicos de IPv6[71]

Cuestionario realizado a funcionarios del área de tecnologías del instituto con una serie de preguntas técnicas para que desde la dirección del proyecto y ellos mismos pudieran evaluar sus conocimientos en IPv6.

Elige todas las opciones que creas válidas en cada respuesta:

1) ¿Cuántos bits usa una dirección IPv6?
a. 32-bits
b. 64-bits
c. 256-bits

[71] CASTILLO, Javier. (2015) ¿Cuánto sabes de IPv6? Obtenido el 26 de junio de 2016. Disponible en: http://itblog.a-e.es/test-ipv6/

d. 128-bits

2) Verdadero o Falso: IPv6 es compatible con IPv4
a. Verdadero, ambos son IP
b. Falso, es totalmente incompatible
c. Verdadero, algunos protocolos si funcionan, como el ARP

3) IPv6 define varios tipos de direcciones. De las siguientes, ¿cuál no se implementa en IPv6?
a. Anycast
b. Multicast
c. Broadcast
d. Unicast

4) IPv6, dentro de las direcciones Unicast, define 3 tipos de subconjuntos, cada uno con un uso espec ífico. ¿Cuáles son esos 3 subconjuntos?
a. Global, Link-Local, Unique-Local
b. Global, Internet, Subnet
c. Internet, Subnet, Superset
d. Global, Link-Local, Site-Local

5) Una dirección IPv6, se puede representar de distintas formas. De las siguientes, ¿cuáles son válidas?
a. 2001:0db8:0000:0000:0000:0000:1428:57ab
b. 2001:0db8::1428:57ab
c. 2001::1685:2123::1428:57ab
d. 2001:99:ab:1:99:2:1:9
e. 2001:1428:57ab:1685:2123:1428:57ab

6) ¿Cuál es la dirección de Loopback en IPv6?
a. ::127
b. ::1
c. ::FF
d. ::255

7) ¿Cuál es el prefijo de una dirección de tipo Link-Local?
a. FE80
b. FF00
c. 2002
d. FC00

8) ¿Cómo se crea una dirección IPv6 tipo Link-Local?
a. Es una combinación del prefijo FE80, 54 bits a 0, y un identificador IPv6 de 64bits
b. Se generan aleatoriamente, con el prefijo FFCC
c. Se generan aleatoriamente, con el prefijo FF00

d. Se usa la dirección MAC del equipo, y poniendo un prefijo FF00

9) Un Router que tiene configurado IPv4 e IPv6 simultáneamente en un interfaz, se dice que está configurado como:
a. 6to4
b. 4to6
c. NAT-PT
d. ISATAP
e. Dual-Stack

10) ¿Qué protocolo en IPv6 cumple (y extiende) las funciones del protocolo ARP de Ipv4?
a. ARPv6
b. DHCPv6
c. NDP
d. En IPv6 ya no es necesario relacionar direcciones IPv6 con direcciones MAC

11) De las siguientes máscaras de red, ¿cuáles son válidas?
a. /128, define un Host
b. /127, un enlace punto a punto, como los /30 de IPv4
c. /126, para pequeñas subredes de solo 4 IPs IPv6
d. /64, la máscara que permite 2^64 máquinas en una subred cualquiera, por pequeña que sea

12) En IPv4, la forma de asignar una dirección IP a un interfaz, es mediante configuración manual, o DHCP. En IPv6, los métodos disponibles son:
a. Manual
b. DHCPv6
c. Stateless Address Autoconfiguration

13) En IPv4, los problemas de MTU son resueltos por los nodos intermedios o routers, mediante el uso de la fragmentación del paquete IP. En IPv6:
a. No es necesario nunca fragmentar
b. El comportamiento es igual que en IPv4, fragmentan los routers del camino
c. Son los equipos extremos (PC/Servidor por ejemplo), los que han de conocer la MTU del path completo, y lidiar con los posibles problemas de fragmentación.
d. Con enviar paquetes de 1200bytes ya funcionar ía todo.

14) En IPv4, el uso de la traducción de direcciones ó NAT44, permite el usar direccionamiento no válido en INET dentro de una empresa y a la vez navegar por internet usando una IP pública. En IPv6:
a. No existe el NAT66, las direcciones Unicast-Global no se pueden someter a NAT
b. Si existe un mecanismo igual, para facilitar el despliegue de IPv6

15) El protocolo de resolución de nombres de Internet ó DNS, en IPv4 define los registros tipo ‘A’ para traducir un nombre a una IP(v4). En IPv6, se tiene que:
a. Se siguen usando los registros A para traducir un nombre a una dirección IPv6
b. Se usan los registros AAAA
c. Se usan los registros Av6
d. Se usan los registros TXT

Resultados del test aplicado al equipo.

Tabla 6. Resultados del test de conocimientos en IPv6 a equipo de trabajo

Nombre	Calificación (Respuestas correctas/Número de preguntas)
Ing. Dimelza Rozo	9/15
Ing. Henry De la Hoz	12/15
Ing. Hector Cristancho	8/15
Ing. Jorge Rojas	12/15
Ing. Oswaldo Saumet	13/15
Ing. Bibian Peña	9/15
Ing. David Espinoza	8/15
Ing. Rosa Ortega	7/15
Fuente: Elaboración propia	