Análisis y desarrollo del protocolo IPv6 en la red de datos de la Defensoría del Pueblo Regional Cesar

Jorge Carlo Jiménez Paredes

Asesor

Iván Camilo Nieto Sánchez

Universidad Nacional Abierta y a Distancia - UNAD Escuela de Ciencias Básicas, Tecnología e Ingeniería - ECBTI

Maestría en Gestión de Tecnología de la Información

2025

Dedicatoria

A mi Dios que me permite avanzar en mi vida personal y profesional, a mi familia; esposa e hijos quienes se convirtieron en el apoyo fundamental para este logro.

Agradecimientos

A la Universidad Nacional Abierta y a Distancia UNAD, por abrirme sus puertas y así poder prepararme como Magister en Gestión de Tecnología de la Información.

A mi director de proyecto, Mg. Iván Camilo Nieto Sánchez por sus consejos acertados en cada paso del camino.

A todas aquellas personas y compañeros que contribuyeron de diversas maneras a construir este proyecto.

Resumen

Este proyecto tiene como propósito principal planificar la transición del protocolo IPv4 a IPv6 en la Defensoría del Pueblo – Regional Cesar, en cumplimiento de la Resolución 1126 de 2021 del MinTIC. La iniciativa se justifica por la necesidad de resolver problemas de conectividad, seguridad y agotamiento de direcciones IPv4, además, de fortalecer la infraestructura tecnológica de la entidad.

Se identifican múltiples falencias en la red actual, como la limitada cobertura del acceso a Internet y lentitud en los servicios digitales. A través del diagnóstico se encontró que el 89% del hardware y software ya es compatible con IPv6, y se sugieren actualizaciones mínimas.

El proyecto está estructurado en dos fases, la fase I – Planeación, incluye inventario de TI, diagnóstico de compatibilidad, análisis de topología, políticas de seguridad y plan de direccionamiento IPv6. En cuanto a la fase II – Desarrollo del plan de implementación, la simulación del direccionamiento, configuración de servicios como DNS y VPN, y activación de IPv6 en aplicaciones y dispositivos de red en coordinación con el proveedor ISP. Así mismo, se propone el uso de doble pila (dual stack) para garantizar la coexistencia entre IPv4 e IPv6 y una estrategia de capacitación del personal de TI. También se formulan lineamientos de seguridad acordes con la normativa institucional.

Este plan no solo busca cumplir con los requerimientos normativos del MinTIC, sino también establecer un modelo replicable en otras sedes de la Defensoría a nivel nacional, contribuyendo así a la transformación digital del sector público en Colombia.

Palabras clave: IPv6, Transición, Protocolo, Doble Pila, Activo de Información

Abstract

This project's main objective is to plan the transition from the IPv4 protocol to IPv6 at the Ombudsman's Office – Cesar Regional Office, in compliance with Resolution 1126 of 2021 issued by MinTIC. The initiative is justified by the need to address issues related to connectivity, security, and the exhaustion of IPv4 addresses, as well as to strengthen the entity's technological infrastructure.

Several shortcomings have been identified in the current network, such as limited internet access coverage and slow digital services. Through the assessment, it was found that 89% of the hardware and software is already compatible with IPv6, with only minimal upgrades suggested.

The project is structured in two phases. Phase I – Planning, includes an IT inventory, compatibility assessment, topology analysis, security policies, and an IPv6 addressing plan. Phase II – Implementation Plan Development, involves addressing simulation, service configuration such as DNS and VPN, and activation of IPv6 in applications and network devices in coordination with the ISP. Additionally, the use of dual stack is proposed to ensure coexistence between IPv4 and IPv6, along with a training strategy for IT personnel. Security guidelines aligned with institutional regulations are also formulated.

This plan not only aims to meet MinTIC's regulatory requirements but also to establish a replicable model for other branches of the Ombudsman's Office nationwide, thereby contributing to the digital transformation of Colombia's public sector.

Keywords: IPv6, Transition, Protocol, Dual Stack, Information Asset

Tabla de Contenido

Lista de tablas

Lista de figuras

Lista de Apéndices

Introducción

En Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones – en adelante MinTIC, es la entidad encargada de regular la adopción del protocolo IPv6, para lo cual ha establecido en el artículo 1 – plazo de adopción – de la Resolución 1126 del 14 mayo de 2021, entre otros aspectos, exigir a las entidades públicas y privadas elaborar el plan de transición entre las tecnologías IPv4 e IPv6, y como fecha máxima de entrega para las entidades estatales de carácter nacional el 30 de junio de 2022, es decir, esto aplicaría para la red de datos de la Defensoría del Pueblo – Regional Cesar. El MinTIC, también ha establecido una Guía de Transición que tiene por objetivo principal *presentar un marco de referencia para facilitar el proceso de transición de IPv4 a IPv6, que permita orientar a las Entidades del Gobierno y a la sociedad en general, en el análisis, la planeación, la implementación y las pruebas de funcionalidad del protocolo IPv6, con el fin de incentivar el proceso de adopción y despliegue del protocolo IPv6 en el país*. (MinTIC, 2021, p. 11).

Este proyecto también tiene en cuenta el problema de la conectividad a través de Internet y los diversos servicios que se ofrecen por dicho medio y la posibilidad latente que las direcciones IP disponibles en todo el globo no cubran la necesidad en constante crecimiento y demanda, además de las vulnerabilidades de los datos e información que por allí se envían y reciben. Y de igual manera, minimizar el impacto que pueda acarrear no realizar la transición con sus altos costos y también el desarrollo de nuevas aplicaciones.

Así mismo, la temática esbozada tiene su apoyo en la Gestión de TI a través de las diversas metodologías tales como ITIL (IT Infrastructure Library, biblioteca de infraestructura de TI), COBIT (Control Objectives for Information and related Technology, Objetivos de Control para Información y Tecnologías Relacionadas), CMMI (Capability Maturity Model Integration,

Integración de sistemas modelos de madurez de capacidades), entre otros, y en especial, a través del Manual de Gobierno en Línea, que en su componente de Privacidad y Seguridad de la Información incluye el Modelo de Seguridad y Privacidad de la Información (MSPI), y para ello cuenta con una serie de guías anexas que ayudan a las entidades a cumplir lo solicitado permitiendo abordar de una manera detallada cada una de las fases del modelo, buscando a su vez comprender cuáles son los resultados a obtener y cómo desarrollarlos, incluyendo los lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano, tal y como se menciona en el portal del Fortalecimiento de la Gestión TI del Estado.

Lo anterior permite analizar la misión, visión y objetivos estratégicos de una organización y con el apoyo del área de TI realizar los ajustes pertinentes a los procesos internos aportando valor a la empresa y a los usuarios que acuden en busca de los servicios.

Justificación

El proyecto se enmarca en la línea de profundización: Tecnología de la Información como valor estratégico para las organizaciones, fomentando un clima de eficiencia y confianza entre los ciudadanos que solicitan los servicios de la entidad, y adicionalmente, la satisfacción de estos. Lo anterior, a través del uso de herramientas tecnológicas actuales, mitigando las falencias evidenciadas.

La Defensoría del Pueblo es una entidad gubernamental del orden nacional que hace parte del ministerio público y a su vez de los órganos de control, entre sus principales funciones se encuentran:

- La promoción y divulgación de los derechos humanos.
- Atender, orientar y asesorar en el ejercicio de sus derechos.
- Proveer el acceso a la administración de justicia, en los casos señalados en la ley.

En la actualidad se utiliza una plataforma misional llamada Visión Web, en la cual se lleva el registro de todos los peticionarios y los distintos servicios que solicitan a la entidad tales como:

- Registro Único de Peticiones (RUP)
- Atención y Trámite de Quejas (Solicitud, Queja)
- Recursos y Acciones Judiciales (Litigio defensorial)
- Defensoría Pública (Áreas penal y no penal, Representación judicial o extrajudicial)
- Víctimas del conflicto armado (Ley 1448/2011 - SIIJIT)
- Asesoría
- Mediación, conciliación y coadyuvancia (Defensoría del Pueblo, s.f)

información general, SiSAT, Paloma Mensajera (Intranet), Vivanto, SIIJIT, telefonía IP (Avaya), videoconferencias (Polycom), gestión documental, entre otros, los cuales se acceden a través de un canal dedicado de 15 Mbits de ancho de banda, el cual es subutilizado dado que luego de llegar al router se conecta a un punto de acceso que convierte la señal en inalámbrica (WiFi) con los inconvenientes de fallos recurrentes de conexión, lentitud, pérdida de datos, posibles intrusiones y robos de información, demoras en atención a los peticionarios y traumatismos.

El Ministerio de Tecnologías de la Información y las Comunicaciones, en función de lo dispuesto en el Marco de Referencia de Arquitectura Empresarial, la Estrategia de Gobierno en Línea y la Subdirección de Seguridad y Privacidad de TI, pone a disposición de las entidades, la siguiente guía, la cual permite a las entidades contar con una línea base para el análisis de la implementación del modelo de seguridad, privacidad e IPv6, de esta manera ayudar a proteger los bienes, activos, servicios, derechos y libertades dependientes del Estado.

(MinTIC, 2016, p. 20).

Por todo lo enunciado anteriormente se hace imperante la elaboración del plan de transición de IPv4 a IPv6 que comprende las Fases I y II, para la red de datos de la Defensoría Del Pueblo Regional Cesar, el cual garantizará el acceso oportuno y ágil, así como la seguridad y la privacidad de la información de los usuarios del servicio. Dicho protocolo (IPv6) también permite un mayor número de direcciones disponibles pero escalables, es decir, ayuda a organizar y estructurar la red de datos ahora y hacia el futuro crecimiento. De igual manera garantiza la disponibilidad, confiablidad e integridad de la información, así como el aprovechamiento de nuevas tecnologías. Teniendo en cuenta la “Ley del Habeas Data”. (Dinero, 2013)

Objetivos

Objetivo General

Construir un plan para la transición del protocolo IPv6 en la red de datos de la Defensoría del Pueblo Regional Cesar, utilizando las fases I y II de la guía del Ministerio de Tecnologías de la Información y las Comunicaciones.

Objetivos Específicos

Identificar los requerimientos físicos y técnicos a partir del inventario TI existente, evaluando la posibilidad de una transición satisfactoria al protocolo IPv6.

Valorar la situación actual de la Defensoría del Pueblo Regional Cesar en cuanto a la implementación de IPv6, estableciendo el grado de preparación de la organización respecto al nuevo protocolo.

Evaluar la configuración del protocolo IPv6 en aplicativos, sistemas de comunicaciones, sistemas de almacenamiento y en general de los equipos susceptibles a emplear direccionamiento IP a través de un software de pruebas.

Proponer un modelo de implementación flexible como aporte a la transición hacia IPv6 en otras sedes de la Defensoría del Pueblo.

Planteamiento del Problema

Descripción del Problema

Actualmente, la Defensoría Del Pueblo Regional Cesar presenta falencias de carácter tecnológico relacionado con el acceso oportuno a los sistemas de información misional, así como a los diversos servicios que requieren de la red de redes - Internet para su normal funcionamiento, tales como: Vision Web y SiSAT, correo electrónico, sistema de gestión documental, telefonía basada en IP, videoconferencias, entre otros. Además, el cumplimiento de garantizar el tratamiento y la seguridad de los datos de los usuarios del servicio. Adicionalmente, cuenta con una red de datos inalámbrica que ante la concurrencia de usuarios solicitando los servicios de acceso a Internet y a las distintas plataformas requeridas genera cuellos de botella y largas filas para recibir asesoría y atención personalizada, lentitud en la prestación del mismo servicio y desistimiento de parte de los peticionarios por las demoras.

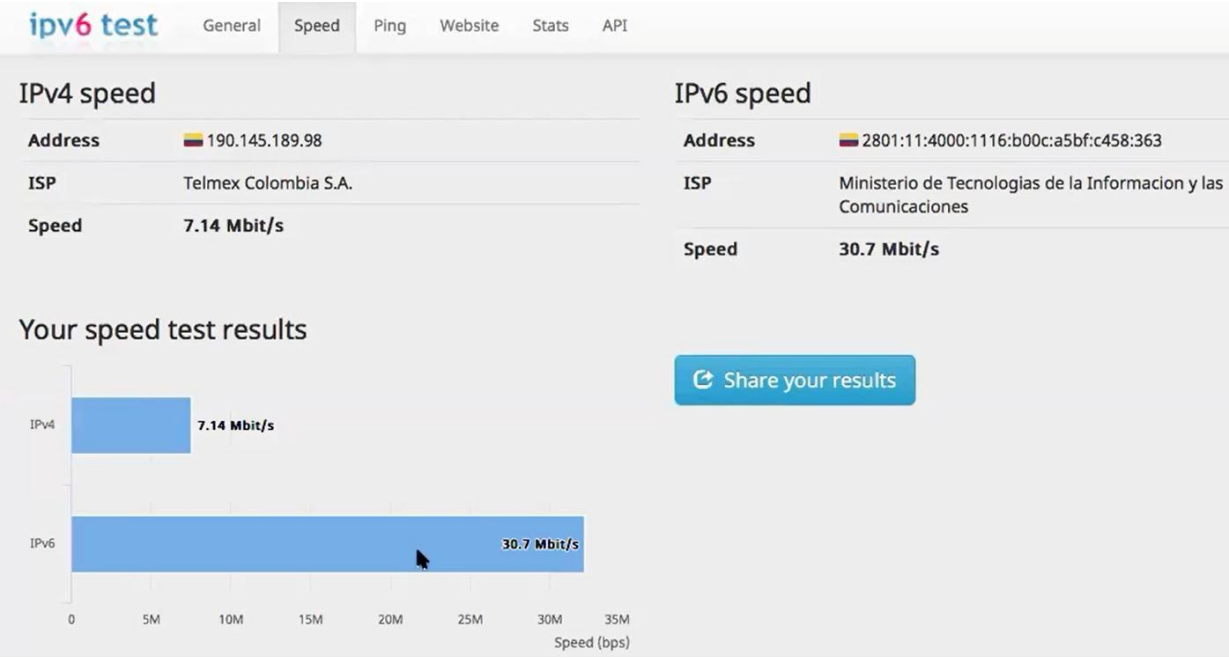
Una consecuencia notoria de no contar con el protocolo IPv6 son las amenazas de posibles ataques cibernéticos que pueden dejar a la institución sin información y sin datos; phishing a través de correo electrónico, ransomware como WannaCry, entre otras. Con una implementación adecuada del protocolo IPv6; considerada una tendencia disruptiva, se reducirán los tiempos de acceso al aplicativo misional y de esta manera atender oportuna y eficazmente a los peticionarios del servicio; salvaguardando la integridad de los datos y la información que éstos suministran.

En la Figura 1 se demuestra de manera clara, a través de una prueba de velocidad realizada por MinTIC; quienes ya tienen implementado IPv6 en su red de trabajo, que el protocolo IPv6 es 4 veces más veloz que su predecesor, IPv4. Pasando de una velocidad de transmisión de 7.14 Mbit/s a 30.7 Mbit/s. Este es un caso de éxito en el país que al implementar

comunicación. Además, brindan apoyo a todas las empresas públicas y privadas que requieran el servicio como acompañamiento durante el proyecto de transición e implementación.

Figura 1

Comparativa Velocidad

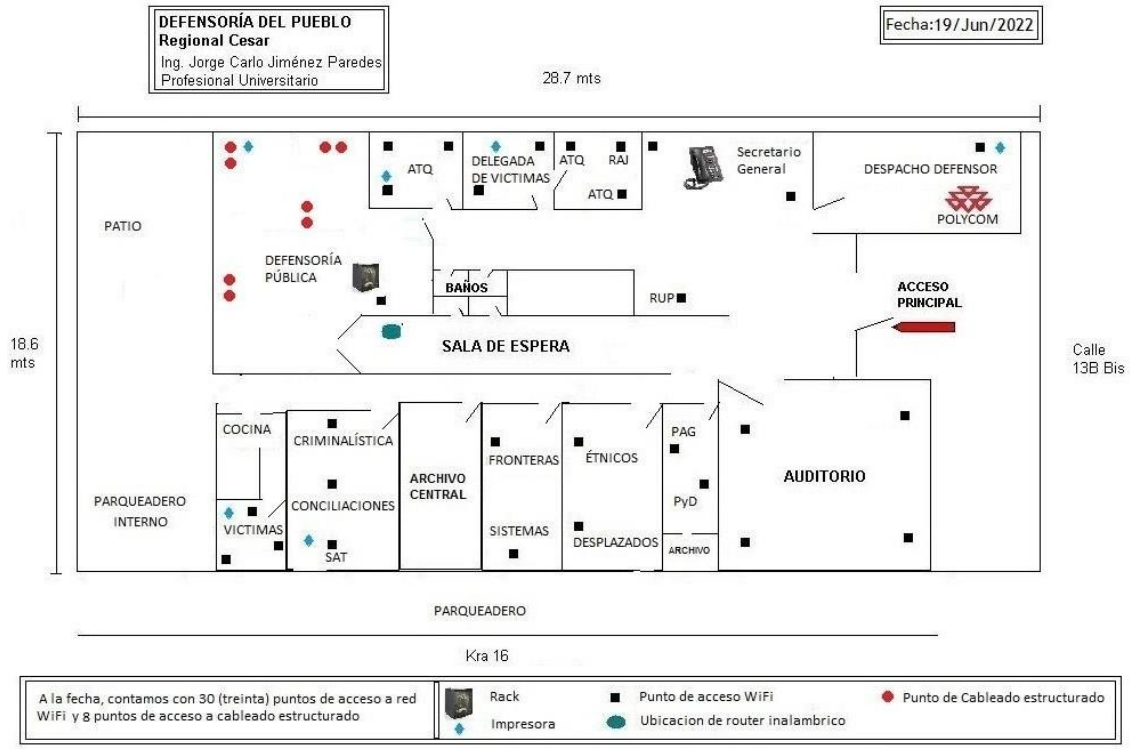


Nota. Captura pantalla Webinar 05-Oct-2018.

Mediante la Figura 2 se evidencia el plano de la red de datos actual de la sede del Cesar de la Defensoría del Pueblo, donde se evidencia que dicha sede cuenta con un solo piso y treinta y un equipos conectados a través del access point.

Figura 2

Plano de la Red de Datos de la Defensoría del Pueblo – Regional Cesar



Nota. Plano de la red de datos.

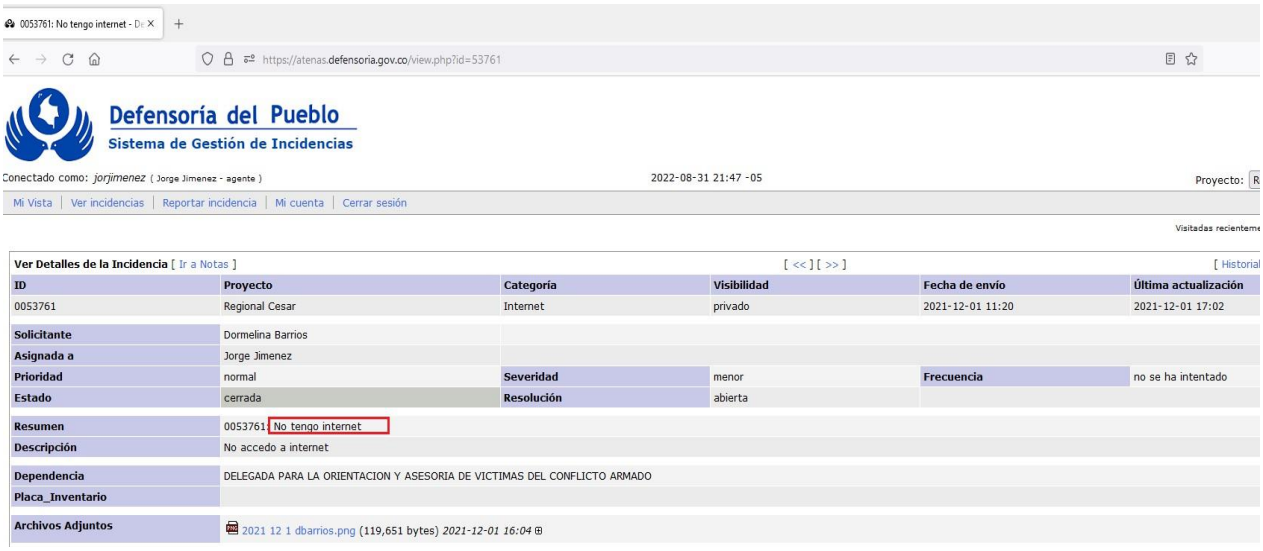
En la actualidad, la red de datos de la Defensoría del Pueblo – Regional Cesar cuenta con un gabinete de 45U al cual llega la última milla en fibra óptica con un canal dedicado de 15Mbits de acho de banda proveído por Claro, sin embargo, dicha señal se conecta a un switch 3COM para luego enlazarse a un access point marca Dlink, referencia DWL-3200AP, que la convierte en inalámbrica para brindar el servicio a treinta (30) equipos de escritorio y un portátil, lo cual casi siempre ocasiona que colapse el acceso a Internet. Los únicos dispositivos que cuentan con acceso con cableado certificado son 5 computadores de la oficina de Pública y por medio de cableado (no certificado) se encuentran el teléfono para voz IP marca Avaya ubicado cerca al

puesto de trabajo del secretario y el equipo de videoconferencias Polycom, instalado en el despacho del Defensor Regional.

A través de la Figura 3 y la Figura 4 se evidencia la falla recurrente del acceso a Internet, donde la funcionaria atiende a peticionarios víctimas del conflicto armado quienes en muchas ocasiones viajan desde municipios, corregimientos y veredas, para que se les realice la toma de la declaración de sus hechos victimizantes a través de la plataforma en línea RUV – Registro Único de Víctimas, y al no contar con un servicio eficiente debe realizarse de forma manual o agendar una nueva cita con el peticionario. Según el análisis realizado a las estadísticas registradas en el Sistema de Gestión de Incidentes TIC del mes de marzo de 2021, las horas pico de tráfico desde y hacia Internet comprende el horario entre las 10:30 a.m. y las 11:45 a.m., en la jornada de lunes a viernes.

Figura 3

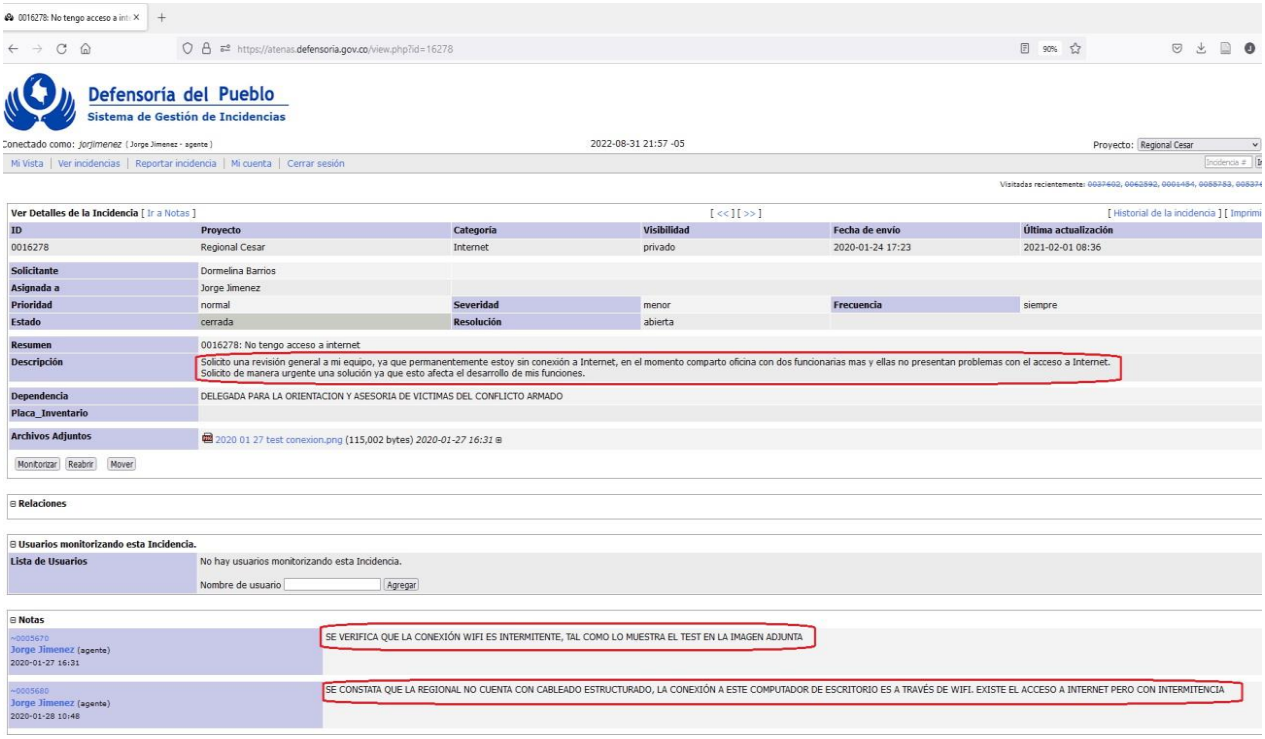
Reporte Falla de Acceso a Internet



Nota. Captura pantalla Sistema de Gestión de Incidencias, 1-Dic-2021.

Figura 4

Reporte Falla de Acceso a Internet

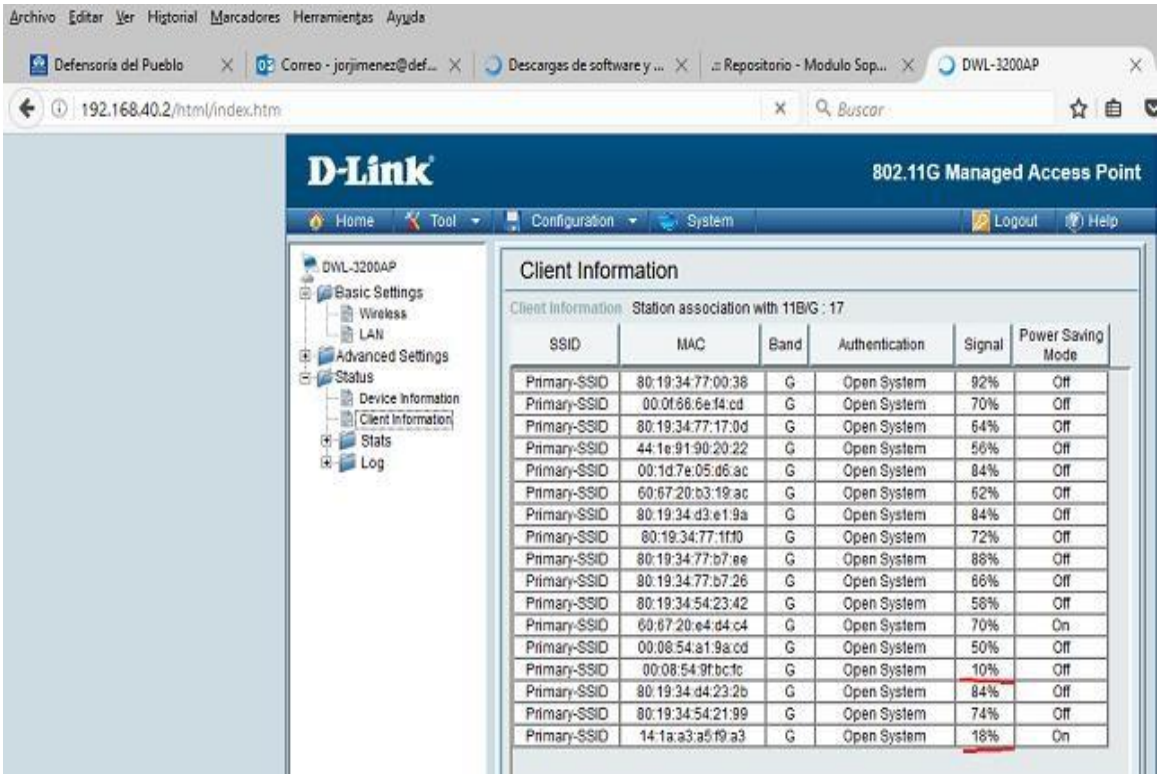


Nota. Captura pantalla Sistema de Gestión de Incidencias, 24-Ene-2020.

En la Figura 5 se observan varios computadores conectados a Internet a través del punto de acceso, el cual le brinda menos del 20% de la potencia de la señal a dos de ellos, y tan solo 4 de las 17 máquinas conectadas en ese momento mantienen una potencia de señal de 84% o más, indicando que la señal de la conexión es atenuada por los muros del edificio y la baja capacidad del punto de acceso, pero a su vez, genera un cuello de botella que no permite el acceso a los servicios web, por lo tanto, no cargan las páginas de manera adecuada y no permite al funcionario ser productivo en su labor.

Figura 5

Clientes Conectados al Access Point

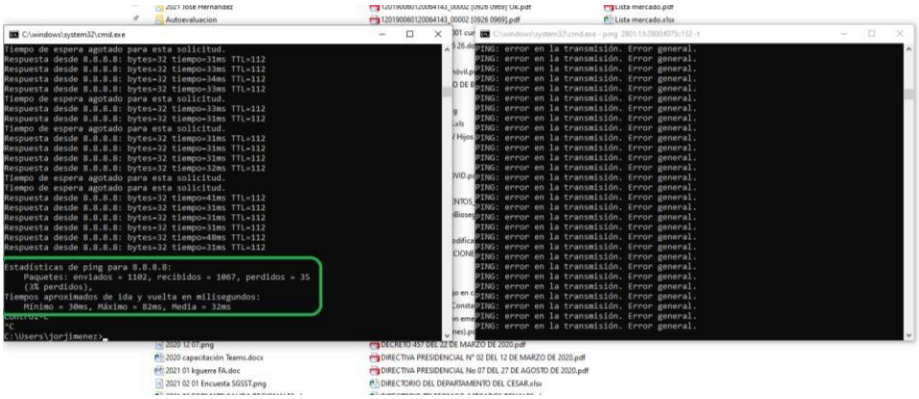


Nota. Captura pantalla “clientes” conectados al access point, 04-Ago-2021.

Como se observa en la Figura 6 se aprecia un retardo de hasta 32 milisegundos en el tiempo de vida (TTL) que requiere un paquete para realizar la comunicación con el servidor de Google, o sin respuesta, es decir, se agota el tiempo de respuesta y, por lo tanto, en ese instante no hay comunicación. En la prueba realizada se muestran las fluctuaciones en la señal, las pérdidas y retardos en el acceso a Internet, lo cual es una constante diaria.

Figura 6

Prueba de Conexión con el Servidor Google

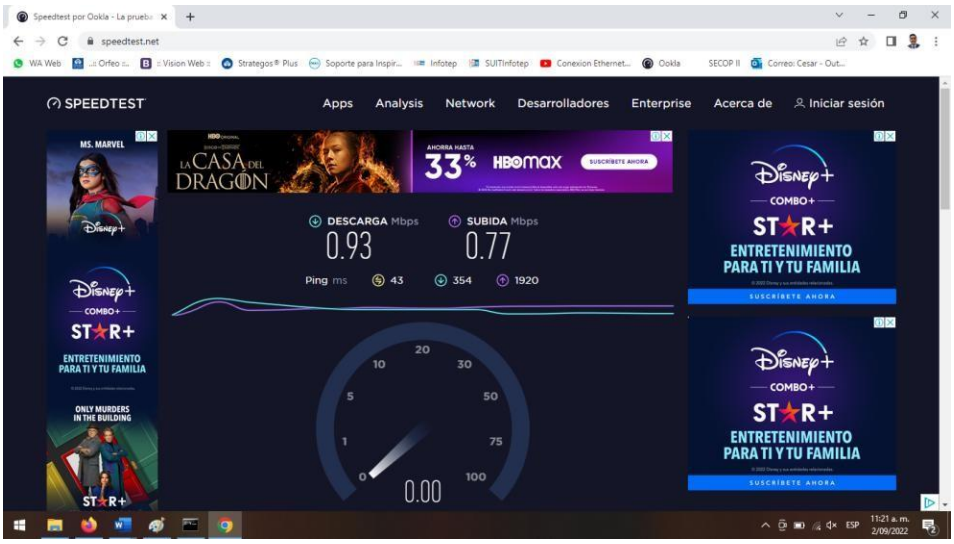


Nota. Test ping, 19-May-2022.

Para evidenciar lo anterior, se realiza una prueba de velocidad que arroja una respuesta de "ping" de 129 milisegundos y una velocidad de descarga de 0,0 o incluso nula. En la Figura 7 se demuestra las deficiencias de la conexión a Internet a través de la red inalámbrica.

Figura 7

Prueba de Velocidad Computador Conectado por Red Inalámbrica

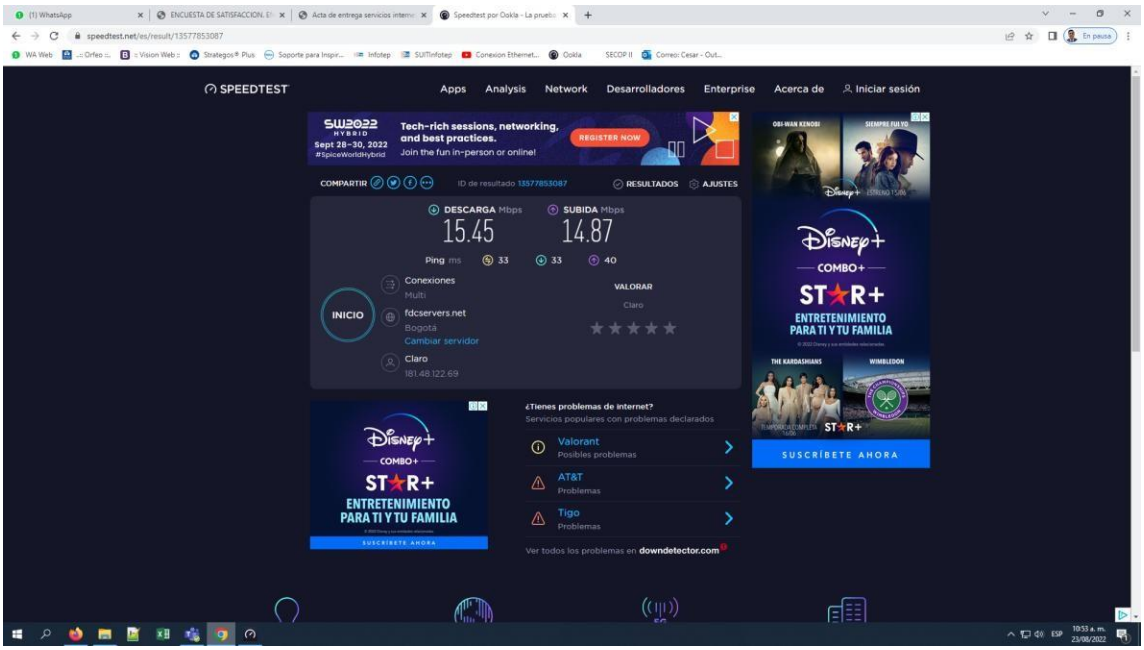


Nota. Test de velocidad inalámbrico speedtest.net, 2-Sep-2022.

directamente al router y al puerto LAN del computador de prueba, es estable y acorde al ancho de banda ofertado por la ISP.

Figura 8

Prueba de Velocidad Computador Conectado por Cable



Nota. Test de velocidad alámbrico speedtest.net, 23-Ago-2022.

Adicionalmente, se debe pensar en la posibilidad de que se agoten las direcciones IPv4 y la entidad pueda quedarse sin acceso a Internet.

Según el Registro de Direcciones de Internet para América Latina y el Caribe – en adelante LACNIC (por su sigla en inglés), responsable de la asignación de recursos para esta región, anunció el agotamiento del stock de direcciones IPv4 y expresó su preocupación por la demora de operadores y gobiernos en desplegar el protocolo de Internet IPv6 en la región.

stock, comienzan a regir políticas restrictivas para la entrega de recursos de Internet en el continente, que en la práctica significa el agotamiento de las direcciones de IPv4 para los operadores de redes en América Latina y el Caribe. (Portal IPv6 - LACNIC, s.f, p. 6)

A partir del contexto presentado, se plantea la siguiente pregunta de investigación:

¿De qué manera la transición al protocolo IPv6 en la red de datos de la Defensoría del Pueblo Regional Cesar, en cumplimiento de los lineamientos establecidos por la guía del MinTIC, contribuyen al fortalecimiento tecnológico de la entidad, facilitando su adopción frente a las crecientes necesidades de direccionamiento y conectividad?

Alcances y limitaciones

A través de este proyecto se busca elaborar un "plan de transición" del protocolo IPv4 a IPv6 en la red de datos de la Defensoría del Pueblo – Regional Cesar, teniendo en cuenta las instrucciones brindadas por MinTIC en la "Guía de transición de IPv4 a IPv6 para Colombia" y sus directrices específicas al momento de hacer la planeación de la transición en la entidad; según dicha guía, se deben realizar las actividades sugeridas para generar el plan de diagnóstico que incluye el inventario de activos de información, y el informe de la infraestructura de red de comunicaciones y las recomendaciones acerca de los dispositivos que no soportan el nuevo protocolo, además, de un documento que contenga el plan para el proceso de transición.

También servirá como una propuesta piloto que pueda adaptarse a cualquier sede de la institución a nivel nacional. Es importante recordar que la Defensoría del Pueblo cuenta en la actualidad con cuarenta y dos (42) regionales en todo el territorio Colombiano, e igualmente aclarar que el objeto de este documento se limita al desarrollo de la fase de planeación de la migración a IPv6, por ende al finalizar no se habrá descrito ningún proceso que tenga que ver

con el diseño de la red necesaria para la migración o con la implementación del nuevo protocolo, dado que la organización no ha destinado los recursos económicos requeridos para implementar la solución. Todo lo anterior, teniendo en cuenta la información y necesidades presentes en la red de datos de la Defensoría del Pueblo – Regional Cesar, entidad en donde se desarrolla la primera y segunda fase del plan de transición a IPv6.

Bajo este contexto, este será el primer paso para dar cumplimiento al artículo 1 de la Resolución 1126 de 2021 de MinTIC, la cual otorga como plazo máximo de transición al protocolo IPv6 a las entidades de orden nacional hasta el día 30-jun-2.022, es decir, que en dicha fecha deben coexistir el protocolo IPv4 con el IPv6.

Marco Teórico

En este capítulo se describe el marco de referencia teniendo en cuenta las consideraciones teóricas, así como la recopilación de antecedentes e investigaciones previas en las que se sustenta este proyecto.

Tcp/Ip

"Las siglas TCP/IP se refieren a un conjunto de protocolos para comunicaciones de datos. Este conjunto toma su nombre de dos de sus protocolos más importantes, el protocolo TCP (Transmission Control Protocol) y el protocolo IP (Internet Protocol)" (Duque, 2014).

Dirección IP

Las direcciones IP, como se mencionó anteriormente, permiten comunicar diversos dispositivos entre sí, además de que hacen posible su ubicación en una red. Mediante el direccionamiento varias computadoras pueden establecer comunicación entre sí, encontrándose en la red. (UnADM, 2024).

Toda computadora conectada a Internet (o a cualquier red) posee una identificación única, llamada dirección IP (en inglés, Internet Protocol), compuesta por cuatro combinaciones de números (p.ej. 187.25.14.190).

Estos números, llamados octetos, pueden formar más de cuatro billones de direcciones diferentes. Cada uno de los cuatro octetos tiene una finalidad específica. Los dos primeros grupos se refieren generalmente al país y tipo de red (clases). Este número es un identificador único en el mundo: en conjunto con la hora y la fecha, puede ser utilizado, por ejemplo, por las autoridades, para saber el lugar de origen de una conexión. (¿Qué es la dirección IP?, 2018)

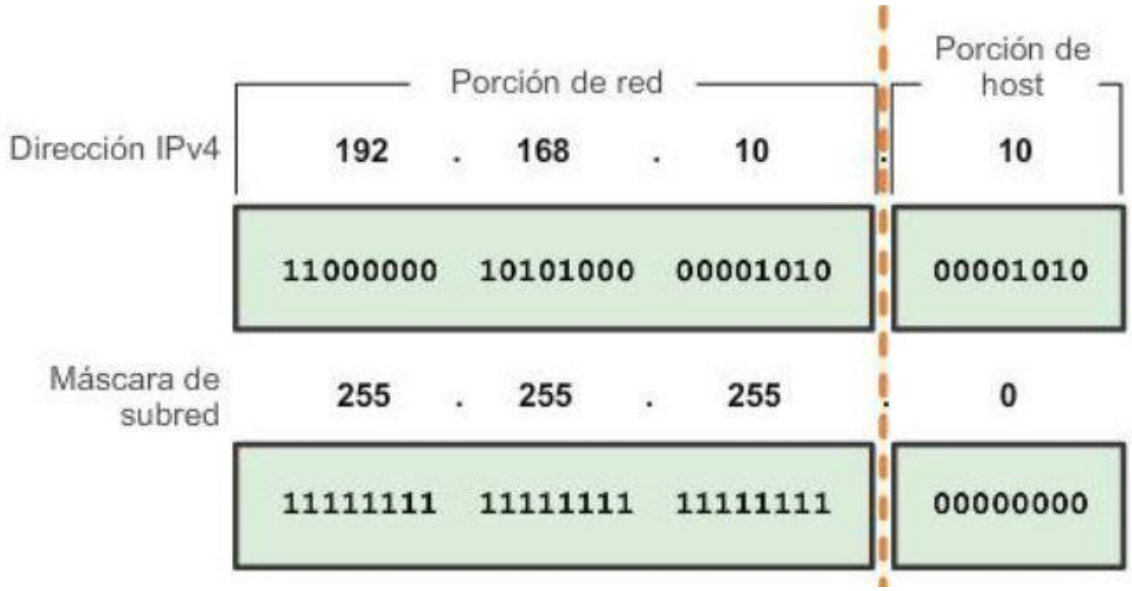
IPv4 (Protocolo de Internet Versión 4)

Con el aumento extensivo de internet y los diversos dispositivos interconectados, se ve la necesidad de mejorar el protocolo IP, desarrollándose la versión cuatro de este protocolo (IPv4), el cual utiliza una dirección única de 32 bits para identificar una máquina y la red a la cual está conectada. (Parker, 1995)

Tal como se describe en la Figura 9 nos muestra un ejemplo de una dirección IP del protocolo versión 4.

Figura 9

Detalle de una Dirección IPv4, Expresada en Notación Decimal



Nota. Tomado de http://www.ingenieriasystems.com, (2017)

IPv6 (Protocolo de Internet Versión 6)

IPv6 (Internet Protocol Version 6) o IPng (Next Generation Internet Protocol) es la nueva versión del protocolo IP (Internet Protocol). Ha sido diseñado por el IETF (Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual, el IPv4.

son utilizadas o se usan con poca frecuencia, se quitaron o se hicieron opcionales, agregándose nuevas características. (RAMÍREZ, Sergio, y CERVANTES, María, (2005), "Introducción a IPV6")

¿Por qué surge?

El motivo básico para crear un nuevo protocolo fue la falta de direcciones. IPv4 tiene un espacio de direcciones de 32 bits, en cambio IPv6 ofrece un espacio de 128 bits. El reducido espacio de direcciones de IPv4, junto al hecho de falta de coordinación para su asignación durante la década de los 80, sin ningún tipo de optimización, dejando incluso espacios de direcciones discontinuos, generan en la actualidad, dificultades no previstas en aquel momento.

Otros de los problemas de IPv4 es la gran dimensión de las tablas de ruteo en el backbone de Internet, que lo hace ineficaz y perjudica los tiempos de respuesta.

Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, aspectos que no fueron contemplados en el análisis inicial de IPv4, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades. Entre las más conocidas se pueden mencionar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec) y movilidad. (RAMÍREZ, Sergio, y CERVANTES, María, (2005), "Introducción a IPV6")

Características principales

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direccionamiento y más nodos direccionables.

- Simplificación del formato del Header (encabezado). Algunos campos del header IPv4 se quitan o se hacen opcionales
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del router.
- Posibilidad de paquetes con carga útil (datos) de más de 65.355 bytes.
- Seguridad en el núcleo del protocolo (IPsec). El soporte de IPsec es un requerimiento del protocolo IPv6.
- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) de tráfico particular, que requieren manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real. Por ejemplo, video conferencia.
- Autoconfiguración: la autoconfiguración de direcciones es más simple. Especialmente en direcciones Aggregatable Global Unicast, los 64 bits superiores son seteados por un mensaje desde el router (Router Advertisement) y los 64 bits más bajos son seteados con la dirección MAC (en formato EUI-64). En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red. Además, el largo del prefijo no depende en el número de los hosts por lo tanto la asignación es más simple.
- Renumeración y "multihoming": facilitando el cambio de proveedor de servicios.
- Características de movilidad, la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.
- Ruteo más eficiente en el backbone de la red, debido a la jerarquía de direccionamiento basada en agregación.

- Calidad de servicio (QoS) y clase de servicio (CoS).
- Capacidades de autenticación y privacidad (RAMÍREZ, Sergio, y CERVANTES, María, (2005), “Introducción a IPV6”)

Doble pila (Dual Stack)

Arafat (como se citó en Albkerat, 2014) piensa que la técnica de pila dual utiliza IPv4 e IPv6 dentro de la misma pila en paralelo. La elección del protocolo es decidida por las políticas del administrador, junto con qué tipo de servicio se requiere y qué tipo de red se utiliza. Esta tecnología no realiza ningún cambio en el encabezado del paquete y al mismo tiempo no realiza encapsulación entre IPv4 e IPv6. Esta tecnología es conocida como pila dual nativa o doble capa IP.

El Ministerio de Tecnologías de la Información y las Comunicaciones, según la Ley 1341 o Ley de TIC, es la entidad que se encarga de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector de las Tecnologías de la Información y las Comunicaciones.

Lidera la reglamentación para la adopción de IPv6 en Colombia.

Sobre IPv6 el MinTIC expidió los lineamientos de Gobierno en Línea (GEL), Circular No.002-2011 y las guías de planeación y seguridad IPv6. Así como la Resolución 1126 de 2021 que establece un nuevo plazo para el proceso de transición en Colombia.

La meta de MinTIC es que todas las entidades de Gobierno, las empresas privadas, la academia y en general todos los colombianos, se conecten a Internet usando IPv6. (MinTIC, 2011)

En cuanto al estado del arte; luego de la respectiva indagación, se obtienen varias monografías como referencia:

realizadas por el Min TIC Colombia", Diana Catalina Fonseca Castro.

El plan de transición a IPv6 diseñado de acuerdo con los lineamientos dados por MinTIC ayudó no sólo en el levantamiento de la información necesaria para conocer y entender el funcionamiento actual de la red de datos de la entidad, sino que sirvió para encontrar las falencias a nivel de red que pueden retrasar el proceso de migración, y sugerir estrategias para superarlas. De esta manera se obtuvo una mirada holística de la red de comunicaciones de la entidad, que efectivamente permitió obtener el diagnóstico e indicar qué tan lista se encuentra la entidad para empezar con la etapa de implementación de IPv6.

El despliegue del inventario de activos de información resultó un primer paso valioso en la determinación del porcentaje de compatibilidad y el grado de avance de la red en la implementación de IPv6, por ello se puede decir que es una de las actividades más importantes de la fase de planeación, pues con ésta se determinó en primera instancia que la entidad está apta para comenzar con el proceso de migración, ya que se encontró que gran parte de equipos funcionando en la red son compatibles con el protocolo versión 6, además que los que no lo están no retrasan el proceso gracias a los mecanismos de implementación y coexistencia sugeridos. (Fonseca, 2017, p. 54)

Con el desarrollo del proyecto se conoce de manera clara la red de datos y así mismo se detectan las falencias que deben ser superadas. También se obtiene un diagnóstico que permite conocer qué tan preparada se encuentra la entidad para la transición. Además, se genera el inventario de activos de información, insumo valioso para el perfeccionamiento del proyecto.

"IPv6: estudio sobre las barreras para su implementación", Gustavo Eduardo Mendoza Ramírez, Sergio Andrés Quintana Burgos.

En la actualidad, hablar de IPv6 no es un mito, es más que una realidad, una definición tangible, en la cual al pasar los días las empresas se verán obligadas a ir migrando sus aplicaciones y entorno hacia este nuevo tema. De acuerdo con la escasez de direcciones IPv4, la necesidad de migración es algo necesario, y en base a esto, nuestro estudio analizó y observó cuáles han sido aquellas barreras en las que se ha visto inmersa la transición a este nuevo protocolo. (Mendoza y Quintana, 2011)

"*Propuesta para la migración del protocolo IPv4 a protocolo IPv6 para la secretaria del Sisbén de la Alcaldía de Tunja*", Juan Pablo Montañez Prieto.

La metodología utilizada por el autor fue un estudio descriptivo: "con el fin de caracterizar los elementos necesarios para el cambio progresivo de la red de comunicaciones y su migración de IPv4 a IPv6." (Montañez, 2018, p. 50)

Su objetivo principal fue desarrollar una propuesta para la migración del protocolo de Internet IPv4 al protocolo IPv6 y mejorar la seguridad y la administración de la red en la Secretaría del Sisbén de la Alcaldía de Tunja.

Adicionalmente, emplea como herramienta de apoyo para la simulación de los distintos escenarios de la organización el programa denominado Cisco Packet Tracer que es un software propiedad de Cisco System, Inc. ®, diseñado para la simulación de redes basadas en los equipos de la citada compañía. Junto con los materiales didácticos diseñados con tal fin, es la principal herramienta de trabajo para pruebas y simulación de prácticas en los cursos de formación de Cisco System.

La investigación de Montañez se sustentó en los trabajos de Pulgarín (2011), Ramírez, Guzmán y Beltrán (2015), Sabogal y Grossy (2017) en cuanto al uso de doble pila como metodología para la coexistencia de ambos protocolos.

Así mismo, se tuvieron en cuenta los siguientes artículos:

"*Diseño e implementación de una red IPv6 para transición eficiente desde IPv4*", de los autores Bolívar, Guerrero y Polanco, publicado en la revista Ingeniería y Competitividad, Volumen 14, No. 2, p. 179 - 189 (2012), en el cual buscan "el establecimiento de una conexión IPv6 entre las oficinas remotas y la red de la oficina central mediante 6PE, para obtener una Intranet IPv6 nativa; proveer el servicio de Internet IPv6 a la Intranet mediante 6to4 conservar el acceso al servicio Internet IPv4 para la Intranet mediante el uso de NAT64 y DNS64". Concluyendo con su investigación lo siguiente:

La transición hacia IPv6 es un paso que las entidades se ven obligadas a realizar en el corto plazo debido al rápido agotamiento de las direcciones IPv4, esto se debe llevar a cabo de una manera planeada y sistemática, minimizando el impacto en la operación de la red.

"*Propuesta de conexión de entornos IPv6 mediante un Backbone MPLS/IPv4*", Gelvez, López, Rivas (2013), publicado por la Universidad Distrital Francisco José de Caldas y cuyo objetivo es determinar las ventajas y desventajas de las diferentes técnicas de entunelamiento, a partir de la interconexión de una red de prueba mediante las 4 variantes de túneling IPv6 en los CE mediante el emulador GNS3+Dynamips.

Concluyen que:

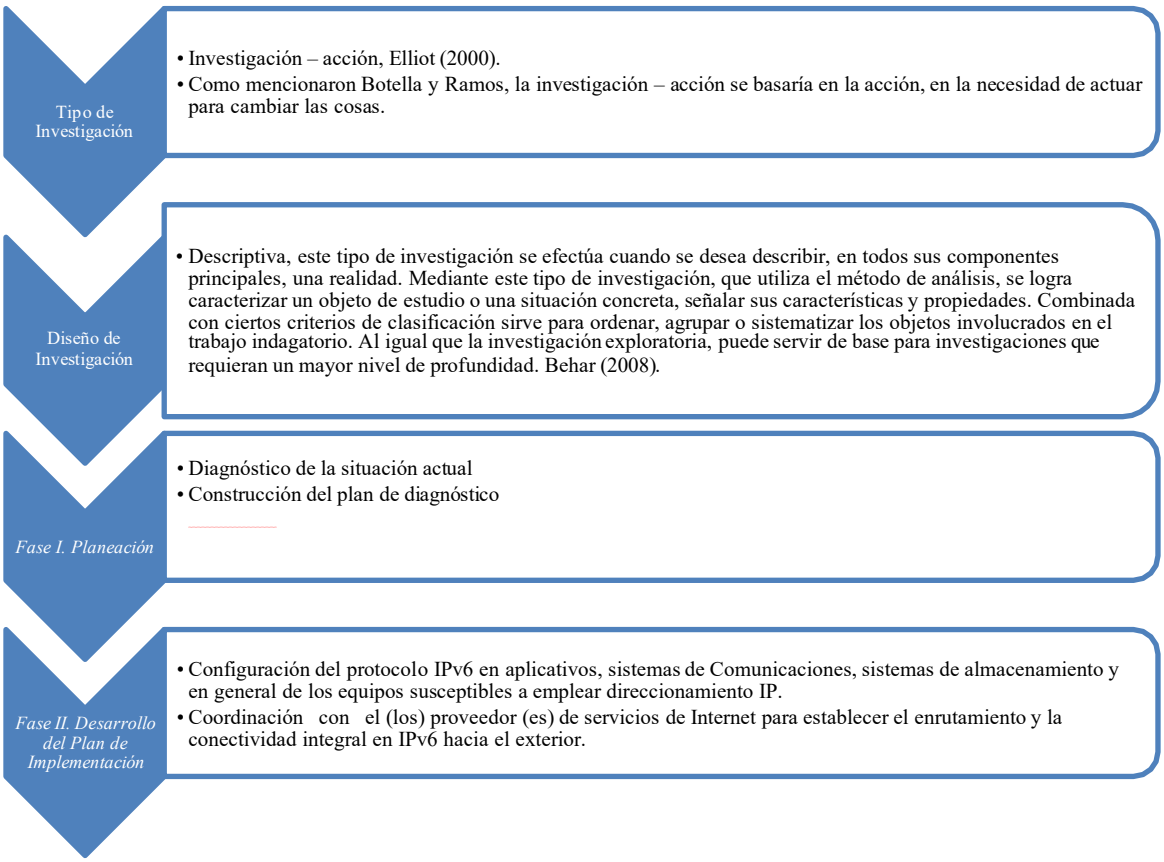
La utilización de túneles dinámicos (6to4 e IPv6 compatible IPv4) para la interconexión de islas IPv6 a través de redes IPv4 resulta comparativamente mejor en cuanto a configuración a medida que aumenta el número de islas a interconectar frente a las técnicas de túneles manuales (manual y GRE).

Metodología

La estrategia metodológica utilizada en este proyecto y su estructura se encuentra representada a través de la Figura 10, teniendo en cuenta el tipo de investigación – acción basado en el reconocimiento de necesidades para el mejoramiento de una situación particular, así como la investigación descriptiva para comprender todos los factores y aspectos para tener en cuenta para su desarrollo que dan lugar a las dos fases planteadas.

Figura 10

Esquema de la Metodología Utilizada

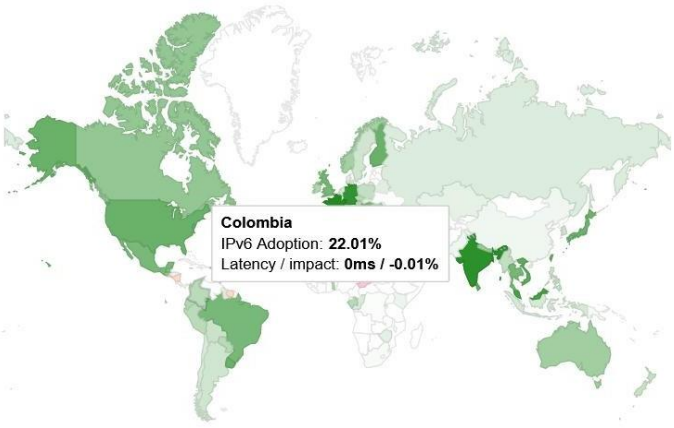


Nota. Esquema del proyecto aplicado, 6-May-2025.

se encuentran rezagados en cuanto al cambio de versión 4 a versión 6 del protocolo de acceso a internet, con un 22.01% de avance y tan solo por encima de Perú, Bolivia, Argentina, Chile y Venezuela.

Figura 11

Monitor Adopción de IPv6 de Google



País	Porcentaje
Uruguay	48,24
Brasil	43,74
Ecuador	24,49
Paraguay	22,43
Colombia	22,01
Perú	21,81
Bolivia	17,01
Argentina	15,11
Chile	12,7
Venezuela	0,61

Nota. Tomado de https://www.google.com/intl/es/ipv6/statistics.html#tab=per-ountry-pv6-adoption, adaptado por el autor.

Este documento se fundamenta en los lineamientos técnicos que se requieren tener en cuenta para seguir el proceso de transición de IPv4 a IPv6, en las distintas organizaciones del Estado, es decir, a través del desarrollo de tres fases, cabe aclarar que el presente proyecto

culminará cuando se complete la segunda fase debido a que en la tercera fase o implementación se requieren recursos económicos que en el momento está gestionando la organización ante el ministerio de hacienda y el BID (Banco Interamericano de Desarrollo) para el fortalecimiento institucional con el apoyo de las TICs, pero aún no son apropiados en el presupuesto. Lo anterior, acorde al documento CONPES 3925 del 18 de mayo de 2018, a través del cual se da:

"Concepto favorable a la nación para contratar un empréstito externo con la banca multilateral hasta por USD $ 18 millones, o su equivalente en otras monedas, destinado a financiar el programa de fortalecimiento de la capacidad institucional de la Defensoría del Pueblo de Colombia".

A continuación, se describen las tres fases que MinTIC sugiere desarrollar en la guía para la transición (acorde a lo dispuesto en la Resolución 1126 de 2021) incluye la planeación, desarrollo e implementación del protocolo IPv6 en las entidades. Teniendo presente que en cada una de ellas existen unas actividades generales y al finalizar cada fase se producen unos entregables, los cuales son insumos para la siguiente etapa.

En ese sentido la Tabla 1 corresponde a la Fase I, la planeación.

Tabla 1

Fase I. Planeación de IPv6

Fase I	Actividades Generales	Tiempo en meses de la actividad
Diagnóstico de la Situación Actual	Construcción del plan de Diagnóstico	1
	Inventario de TI (Hardware, Software)	1
	Análisis de la nueva topología de la infraestructura actual y su funcionamiento	2
	Protocolo de pruebas de validación de aplicativos, comunicaciones, plan de seguridad y coexistencia de los protocolos	1
	Planeación de la transición de los servicios tecnológicos de la Entidad. Plan de direccionamiento de IPv6 y plan de contingencia de IPv6	2
	Validación del estado actual de los sistemas de información, los sistemas de comunicaciones, las interfaces y revisión de los RFC correspondientes.	2
	Identificación de esquemas de seguridad de la información y las comunicaciones	1

Nota. "Guía de Transición de IPv4 a IPv6 para Colombia.", de MinTIC, 7 de Sep, 2022.

Por otra parte, la Tabla 2 presenta del desarrollo del plan de implementación.

Tabla 2

Fase II. Desarrollo del Plan de Implementación del protocolo IPv6

Fase II	Actividades Generales	Tiempo en meses de la actividad
Desarrollo del Plan de implementación	Habilitación direccionamiento IPv6 para cada uno de los componentes de hardware y software de acuerdo con el plan de diagnóstico de la Primera Fase.	2
	Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros.	2
	Configuración del protocolo IPv6 en aplicativos, sistemas de Comunicaciones, sistemas de almacenamiento y en general de los equipos susceptibles a emplear direccionamiento IP.	2
	Activación de políticas de seguridad de IPv6 en los equipos de seguridad y comunicaciones que posea cada entidad de acuerdo con los RFC de seguridad en IPv6.	1
	Coordinación con el (los) proveedor (es) de servicios de Internet para establecer el enrutamiento y la conectividad integral en IPv6 hacia el exterior.	2

Nota. "Guía de Transición de IPv4 a IPv6 para Colombia.", de MinTIC, 7 de Sep, 2022.

hardware, software y servicios.

Tabla 3

Fase III. Pruebas de funcionalidad de IPv6

Fase III	Actividades Generales	Tiempo en meses de la actividad
Pruebas de funcionalidad de IPv6	Pruebas de funcionalidad y monitoreo de IPv6 en los servicios de la Entidad.	0
	Análisis de información y pruebas de funcionalidad frente a las políticas de seguridad perimetral de la infraestructura de TI.	0
	Afinamiento de las configuraciones de hardware, software y servicios de la Entidad.	0

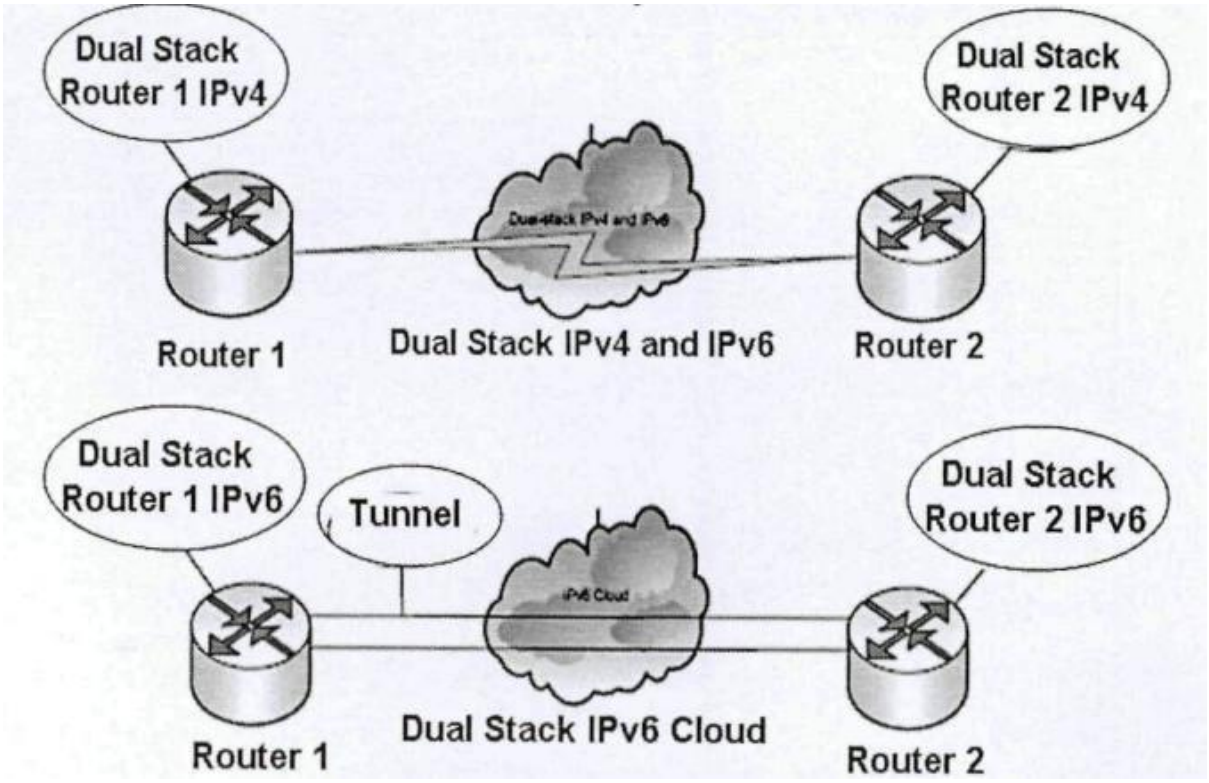
Nota. "Guía de Transición de IPv4 a IPv6 para Colombia.", de MinTIC, 7 de Sep, 2022.

Sin embargo, se tendrá en cuenta la metodología Dual stack o pila doble para tener una transición suave hacia IPv6. (Portal IPv6 - LACNIC, s.f). Es decir, la pila doble se utiliza para "rescatar" la IPv4 y de esta manera conectarla con el IPv6. (What is IPv4/IPv6 Dual Stack?, s.f)

A través de la Figura 12, se plasma la comunicación entre dos routers, los cuales utilizan el mecanismo de pila doble para el intercambio de datos.

Figura 12

Implementación Doble Pila para IPv6



Nota. (MOHD, 2013)

Así mismo, “La mayor desventaja de esta aproximación ideal, es que requiere que todo el equipamiento soporte ambos protocolos, lo cual no es la situación real.” (Bienvenidos al Portal IPv6 Cuba, s.f)

Contexto Organizacional

Para el desarrollo del proyecto es necesario conocer de forma general la entidad y su quehacer, entendiendo que este contexto nos ayuda a comprender mejor el por qué de la investigación y la búsqueda de la solución a la problemática de conectividad.

Reconocimiento de la Organización

Descripción

La labor de vigilancia al poder público, a partir de la expedición de la Constitución Política de 1991, se amplió gracias a la creación de la figura del Defensor del Pueblo, especialmente, en cuanto a protección, defensa, promoción, divulgación y ejercicio de los derechos humanos. Mediante los artículos 281 y 282 de la Constitución, se estructuraron las características, facultades y funcionamiento de la Defensoría del Pueblo, como proyección y desarrollo de la concepción del Estado Social de Derecho.

De esta manera se constituye en autoridad estatal, cuya misión consiste en el control de la actividad de la institucionalidad pública y de algunos particulares a quienes se les ha delegado funciones de carácter público, respecto de los derechos fundamentales y las garantías para ejercerlos, para lo cual se le ha surtido de procedimientos flexibles, informales y expeditos para desempeñar sus acciones y tareas.

La finalidad del ente Defensorial es la protección de los derechos humanos y de las libertades de todas las personas frente a actos, amenazas o acciones ilegales, injustas, irrazonables, negligentes o arbitrarias de cualquier autoridad o de los particulares. La Defensoría del Pueblo se instituye, entonces, como el organismo tutelar de los derechos y garantías de los habitantes del territorio nacional como de los colombianos residentes en el exterior.

Junto con la Procuraduría General de la Nación y las personerías municipales, la Defensoría del Pueblo hace parte de lo que se denomina el Ministerio Público.

Estructura Organizacional

La entidad está conformada por cuatro Direcciones Nacionales y doce delegadas; adicionalmente, cuenta con cuarenta y dos Defensorías Regionales distribuidas a lo largo y ancho del territorio colombiano.

Infraestructura

Defensoría del Pueblo - Regional

Cesar. Tipo A con sede propia.

Un piso, con 533 metros cuadrados.

No se cuenta con cableado estructurado.

Treinta y dos (32) funcionarios de planta y siete contratistas. (Ver Figura 2)

Estado Actual con Respecto a IPv6

A continuación, se realiza un análisis detallado con respecto al inventario de hardware, software e información actual de la entidad, determinando con así el porcentaje de compatibilidad en cuanto al protocolo IPv6 y las recomendaciones necesarias para lograr la transición.

Fase I. Planeación de IPv6

La Fase I, abarca las siguientes actividades generales:

- ✓ Construcción del plan de Diagnóstico
- ✓ Inventario de TI (Hardware, Software)
- ✓ Análisis de la nueva topología de la infraestructura actual y su funcionamiento

- ✓ Protocolo de pruebas de validación de aplicativos, comunicaciones, plan de seguridad y coexistencia de los protocolos.
- ✓ Planeación de la transición de los servicios tecnológicos de la Entidad
- ✓ Validación de estado actual de los sistemas de información, los sistemas de comunicaciones, las interfaces y revisión de los RFC correspondientes.
- ✓ Identificación de esquemas de seguridad de la información y las comunicaciones.

Plan de Trabajo para la Adopción de IPv6 en la Regional Cesar

La planeación de la migración al protocolo IPv6 tiene como objetivo fundamental identificar los recursos de hardware y software que dependen del protocolo IPv4, para lo cual se debe verificar con el fabricante de este sus características y posibles incompatibilidades. En dicho escenario de no soporte del nuevo protocolo, se deben realizar las recomendaciones de adquisición de aquellos dispositivos que sean esenciales para garantizar la conexión de la red de datos.

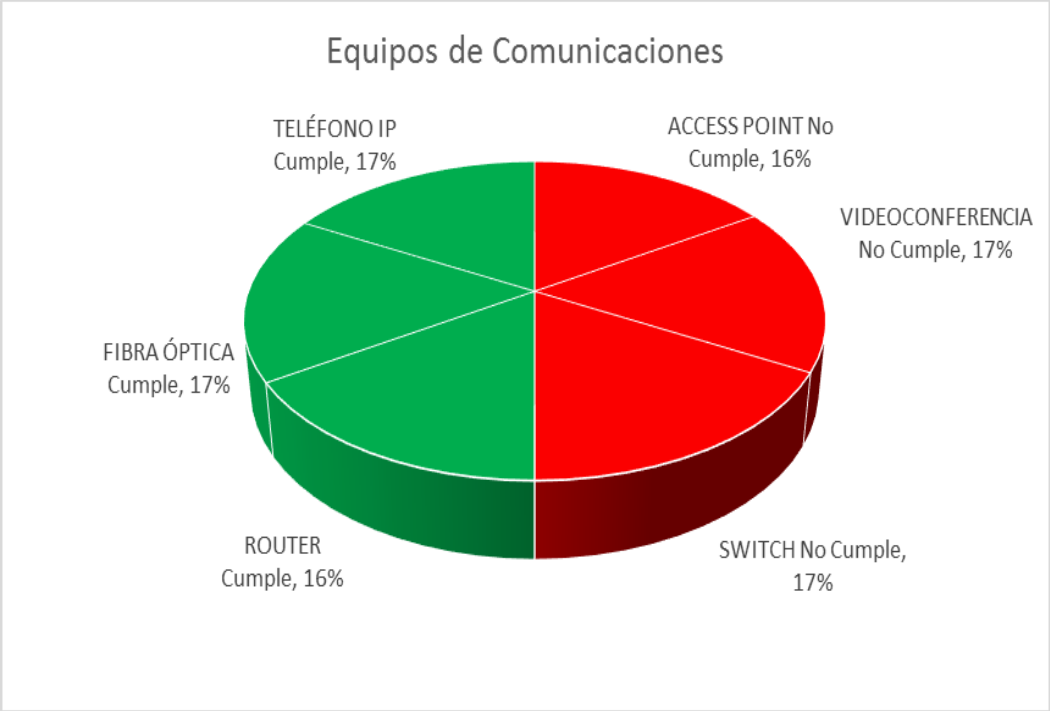
También, se realiza un plano de las instalaciones de la sede de la Defensoría del Pueblo – Regional Cesar, en el cual se pueda identificar los dispositivos de la red actual, tales como el rack principal, el router, los switches, impresoras, equipos de usuarios, entre otros.

Inventario de TI (Hardware y software)

Dentro del análisis del hardware y software que actualmente tiene la Defensoría del Pueblo del César, se encontró que son pocos los dispositivos que se pueden utilizar en una transición a IPv6 y que serán completamente funcionales. A través de la Figura 13 se muestra el porcentaje de compatibilidad de los equipos de comunicación que posee la entidad. (Ver Apéndice A)

Figura 13

Porcentaje de Equipos de Comunicación que Soporta IPv6.



Nota. Porcentaje de compatibilidad con el protocolo IPv6.

De acuerdo con la información recolectada, la entidad; en cuanto a los equipos de comunicaciones, cumple con el 50% de equipos que soportan el protocolo IPv6 y pueden involucrarse en el proceso de migración a IPv6.

Sugerencias para la Transición a IPv6

Se recomienda la adquisición de los equipos necesarios que permitan la transición al nuevo protocolo, es decir, Access point, switch y dispositivo de videoconferencias. Lo anterior, en aras de garantizar el correcto funcionamiento de la doble pila. (Ver Apéndice B)

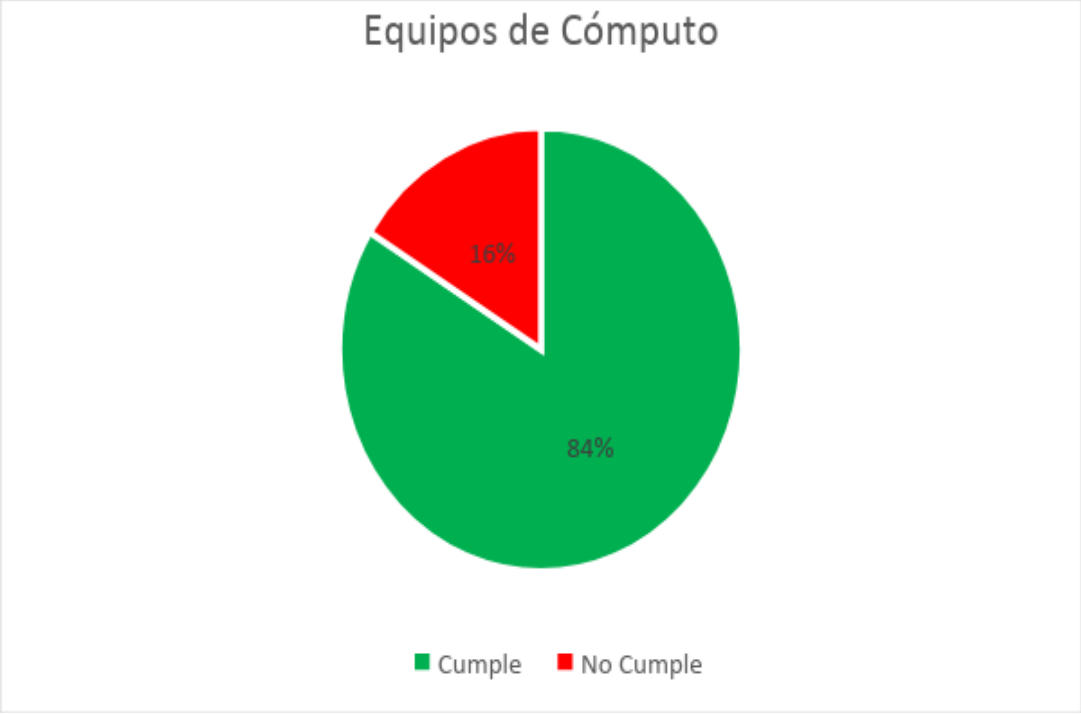
Se describe el inventario de equipos de cómputo de la entidad, (Ver Apéndice C) caracterizándolo por marca, modelo, dependencia, placa de inventario, memoria RAM,

procesador, tamaño del disco duro; de igual manera, sistema operativo, junto el paquete ofimático y el antivirus. Además, el rol dentro de la red y si es compatible con uno o ambos protocolos.

En la actualidad se cuenta con treinta (30) equipos de escritorio y un computador portátil, y como lo demuestra la Figura 14, la entidad y sus equipos de cómputo alcanzan un 84% de compatibilidad con el protocolo IPv6. Es decir, que se cuenta con cinco computadores que utilizan el Sistema Operativo Windows Xp, el cual no permite el uso de la nueva tecnología.

Figura 14

Porcentaje de Equipos de Cómputo que Soporta IPv6



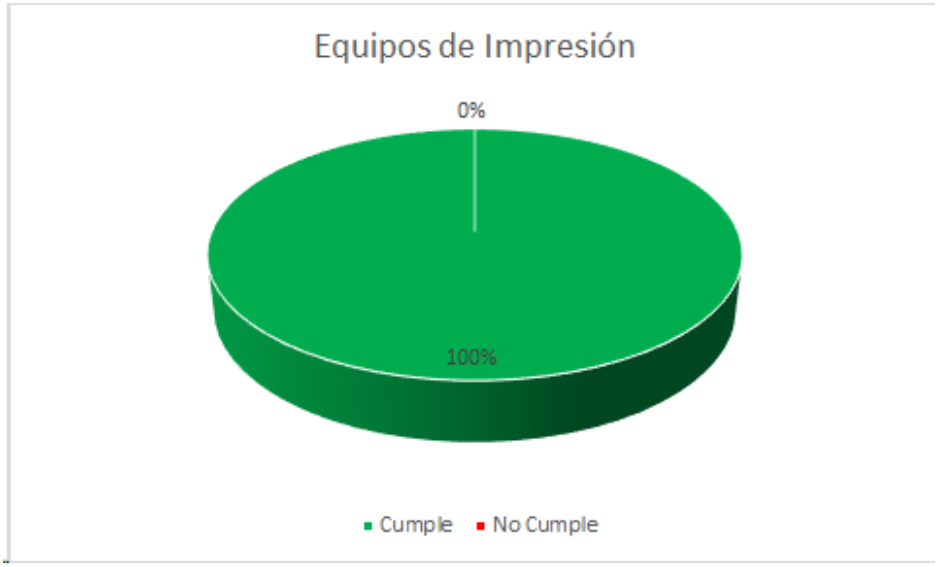
Nota. Compatibilidad de equipos de cómputo.

Se deben reemplazar los cinco computadores por ser tecnológicamente obsoletos, sus características técnicas de memoria RAM, disco duro, fecha de adquisición, entre otros, los hacen improductivos. Dicho reemplazo se puede llevar a cabo de manera gradual, es decir, no es necesario hacerlo en simultáneo, se puede producir durante la migración. Debe incorporarse en el Plan Anual de Adquisiciones y en el presupuesto de la entidad.

Como se ilustra en la Figura 15 se puede evidenciar que todas las impresoras y multifuncionales con que cuenta la entidad en la actualidad soportan el protocolo IPv6, no es necesario realizar una sustitución o cambio. (Ver Apéndice D)

Figura 15

Porcentaje de Equipos de Impresión que Soportan IPv6.



Nota. Revisión de equipos de impresión.

Se puede comprobar; observando la Figura 16, que los aplicativos tanto externos como internos a la entidad soportan el protocolo IPv6. (Ver Apéndice E)

Figura 16

Porcentaje de Aplicaciones que Soportan IPv6.

Nota. Todas las actuales aplicaciones son compatibles.

Hoy por hoy, la Defensoría del Pueblo cuenta con distintos servidores, los cuales son 100% compatibles con el protocolo IPv6. Tal como lo demuestra la Figura 17. (Ver Apéndice F)

Figura 17

Porcentaje de Servidores que Soportan IPv6.

Nota. Todos los servidores actuales soportan el nuevo protocolo.

Sugerimos; para la transición a IPv6, utilizar el mecanismo de Dual Stack o Doble Pila como solución para la convivencia entre los protocolos de comunicación IPv4 e IPv6, los equipos servidores y los equipos de los usuarios que utilizan IPv4.

A través de la Tabla 4, se identifica al proveedor de servicios de Internet de la entidad, el ancho de banda ofertado y el tipo de tecnología utilizado para la conexión.

Tabla 4

ISP

Oficina	Proveedor	Ancho de Banda	Tecnología
Regional Cesar - Valledupar	Claro Bussiness	15 Mbps	Fibra óptica-Dedicado

Nota. La ISP Claro oferta un servicio de canal dedicado.

Según el portal web de LANIC, Claro cuenta con una gran red de fibra óptica en Colombia y América Latina, brindando acceso a nuestros clientes bajo el protocolo IP, además del transporte nacional con un robusto core MPLS en la modalidad de 6VPE. Nuestra infraestructura cuenta con soporte IPv6 en su modalidad “Dual Stack” en nuestros equipos de borde y de última milla, facilitando la operación de IPv4 e IPv6 de forma paralela sin inconvenientes. Actualmente Claro provee acceso IPv6 a grandes clientes en Colombia.

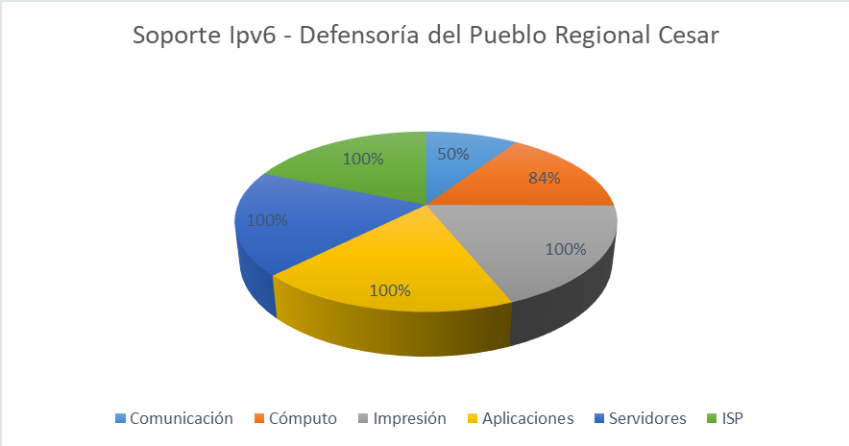
Se debe solicitar el aumento de ancho del canal dedicado a 30Mbps y de manera directa a LANIC el segmento, grupo o pool de direcciones IPv6 para su implementación para de esta manera no depender de la ISP. De acuerdo con lo establecido en el RFC 6177.

Informe de Cumplimiento de IPv6 por cada Elemento de Hardware y Software

A través de la Figura 18 se evidencia el porcentaje de soporte del nuevo protocolo por categoría.

Figura 18

Porcentaje de Soporte IPv6 por Categoría



Nota. Resumen de compatibilidad por categoría.

Por otra parte, la Figura 19 resume el grado de compatibilidad global de la institución.

Figura 19

Porcentaje de Soporte IPv6

Nota. Nivel de preparación de la Defensoría del Pueblo – Regional Cesar.

La Tabla 5 y Tabla 6, listan el porcentaje de compatibilidad con el protocolo IPv6 de manera detallada y general, respectivamente.

Tabla 5

Porcentaje de compatibilidad con IPv6 de Hardware y Software

Equipos	Soporte Ipv6
Comunicación	50%
Cómputo	84%
Impresión	100%
Aplicaciones	100%
Servidores	100%
ISP	100%

Nota. Equipos de la entidad.

Tabla 6

Promedio de compatibilidad con IPv6 de Hardware y Software

	Promedio
Cumple	89%
No cumple	11%

Nota. Equipos de la entidad.

Se determina que en la Defensoría del Pueblo Regional Cesar tanto los equipos de comunicación y de cómputo, así como los dispositivos de aplicaciones y servidores cumplen con el soporte del protocolo de comunicaciones IPv6 en un 89%.

Recomendaciones para Adquisición de Elementos de Comunicaciones, de Cómputo y Almacenamiento con el Cumplimiento de IPv6

Se recomienda adquirir y configurar los equipos del listado del Apéndice B, con el fin de alcanzar el 100% de compatibilidad con el nuevo protocolo y de esta manera evitar traumas en la entidad, sobre todo en el periodo de transición.

Informe con el Plan de Direccionamiento en IPv6

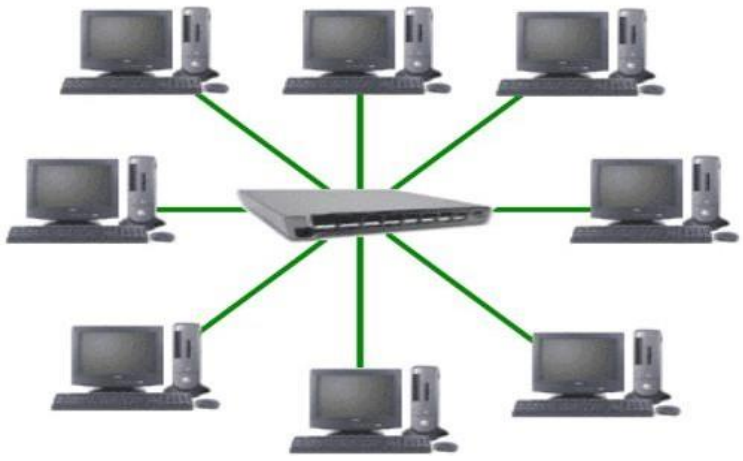
En cuanto a la topología actual de la red de datos se tiene:

Topología en Estrella. Red en la cual las estaciones están conectadas directamente al servidor u ordenador y todas las comunicaciones se han de hacer necesariamente a través de él. Todas las estaciones están conectadas por separado a un centro de comunicaciones, concentrador o nodo central, pero no están conectadas entre sí. (Molina, s/f)

Tal como se aprecia en la Figura 20 es un ejemplo de una red que utiliza la topología en estrella.

Figura 20

Topología de Red en Estrella



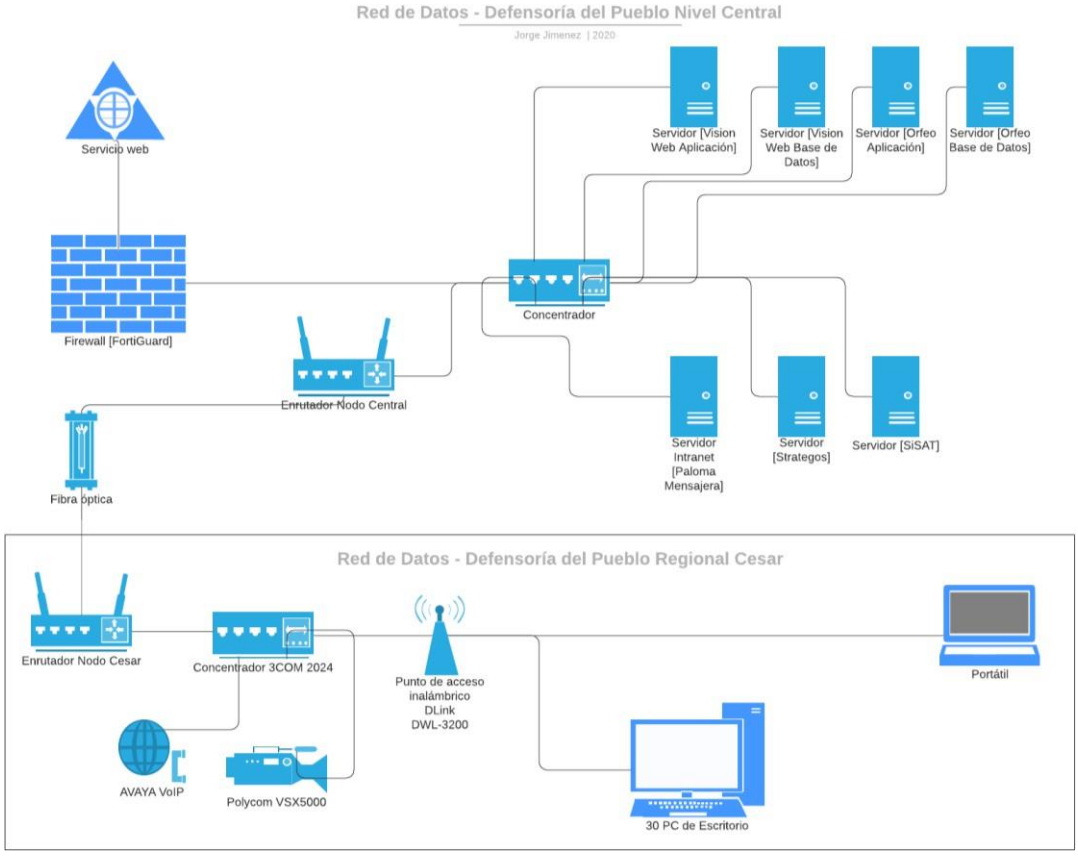
Nota. Muestra de la topología de red en estrella (Molina, s/f).

La topología de red utilizada en la red de datos de la Defensoría del Pueblo – Regional Cesar es en estrella extendida. Es igual a la topología en estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella. (Cisco Networking Academy Program, 2003)

Por medio de la Figura 21 se observa la topología actual de la red de datos de la Defensoría del Pueblo Regional Cesar, la cual es estrella extendida.

Figura 21

Topología de Red en Estrella Extendida, AS IS



Nota. Elaborado mediante el uso de la aplicación: www.lucidchart.com

En la actualidad, el funcionamiento de la red de datos implica la conexión del segmento de red 192.168.40.*XXX* al nodo principal en el Nivel Central, en la ciudad de Bogotá a través de un canal dedicado con la última milla en fibra óptica que nos brinda la ISP y luego se accede a Internet. En el caso; por ejemplo, de un equipo conectado por medio de una tarjeta de red inalámbrica, la ruta a seguir es:

Usuario → Punto de acceso → Switch → Router (nodo Cesar) → Router (nodo Central) →Switch (Nivel Central) → Firewall → Internet.

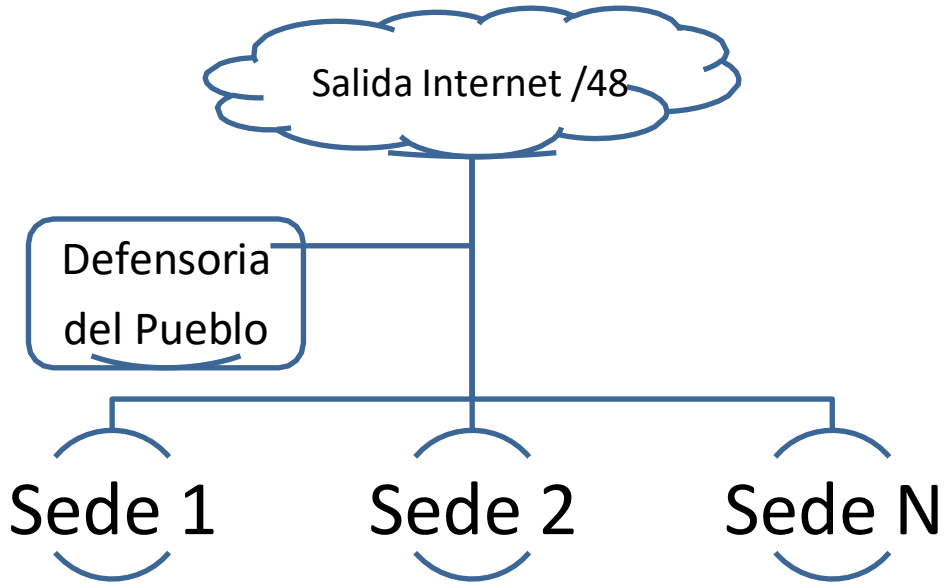
Las direcciones IP de la entidad son fijas o estáticas, pero sin una adecuada segmentación.

Se recomienda segmentar la red y establecer subredes acordes a las áreas misionales y la parte administrativa. Teniendo en cuenta para ello lo indicado en el RFC 4291, es decir, que las subredes cuenten con máscara /64.

El diagrama de red a emplear se evidencia a través de la Figura 22, teniendo presente una cantidad N de sedes que acceden al nodo principal y a su vez al servicio de Internet; el cual, debería ser de tipo /48.

Figura 22

Diagrama de Red, TO BE



Nota. Diagrama de red por sede.

Teniendo en cuenta que luego de la adquisición de la membresía y el pago del costo anual de administración a LANIC (Registro de Direcciones de Internet para América Latina y el Caribe) el segmento asignado sea, por ejemplo:

Prefijo 2801 : ab12 : abcd

La Tabla 7 representa la asignación de segmentos de red teniendo en cuenta el prefijo de ejemplo que asigna LACNIC a Nivel Central y en la sede de la Regional Cesar.

Tabla 7

Direccionamiento IPv6

SEGMENTO											ASIGNACIÓN
2801	ab12	abcd	1000	0	0	0	0	/	48		Salida a Internet
2801	ab12	abcd	1000	0	0	0	0	/	52	Sede	**Nivel Central**
2801	ab12	abcd	1000	0	0	0	0	/	64	Subred	Reservada
2801	ab12	abcd	1001	0	0	0	0	/	64	Subred	Piso No. 1
2801	ab12	abcd	1002	0	0	0	0	/	64	Subred	Piso No. 2
2801	ab12	abcd	1003	0	0	0	0	/	64	Subred	Piso No. 3
2801	ab12	abcd	1004	0	0	0	0	/	64	Subred	Piso No. 4
2801	ab12	abcd	1005	0	0	0	0	/	64	Subred	Piso No. 5
2801	ab12	abcd	1006	0	0	0	0	/	64	Subred	Piso No. 6
2801	ab12	abcd	1007	0	0	0	0	/	64	Subred	Piso No. 7
2801	ab12	abcd	1008	0	0	0	0	/	64	Subred	Piso No. 8
2801	ab12	abcd	1009	0	0	0	0	/	64	Subred	Piso No. 9
2801	ab12	abcd	2000	0	0	0	0	/	52	Sede	**Regional Cesar**
2801	ab12	abcd	2000	0	0	0	0	/	64	Subred	Reservada
2801	ab12	abcd	2001	0	0	0	0	/	64	Subred	Piso No. 1

Nota. Listado con el direccionamiento propuesto para la sede Central y la Regional Cesar.

Plan de manejo de Excepciones, Definiendo Aquellos Elementos de Hardware y Software (Aplicaciones y Servicios) que Sean Incompatibles con IPv6

Se hace imperativo la adquisición de los equipos de comunicación descritos en el Apéndice A

, es decir, switch, access point y equipo de videoconferencias. En cambio, los computadores de escritorio podrán tener seis (6) meses más de espera debido a que no son equipos de vital importancia para el funcionamiento de la red y de la institución.

Informe De Preparación de los Sistemas de Comunicaciones, Bases de Datos y Aplicaciones

Es necesario realizar un backup de las bases de datos de Informix Enterprise13 para Vision Web, MySql para la Intranet, Postgres 9.3 para Strategos, SQLServer2012 para SiSAT y Postgres 9.2 para Orfeo – Gestión Documental, así como de las distintas configuraciones de los dispositivos e interfaces de comunicación, tales como routers, teléfonos IP Avaya. Dicha copia de seguridad se debe obtener lo más cercana posible antes de la implementación del protocolo para de ser necesario, realizar un rollback o marcha atrás del proceso de transición.

Se deben realizar las pruebas de funcionalidad que indiquen la viabilidad de la transición, las cuales se pueden completar en simuladores para luego ser implementadas. De la mano con las pruebas se lleva un monitoreo y registro permanente de cada actividad y su afectación a la entidad. (Ver Apéndice G)

Documento que Define Los Lineamientos de Implementación de Ipv6 en Concordancia con La Política de Seguridad de Información y los Controles de Seguridad Informática de la Entidad.

Acorde a las políticas de seguridad de la información del Grupo de Sistemas a cargo de la Secretaría General de la Defensoría del Pueblo se exige la salvaguarda de los activos de información a cargo de funcionarios, contratistas o terceros que cumplan función de custodia y protección.

El servicio de Internet suministrado por la Defensoría del Pueblo es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios, por lo tanto, sin perjuicio de la responsabilidad penal, administrativa o disciplinaria a que haya lugar, éstos al utilizarlo, deben observar y cumplir las directrices que a continuación se enlistan:

- El servicio de Internet institucional únicamente puede ser utilizado para el desarrollo de actividades directamente relacionadas con el cumplimiento de la misión de la Defensoría del Pueblo y las funciones de sus servidores.
- No se permite la utilización de cuentas o contraseñas genéricas para las conexiones de acceso remoto.

Identificación de los Equipos en las Redes

Los dispositivos de cómputo y comunicaciones deben tener un nombre lógico, el cual deberá mantenerse como parte de los registros del activo, para permitirle al administrador de red identificar la ubicación y responsable del mismo.

Protección de los puertos de configuración y diagnostico remoto

El acceso físico a los puertos de configuración y diagnostico debe estar restringido exclusivamente a los responsables de dichas actividades en los respectivos dispositivos.

La red interna de la Defensoría debe contar con una segmentación lógica o física que agrupe los elementos de red con al menos los siguientes segmentos: Red LAN que contiene las estaciones de trabajo y dispositivos de oficina, red para visitantes y red de Servidores.

Control de conexión a las redes.

La Defensoría debe aplicar el principio de menor privilegio posible, que consiste en que solo se otorgan los permisos necesarios para la ejecución de las funciones, de esta forma la conexión desde y hacia redes compartidas debe ser restringida a quienes requieren el acceso y solo con privilegios requeridos.

Controles de las Redes

El administrador de la red es responsable por aplicar los controles necesarios que garanticen la seguridad en la red y de los datos en tránsito. Debe velar que se apliquen al menos los siguientes controles:

- Toda conexión a la red debe contar con un mecanismo de autenticación que valide que el usuario es válido.
- Los usuarios de la red deben utilizar las herramientas de protección configuradas por el Grupo de sistemas, como son antivirus y parches de seguridad.
- El acceso a Internet es realizado únicamente por los medios provistos por la Entidad.
- La seguridad perimetral debe tener mecanismos de control que incluyan: Firewall, IPS, Filtro de contenido, Antivirus y Antispam.
- Las conexiones con las redes públicas deben estar protegidas por un Firewall y los mecanismos de control, que posea las reglas apropiadas para filtrar el tráfico.

- Los usuarios de la red deben hacer uso razonable y con propósitos laborales de la red de comunicaciones.

Plan de Capacitación en IPv6

En cuanto al plan de capacitación a los funcionarios; inicialmente del área de TI de la Defensoría del Pueblo, se recomienda incluirlo y realizarlo en el marco del encuentro anual de ingenieros. Es decir, agendar un espacio en dicho evento para socializar con los demás compañeros la experiencia que nos deja el presente proyecto aplicado. Y así mismo, éstos puedan transmitir el mensaje a las distintas regionales que hacen parte de la institución y los funcionarios que las integran.

La recomendación académica para la programación de cursos de capacitación en el protocolo IPv6 para las Entidades, debe contener como mínimo los siguientes temas:

a. Introducción y aspectos básicos de IPv6

b. Agotamiento de direcciones IPv4, transición a IPv6 y coexistencia

c. Host y enrutamiento en IPv6

d. Servicios y aplicaciones sobre IPv6

e. Seguridad en IPv6 (MinTIC, 2017)

Sin embargo, es vital involucrar a la alta dirección en el proyecto y sobre todo hacerles entender la importancia de implementar IPv6 y su impacto dentro de la organización.

Teniendo en cuenta lo descrito, en la Tabla 8 se sugiere el cronograma de capacitación que se puede llevar a cabo a través de medios virtuales de comunicación.

Tabla 8

Cronograma Capacitación Protocolo IPv6

Fecha	Grupo	Horario
10-OCT-2.024	**Grupo No. 1** (Guajira, Córdoba, Norte De Santander, Meta, Ocaña, Risaralda, Nariño, Urabá, Magdalena Medio, Bolívar)	02:30 – 04:30 P.M.
17-OCT-2.024	**Grupo No. 2** (Antioquia, Atlántico, Chocó, Huila, Cauca, Putumayo, Caquetá, Bogotá, Quindío, Valle)	02:30 – 04:30 P.M.
24-OCT-2.024	**Grupo No. 3** (Arauca, Caldas, Boyacá, Tolima, Guaviare, Santander, Magdalena, Cundinamarca, Sucre, San Andrés)	02:30 – 04:30 P.M.
31-OCT-2.024	**Grupo No. 4** (Amazonas, Casanare, Guainía, Risaralda, Vaupés, Vichada)	02:30 – 04:30 P.M.

Nota. Cronograma para compartir el modelo de transición.

En cuanto a la diagramación del modelo de procesos a través de BPMN se obtiene un prototipo (Ver Apéndice H).

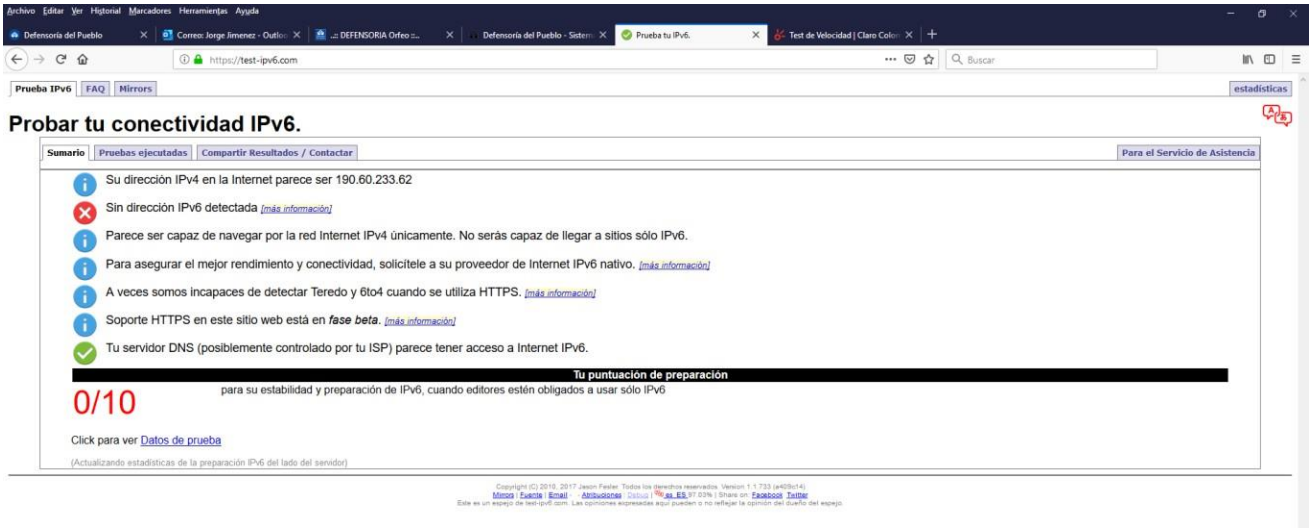
Fase II. Desarrollo del Plan de Implementación del Protocolo IPv6

A lo largo de esta fase se desarrolla el plan de diagnóstico de IPv6 en la red con base en lo establecido en el inventario de activos de información. Con dicho insumo fundamental se define el plan de direccionamiento IPv6, la configuración de direcciones IPv6 en cada uno de los dispositivos, obteniendo; de esta manera, un informe de resultados de las pruebas realizadas a nivel de comunicaciones, aplicaciones y sistemas de almacenamiento.

En la Figura 23 se realiza una prueba para verificar la conectividad actual de IPv6 en la red de datos de la Defensoría del Pueblo Regional Cesar, en la cual se constata que se utiliza una dirección IPv4 (190.60.233.62), también que la ISP es la empresa Claro, de igual manera, detecta que esta “parece tener acceso a Internet IPv6“.

Figura 23

Prueba de Conectividad IPv6

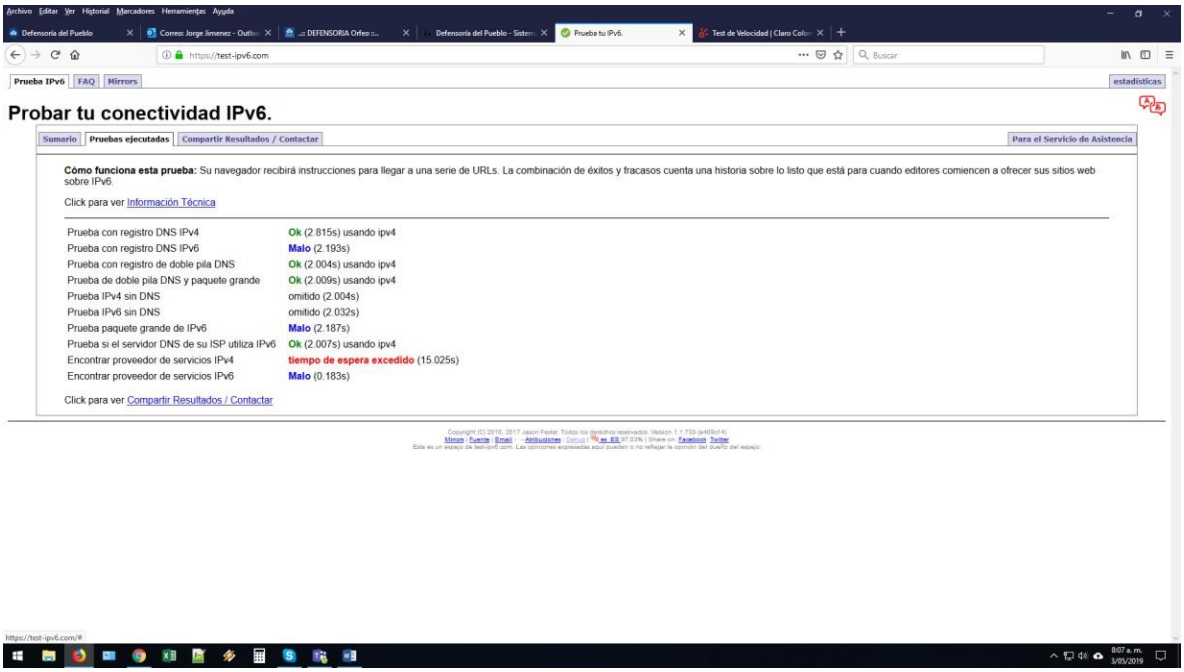


Nota. Se realiza test de conectividad IPv6, indicando que no se detecta la dirección IPv6.

A través de la Figura 24 se detecta que la doble pila para DNS funciona, así mismo los servidores DNS de la ISP están preparados para utilizar IPv6. Se ejecuta una prueba de conectividad en línea desde el sitio htpps://test-ipv6.com, la cual nos permite concluir que la entidad no está utilizando el protocolo IPv6.

Figura 24

Pruebas de IPv6 Ejecutadas



Nota. Se ejecuta prueba, encontrando que los DNS y paquetes IPv6 no funcionan**.**

Ahora, se describe el plan de diagnóstico que tiene como meta utilizar los resultados obtenidos en la Fase I, y decidir cuál es la manera más viable para desarrollar el plan de implementación dejando de forma clara la técnica que se debe tener en cuenta; por ejemplo, para activar las políticas de seguridad o configurar el protocolo IPv6 en los sistemas de comunicación, los aplicativos y los servidores, entre otras actividades.

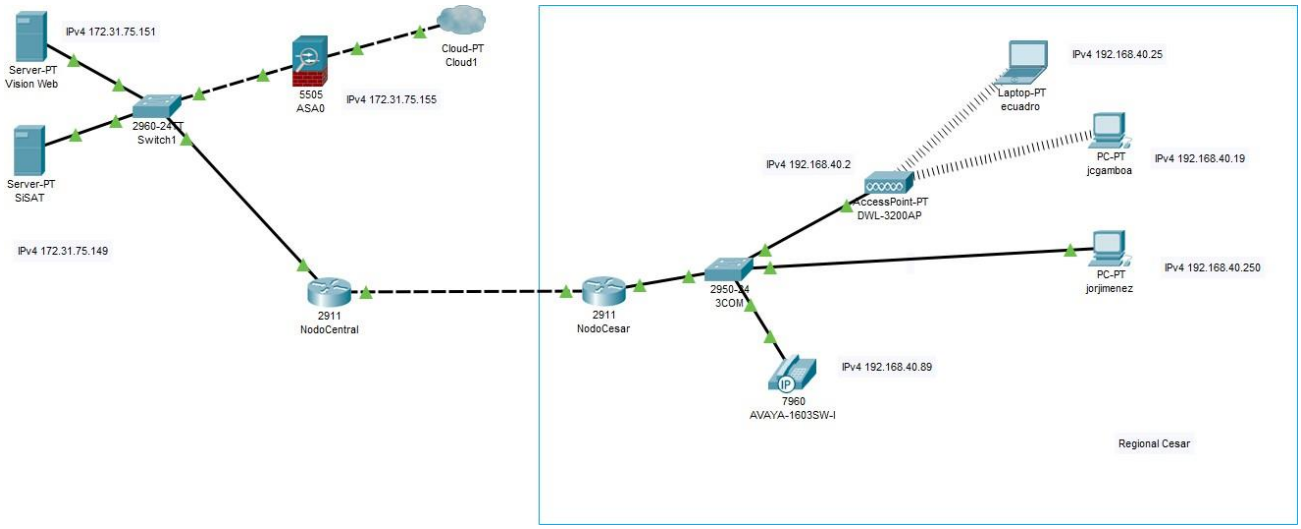
Inicia el Plan de Diagnóstico

Habilitación Direccionamiento Ipv6 para cada uno de los Componentes de Hardware y Software de Acuerdo al Plan De Diagnóstico de la Primera Fase

Para efectos de simular el direccionamiento IPv6 se han tomado como muestra los servidores de VisionWeb y SiSAT en el nodo de Nivel Central en la ciudad de Bogotá, así mismo, la telefonía IP con AVAYA, el PC de jcgamboa, el PC de jorjimenez y la Laptop de ecuadro, en la red de datos de la sede de Valledupar, tal como lo representa la Figura 25.

Figura 25

Diagrama de Red para Pruebas



Nota. Simulación de red por medio de la aplicación: Cisco Packet Tracer v7.2.1

Configuración de servicios de DNS, DHCP, Seguridad, VPN, servicios WEB, entre otros

DNS

El Sistema de Nombres de Dominio es una tecnología indispensable para la navegación en Internet, el Registro de Direcciones de Internet para América Latina y el Caribe - LACNIC recomienda el uso de un software basado en Unix llamado BIND (Berkeley Internet Name

Domain), el cual permite configurar el servidor para que conteste de manera automática al dominio.

Montañez, 2018 afirma: “Es necesario también utilizar una modificación al DNS, llamada DNS64, que permite generar un registro AAAA aun cuando el destino no tenga dirección IPv6 (es decir, el DNS responda sólo con registros de tipo A)” (p 36).

Evidenciamos en la

Figura *26* los DNS utilizados en la actualidad, referenciados así:

Preferido: 172.31.75.152

Alternativo: 172.31.75.143

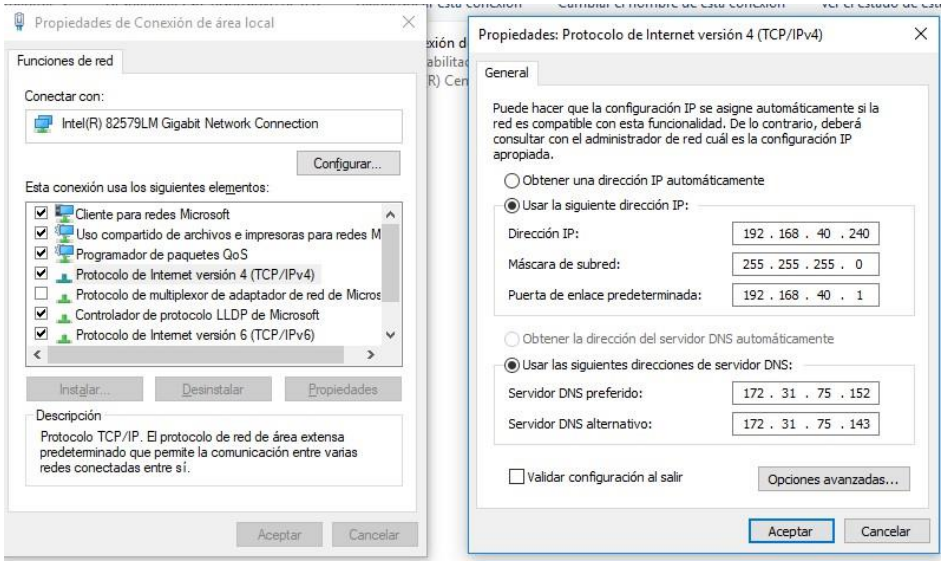
Los DNS para el protocolo IPv6 quedarían de la siguiente manera:

Preferido: 2801:ab12:abcd::8888

Alternativo: 2801:ab12:abcd::4444

Figura 26

DNS IPv4 Actuales

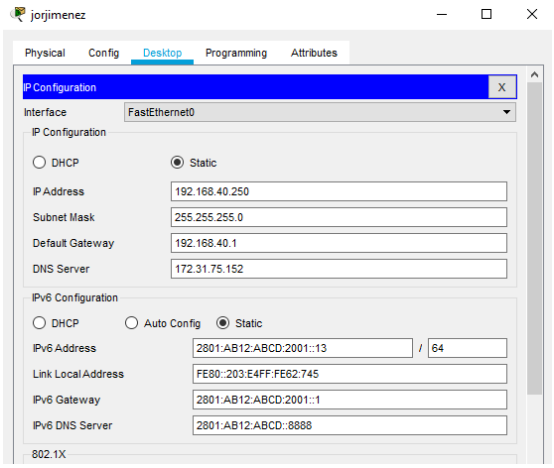


Nota. Vista de los DNS que se utilizan.

Como se aprecia en la Figura 27, la configuración utilizada en la simulación para el computador del usuario “jorjimenez”, tanto para el protocolo IPv4 como para el protocolo IPv6. Teniendo presente el direccionamiento IPv6 de la Tabla 7.

Figura 27

Configuración Ipv4 e IPv6 del Pc Jorjimenez en la Simulación



Nota. Configuración del computador “jorjimenez”.

DHCP

El protocolo de configuración dinámica de host (en inglés: Dynamic Host Configuration Protocol, también conocido por sus siglas de DHCP) permite asignar de forma dinámica las direcciones IP a cada uno de sus clientes. Para la fase de implementación se debe utilizar el Protocolo de Configuración Dinámica de Hosts para IPv6 (DHCPv6), el cual es un protocolo cliente-servidor, definido en la RFC 3315 de la IETF, que proporciona una configuración administrada de dispositivos sobre IPv6.

Sin embargo, se recomienda seguir con la política actual de manejo de direcciones IP, es decir, realizar asignaciones estáticas a cada dispositivo e interfaz de red, lo anterior, en aras de ejercer un control más eficaz al momento de administrar la red de datos. Teniendo en cuenta el listado de la Tabla 7 en cuanto a la asignación de direcciones IPv6.

Seguridad

IPSec (Internet Protocol Security), es un conjunto de estándares del IETF para incorporar servicios de seguridad en IP y que responde a la necesidad creciente de garantizar un nivel de seguridad imprescindible para las comunicaciones entre empresas y comercio electrónico (Pérez, 2018).

IPSec proporciona servicios de protección a la capa IP permitiendo que un sistema elija los protocolos de seguridad necesarios, determine los algoritmos que va a usar para los servicios y ubique las claves criptográficas necesarias para proveer los servicios solicitados (Lobo y Rico, 2011).

De acuerdo con el RFC 2367, IPSec es una parte obligatoria de IPv6, en cambio, su uso es opcional con IPv4.

Es imperativo aplicar las buenas prácticas recopiladas en el RFC 7217, en el cual se describe el método para generar identificadores de interfaz semánticamente opacos a través del uso de SLAAC (Stateless Address Autoconfiguration), siendo ésta a su vez, una metodología para asignación dinámica de direcciones IPv6 para los nodos principales de la red. Aunque; preferiblemente, se realizarán asignaciones estáticas.

VPN

Significa Virtual Private Network, en español Red Privada Virtual.

Con VPN es posible establecer una comunicación vía infraestructura pública entre dos estaciones de trabajo remotas sin correr el riesgo que terceras personas ajenas a la organización pueda acceder a dicha información ni al sistema de interconexión.

Esta tecnología permite crear un túnel de encriptación a través de la Internet u otra red pública de tal forma que permita a los usuarios que se encuentran en los extremos del túnel

disfrutar de la seguridad, privacidad y funciones que antes estaban disponibles solo en redes privadas.

(Limari, 2004, p. 12)

La conmutación de etiquetas multiprotocolo o MPLS (del inglés Multiprotocol Label Switching).

Malek, Alhomdy, Alselwi, Alowiri y Sharaby (2016) aseguran que:

"MPLS es esencialmente un sistema de etiquetado diseñado para aceptar múltiples protocolos. Fue originalmente presentado como una forma de mejorar la velocidad de reenvío de enrutadores. La tecnología MPLS ahora está emergiendo como una tecnología estándar crucial que está siendo utilizada por muchos ISPs. Ingeniería de tráfico y soporte VPN son ejemplos de dos aplicaciones clave donde MPLS es superior a cualquier tecnología IP actualmente disponible".

Teniendo en cuenta lo anterior se debe configurar MPLS 6PE, cuyas principales ventajas son:

- Permite implementar IPv6 sin tocar el CORE
- Solo se configuran los PE
- Se pueden elegir los PE en los que se habilitará
- Los PE serán dual stack y no perderán funcionalidad IPv6
- No tiene problemas de performance o escalabilidad
- Requiere tener MPLS en el backbone

A continuación, en la Tabla 9 se describen los comandos utilizados para configurar el Router del Nodo Central:

Tabla 9

Comandos Utilizados para Configurar el Router del Nodo Central

No.	Comando	Descripción
1	interface FastEthernet0/0 ip address 172.31.75.1 255.255.255.0 ipv6 address 2801:AB12:ABCD:1001::1/52 no shu !activar el puerto	Se habilita el puerto 0/0 y se asignan IPs estáticas en el protocolo 4 y 6
2	!PUERTO SERIE COMUNICAR NodoCesar interface Serial0/1/0 ip address 192.168.3.2 255.255.255.0 ipv6 address 2801:AB12:ABCD:3000::2/52 no shu !activar el puerto	Se habilita y configura el puerto serial para la comunicación entre routers
3	ipv6 unicast-routing	Se habilita el enrutamiento tipo Unicast, es decir, para dirigirse a un host específico
4	!CONFIGURAR LA TABLA DE ENRUTAMIENTO !IPv4 ip route 192.168.40.0 255.255.255.0 192.168.3.1 ipv6 route ::/0 2801:AB12:ABCD:3000::1	Se configuran las tablas de enrutamiento, tanto en IPv4 como en IPv6

Nota. Listado con los comandos que permiten la configuración del enrutador.

Servicios WEB

Un punto para tener en cuenta aquí es que el servidor debería estar configurado para responder requerimientos tanto en IPv4 como en IPv6 (Fonseca, 2017, p. 52).

En el caso de que el servidor web utilice Apache no debe existir ninguna clase de conflicto con IPv6. Después de configurar la interfaz de red, agregó la función IIS a un servidor

Microsoft Windows 2018 R2, la página index.html predeterminada era reemplazada por una página personalizada (Dunand, 2012, p. 39).

En concordancia con lo plasmado en el Apéndice F

; en el momento, todos los servidores web con que trabaja la organización cuentan con soporte de IPv6.

Correo Electrónico

El servicio es provisto de manera externa por Microsoft, por lo tanto, no existe ningún tipo de inconveniente en cuanto a la transición.

Directorio Activo

En lo que respecta al Directorio activo (Dominio), como mencionó Fonseca (2017): "La implementación más utilizada para este tipo de directorios es LDAP y un software de código abierto ampliamente difundido es openLDAP, que soporta IPv6 en modo nativo" (p 52).

Configuración del protocolo IPv6 en Aplicativos, Sistemas de Comunicaciones, Sistemas de Almacenamiento y en General de los Equipos Susceptibles a Emplear Direccionamiento IP

La Tabla 10 lista las direcciones específicas para cada dispositivo y la interfaz que se utilizarán en la Red de Datos de la Defensoría del Pueblo Regional Cesar, teniendo en cuenta la segmentación de la misma para un control eficaz y futuras ampliaciones.

Tabla 10

Direccionamiento IPv6 por Dispositivo

Dispositivo	Interfaz	Dirección / Prefijo Ipv6	Gateway Predeterminado
Router Nodo Nivel Central	G O/O	2801:ab12:abcd:1000:0:0:0:1/52	N/A
Reservada		2801:ab12:abcd:1000:0:0:0:0/64	
Servidor VisionWeb	NIC	2801:ab12:abcd:1001:0:0:0:2/64	2801:ab12:abcd:1000:0:0:0:1
Servidor SiSAT	NIC	2801:ab12:abcd:1001:0:0:0:4/64	2801:ab12:abcd:1000:0:0:0:1
Router Nodo Cesar	G O/O	2801:ab12:abcd:2000:0:0:0:1/52	N/A
Reservada		2801:ab12:abcd:2000:0:0:0:0/64	
Access Point	NIC	2801:ab12:abcd:2001:0:0:0:1/64	2801:ab12:abcd:2000:0:0:0:1
VoIP-AVAYA	NIC	2801:ab12:abcd:2001:0:0:0:10/64	2801:ab12:abcd:2000:0:0:0:1
Laptop-ecuadro	NIC	2801:ab12:abcd:2001:0:0:0:11/64	2801:ab12:abcd:2000:0:0:0:1
PC-jcgamboa	NIC	2801:ab12:abcd:2001:0:0:0:12/64	2801:ab12:abcd:2000:0:0:0:1
PC-jorjimenez	NIC	2801:ab12:abcd:2001:0:0:0:13/64	2801:ab12:abcd:2000:0:0:0:1

Nota. Direcciones IPv6 que corresponden a cada dispositivo que hace parte de la red.

Activación de Políticas de Seguridad de Ipv6 En los Equipos de Seguridad y Comunicaciones que Posea cada Entidad de Acuerdo con los RFC de Seguridad en IPv6

IPSec (Protocolo de Seguridad en Internet), es una herramienta utilizada en las redes virtuales privadas, su uso más difundido es la conexión equipo a equipo.

Plan de Contingencias o Rollback (marcha atrás)

Es muy importante diseñar un plan de contingencias en caso de que se deba reversar todo el proceso de transición, teniendo en cuenta las copias de seguridad (backups) realizadas, así como los tiempos de cada etapa de la contingencia (Ver Apéndice G). En la Figura 28 se aprecian los objetivos de cada etapa, como lo son el punto de recuperación (RPO) antes del inicio del plan de contingencia, así como el tiempo de recuperación (RTO) al completar el plan de contingencia.

Figura 28

Descripción General del Plan de Contingencias

Nota. (MinTIC, 2018).

"No estar preparado es prepararse para fracasar". –

Benjamin Franklin

Coordinación con el (los) Proveedor (Es) de Servicios de Internet ISP, para Establecer el Enrutamiento y la Conectividad Integral en Ipv6 Hacia el Exterior

Desde que inicia el proceso de transición es conveniente contactar con el proveedor del servicio de Internet para empezar un trabajo en conjunto, de él no se necesita sólo la asignación del pool de direcciones, en muchas ocasiones se tienen dispositivos de la entidad en gestión del ISP o dispositivos de éste en alquiler a las entidades, lo que obliga directamente a crear en conjunto una comunicación que no impida el proceso de migración.

(Fonseca, 2007, p. 50)

Se debe realizar el contacto con el ISP Claro para articular el proceso de migración y acordar la ruta de trabajo que permita llevar a cabo la transición. Teniendo en cuenta que el pool de direcciones será solicitado por la organización directamente a LACNIC.

Entregables de la Fase II

a) Preparación y presentación del Informe del plan detallado de implementación del nuevo protocolo.

El plan detallado de implementación en la red de datos de la Defensoría del Pueblo Regional Cesar conlleva:

- Solicitar a LACNIC el pool o segmento de direcciones IPv6.

Por ejemplo: 2001:ab12:abcd /48

- Definir el mecanismo de transición, se recomienda Doble Pila
- Configurar las direcciones IPv6, acorde a la tabla definida
- Realizar las pruebas de conectividad entre nodos, servicios de red y equipos de

b) Documento con todas las configuraciones del nuevo protocolo realizadas en las plataformas de hardware, software y servicios que se han intervenido durante esta fase, incluye las configuraciones a realizar sobre el canal (canales) de comunicaciones con acceso a internet.

A través de la Tabla 11 se registran todos los equipos de la entidad, encontrando cinco equipos "No compatibles" con el protocolo IPv6 debido a que el Sistema Operativo instalado es Windows Xp. Lo anterior, los hace tecnológicamente obsoletos.

Tabla 11

Configuración de los Equipos de Comunicaciones, de Aplicaciones y Sistemas de Almacenamiento

No.	Equipo	Marca	Modelo	Dependencia	Placa	Sistema Operativo	Versión	Dirección IPv6
1	PORTÁTIL	LENOVO	ThinkPad Edge	COMUNITARIOS	24604	Windows	7 Pro	2801:ab12:abcd:2001:0:0:0:20
2	ESCRITORIO	HP COMPAQ	8200 ELITE	DESPLAZADOS	25135	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:21
3	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	VICTIMAS	34512	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:22
4	ESCRITORIO	HP COMPAQ	8200 ELITE AIO	VICTIMAS	29225	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:23
5	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	CRIMINALISTICA	34521	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:24
6	ESCRITORIO	HP COMPAQ	8200 Elite	ATQ	25153	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:25
7	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	PPDD	34520	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:26
8	ESCRITORIO	HP	8300 Elite AIO	SAT	27792	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:27
9	ESCRITORIO	HP COMPAQ	dC5700	PUBLICA	18863	Windows	Xp	NO COMPATIBLE
10	ESCRITORIO	COMPAQ	CQ5105LA	RUP	22779	Windows	Xp	NO COMPATIBLE
11	ESCRITORIO	HP COMPAQ	6200 PRO	SISTEMAS	26155	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:28
12	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	ETNICOS	34514	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:29
13	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	ASUNTOS AGRARIOS	34510	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:30

14	ESCRITORIO	HP	dx2300	PUBLICA	18457	Windows	Xp	NO COMPATIBLE
15	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	PUBLICA	34518	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:31
16	ESCRITORIO	HP COMPAQ	8300 Elite AIO	PUBLICA	27641	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:32
17	ESCRITORIO	HP COMPAQ	6200 PRO	FRONTERAS	26156	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:33
18	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	PUBLICA	34516	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:34
19	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	ATQ	34519	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:35
20	ESCRITORIO	COMPAQ	CQ5105LA	ATQ	22780	Windows	Xp	NO COMPATIBLE
21	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	ATQ	34517	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:36
22	ESCRITORIO	HP COMPAQ	8300 Elite AIO	VICTIMAS	27793	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:37
23	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	VICTIMAS	34513	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:38
24	ESCRITORIO	COMPUMAX	A68F2P-M4	AYUDANTE OFICINA	36816	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:39
25	ESCRITORIO	COMPUMAX	A68F2P-M4	RAJ	36815	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:40
26	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	PUBLICA	34189	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:41
27	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	PUBLICA	34515	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:42
28	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	PUBLICA	34511	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:43
29	ESCRITORIO	COMPAQ	CQ5105LA	ATQ	22781	Windows	Xp	NO COMPATIBLE
30	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	DESPACHO	34187	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:44
31	ESCRITORIO	LENOVO	10NN0006LS	ORFEO	38364	Windows	10 Pro	2801:ab12:abcd:2001:0:0:0:45
32	MULTIFUNCIONAL	HP	LASERJET 2727nf	PUBLICA	26237	NA	NA	2801:ab12:abcd:2001:0:0:0:101
33	MULTIFUNCIONAL	HP	LASERJET 2727nf	ATQ	26238	NA	NA	2801:ab12:abcd:2001:0:0:0:102
34	IMPRESORA	HP	LASERJET P3005dn	SAT	18109	NA	NA	2801:ab12:abcd:2001:0:0:0:103
35	IMPRESORA	LEXMARK	E360dn	DECLARACIONES	29265	NA	NA	2801:ab12:abcd:2001:0:0:0:104
36	IMPRESORA	HP	LASERJET P3015	DUPLA	25250	NA	NA	2801:ab12:abcd:2001:0:0:0:105

37	MULTIFUNCIONAL	LEXMARK	MX511de	SECRETARIA	34879	NA	NA	2801:ab12:abcd:2001:0:0:0:106
38	IMPRESORA	SAMSUNG	PROXPRESS M4030ND	DESPACHO	36552	NA	NA	2801:ab12:abcd:2001:0:0:0:107
39	ACCESS POINT	CISCO	WAP351	TODOS	NT	NA	NA	2801:ab12:abcd:2001:0:0:0:2
40	ROUTER	JUNIPER	SRX300	TODOS	ISP	LINUX	NA	2801:ab12:abcd:2001:0:0:0:1
41	FIBRA ÓPTICA	VCOM	VKS10025A	TODOS	ISP	NA	NA	NO APLICA
42	TELÉFONO IP	AVAYA	1603SW-I	TODOS	NT	NA	NA	2801:ab12:abcd:2001:0:0:0:89
43	VIDEOCONFERENCIA	POLYCOM	RealPresence 500	TODOS	NT	NA	NA	2801:ab12:abcd:2001:0:0:0:222
44	SWITCH	TrendNet	TEG-448WS	TODOS	NT	NA	NA	NO APLICA

Nota. Recopilación del inventario de TI.

Certificado del prefijo expedido por LACNIC. [2001:ab12:abcd /48] Configuración de los Servidores del Nodo Central

Dirección servidor [VisionWeb] en IPv4 Fa0/0 → 172.31.75.151 Dirección servidor [VisionWeb] en IPv6 Fa0/0 → 2801:ab12:abcd:1001::2 Dirección servidor [VisionWeb] en IPv4 Serial 0/1/0 → IPv4 192.168.3.1

Dirección servidor [VisionWeb] en IPv6 Serial 0/1/0 → 2801:ab12:abcd:3000:0:0:0:1/52 Dirección servidor [SiSAT] en IPv4 → 172.31.75.151

Dirección servidor [SiSAT] en IPv6 → 2801:ab12:abcd:1001:0:0:0:4 Dirección servidor [SiSAT] en IPv4 Serial 0/1/0 → 192.168.3.2

Dirección servidor [SiSAT] en IPv6 Serial 0/1/0 → 2801:ab12:abcd:3000:0:0:0:2/52 Configuración de Equipos de la Regional Cesar

Dirección Pc [jorjimenez] en IPv4 → 192.168.40.250

Dirección Pc [jorjimenez] en IPv6 → 2801:ab12:abcd:2001:0:0:0:13 Dirección Laptop [ecuadro] en IPv4 → 192.168.40.25

Dirección Laptop [ecuadro] en IPv6 → 2801:ab12:abcd:2001:0:0:0:11

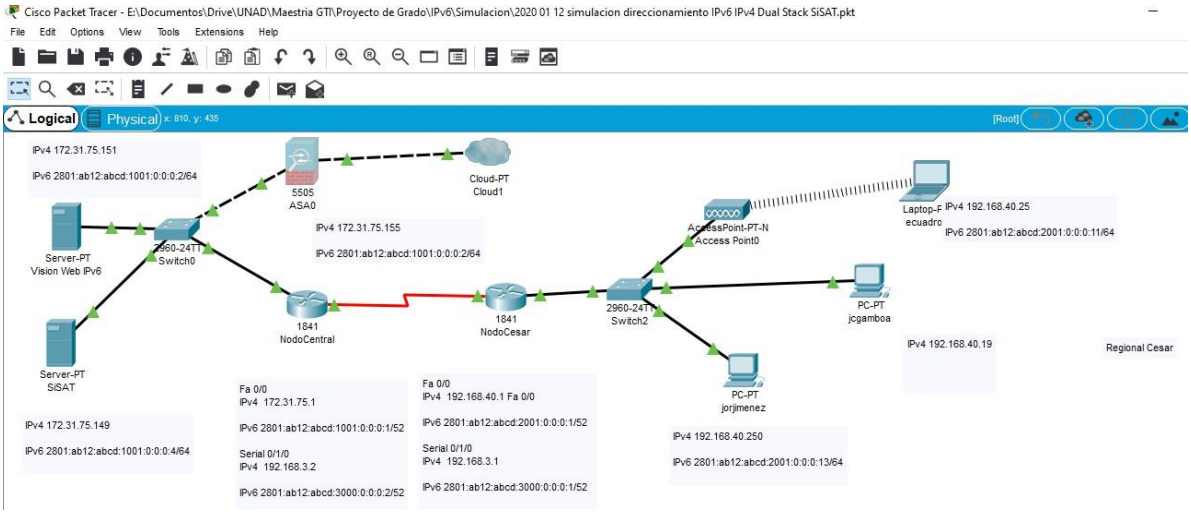
Dirección Pc [jcgamboa] en IPv4 → 192.168.40.19 Dirección Pc [jcgamboa] en IPv6 → no configurado

c) Informe de configuración de las pruebas realizadas a nivel de comunicaciones, de aplicaciones y sistemas de almacenamiento.

Para realizar la simulación, se utilizó el software Packet Tracer con el fin de replicar las condiciones de la Defensoría del Pueblo, por lo tanto, se representa la simulación red de datos por medio de la Figura 29, comunicación entre el nodo Cesar y el nodo Central. Y las respectivas pruebas. (Ver Apéndice I).

Figura 29

Simulación del Direccionamiento con Pila Doble



Nota. Dual stack de la rede de datos de la Defensoría del Pueblo.

Configuración aplicada a los nodos de la red. (Ver Apéndice J)

Presupuesto

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. (Gartner, 2011). A continuación, se describe la Tabla 12, en cuanto al presupuesto.

Tabla 12

Estimación del Recurso Humano y Técnico

Recurso	Descripción	Costo
1. Equipo Humano	Responsable del Grupo de Sistemas Ingeniero de Sistemas de la Regional Asesor MinTIC (Ingeniero de Seguridad)	$ 0.00
2. Equipos y Software	Computadores Acceso a internet	$ 0.00
3. Viajes y Salidas de Campo	Viaje a Bogotá (verificar centro de datos)	$ 500,000.00
4. Materiales y suministros	Papelería, fotocopias, transporte Cableado Estructurado	$ 12,000,000.00
5. Pool LACNIC	Cuota de Membresía	$ 8,000,000.00
	Renovación Anual	$ 1,920,000.00
6. Equipos de Comunicaciones y de Cómputo	Access Point Wireless-N	$ 985,000.00
	Videoconferencia	$ 6,400,000.00
	Switch Capa 3 48 puertos Gigabit	$ 1,700,000.00
	5 Computadores de Escritorio	$ 19,000,000.00
7. Bibliografía	Bibliotecas virtuales: e-Biblioteca, e-Hemeroteca	$ 0.00
8. Imprevistos (15%)	Gastos surgidos no tenidos en cuenta	$ 7,575,750.00
TOTAL		**$ 58,080,750.00**

Nota. Recursos para la ejecución del proyecto.

Conclusiones

El agotamiento de las direcciones IPv4, evidenciado por las alertas de LACNIC, sumado al incremento sostenido de servicios digitales, hacen imperativa la adopción de IPv6. Su implementación garantiza la escalabilidad, seguridad y eficiencia en la prestación de servicios digitales, pilares fundamentales para el cumplimiento de la misión institucional de la Defensoría del Pueblo – Regional Cesar.

Su implementación posiciona a la entidad dentro de los estándares modernos de interoperabilidad exigidos por el Gobierno Digital.

La infraestructura de red inalámbrica, el uso de equipos sin cableado estructurado, el bajo ancho de banda y la congestión en horarios pico son factores que afectan negativamente la calidad del servicio y la atención al ciudadano. Estas condiciones deben abordarse con urgencia mediante la modernización del hardware y el rediseño de la topología de red.

La Fase I permitió realizar un diagnóstico detallado del entorno tecnológico de la Defensoría del Pueblo – Regional Cesar, en donde se evidenció la importancia del levantamiento de inventario de activos de información y su compatibilidad con IPv6, esta etapa resultó crucial para definir la viabilidad y alcance del proceso de transición tecnológica. El estudio determinó que el 89% del hardware y software existente es compatible con IPv6, se identificaron equipos de comunicación y cómputo obsoletos que requieren reemplazo inmediato para evitar cuellos de botella tecnológicos y riesgos de seguridad. (Ver Apéndice B)

La implementación del mecanismo de coexistencia entre IPv4 e IPv6 a través de Dual Stack fue determinada como la estrategia más adecuada para garantizar la continuidad de los servicios mientras se adopta completamente la nueva versión del protocolo. Esta técnica evita interrupciones abruptas y permite una transición fluida.

Se aplicaron estándares internacionales (RFC) para asegurar que las decisiones técnicas —como la asignación de direcciones, seguridad, y mecanismos de coexistencia— estén alineadas con buenas prácticas, garantizando así una transición ordenada y segura.

El trabajo desarrollado en la sede Regional Cesar constituye un piloto aplicable a otras sedes de la Defensoría del Pueblo. La documentación del proceso, el inventario de activos, los planes de direccionamiento y las simulaciones realizadas sientan las bases para una estandarización de la transición en todo el territorio nacional. (Ver Manual IPv6)

El modelo adoptado evidencia que la migración a IPv6 debe ser entendida como un proceso progresivo, donde la participación de todos los actores —técnicos, administrativos y directivos— es crucial para su éxito y sostenibilidad en el tiempo.

Recomendaciones

La Defensoría del Pueblo – Regional Cesar debe implementar el cableado estructurado certificado en la sede de la entidad o en su defecto, adquirir un Access Point Wireless WiFi Dual Band 2.4 + 5GHz AC1200 with PoE, el cual cuenta con soporte IPv6 y WiFi de próxima generación 802.11ac y/o uno con características similares o superiores.

La entidad también debe realizar la solicitud previa del segmento (Pool) de direcciones en IPv6 ante LACNIC, con el fin de preparar la implementación con estas direcciones; teniendo en cuenta que esta actividad representa las siguientes ventajas:

La entidad tendrá su propio segmento de direcciones IPv6 (Portabilidad numérica de direcciones IPv6), cuyo tráfico de IPv6 será visible a nivel de la comunidad de Internet, y esto facilitaría ver el tráfico cursado por la entidad desde LACNIC.

La entidad tendrá total independencia de su proveedor de servicio de internet, sin verse afectado por las licitaciones anuales que conllevan a dicho cambio.

Referencias Bibliográficas

Arafat, M., Ahmed, F. and Sobhan, M. (2014). On the Migration of a Large Scale Network from IPv4 to IPv6 Environment, International Journal of Computer Networks & Communications (IJCNC), 6(2), pp.111-126.

Articles-5482_G20_Transicion_IPv4_IPv6.pdf. (s/f). https://mintic.gov.co/portal/715/articles-125210_Guia_Transicion_IPV4_IPV6_Colombia_27052021.pdf

Cisco (2019). *6lab - The place to monitor IPv6 adoption*. https://6lab.cisco.com/index.php

Duque JL& EO. Protocolo TCP/IP. (2004). http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ir00913a&AN=unad.10596.5339&lang=es&site=eds-live.

Estrategia Gobierno En Línea en MinTIC - Ministerio de Tecnologías de la Información y las Comunicaciones. (s/f). http://www.mintic.gov.co/portal/604/w3-propertyvalue-7060.html

Fonseca, D. (2017). *Plan de transición del protocolo de red IPv4 a IPv6 basado en las recomendaciones realizadas por el Min TIC Colombia*, (tesis de pregrado). Universidad de Cundinamarca, Fusagasugá, Colombia. http://fusagasugacundinamarca.gov.co/Transparencia/MODELO%20INTEGRADO%20DE%20PLANEACION%20Y%20GESTION/Plan%20de%20Transicion%20del%20Protocolo.pdf

Fundamentos IPv6. (s/f). http://www.ipv6.mx/index.php/informacion/fundamentos/ipv6

Fundamentos de Redes. (2024) . Universidad Abierta y a Distancia de México. Unidad 3. Direccionamiento IP.

Cicileo G., Gagliano R., O'Flaherty C., Olvera C., Palet J., Rocha M., Vives A. *IPv6 para todos Guía de uso y aplicación para diversos entornos*. http://www.ipv6tf.org/pdf/ipv6paratodos.pdf

LANIC. http://portalipv6.lacnic.net/quienes-implementan/

Mendoza, G. (2011). *IPv6: estudio sobre las barreras para su implementación* (minor). Universidad Tecnológica de Bolívar, Cartagena de Indias, Colombia. http://biblioteca.utb.edu.co/notas/tesis/0062649.pdf

Mecanismos de Transición y RFCs. (s/f). http://www.ipv6.mx/index.php/informacion/rfcs

Monitor adopción de IPv6 de Cisco. http://6lab.cisco.com/stats/

Performance comparison analysis of E2E Dual-Stack IP protocol method over wired and Wi-Fi broadband access. (2016). *2016 International Conference on Frontiers of Information Technology (FIT), Frontiers of Information Technology (FIT), 2016 International Conference On, 7*. https://bibliotecavirtual.unad.edu.co:2444/10.1109/FIT.2016.7857509

Promoción de la adopción el IPv6 en Colombia http://www.mintic.gov.co/portal/604/articles-5932_documento.pdf

¿Qué es el TCP/IP? - Definición de TCP/IP (s/f). http://www.masadelante.com/faqs/tcp-ip

Malek N. A., Sharaf A. A., Gamil A., Ameen A. A. y Naif S. (2016). Performance Analysis of IPv6 over MPLS & MPLS-VPN for Sana'a University. *IJISET - International Journal of Innovative Science, Engineering & Technology*, *3* (5), 165-169.

¿Qué es la transición a IPv6?

http://www.mintic.gov.co/portal/604/w3-article-5893.html

Palet M. J., IPv6 para Gobiernos y Empresas: Impacto e Implementación en 12Pasos.

https://www.lacnic.net/innovaportal/file/2943/1/ipv6-para-gobiernos-y-empresas-parte1-con-pics.pdf

Ramírez S, y Cervantes M. - "Introducción a IPV6" (2015) Red Académica Uruguaya (RAU)

https://www.rau.edu.uy/ipv6/queesipv6.htm#01

TIC para Servicios - Estrategia GEL. (s/f).

http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-8011.html

Vyncke.org. (2019). *Projection of IPv6 %-age of IPv6-Enabled Web Browsers (courtesy Google) in Colombia*. https://www.vyncke.org/ipv6status/project.php

Apéndices

Apéndice A

Equipos de Comunicaciones

Equipo	Marca	Modelo	Sistema Operativo	Puertos Ethernet	Rol	Versión IP	Dirección IP	PLACA
ACCESS POINT	DLINK	DWL-3200AP	N/A	1 Fast Ethernet x 10/100Mbps. PoE	Punto de acceso WiFi	IPv4	192.168.40.1	18145
ROUTER	JUNIPER	SRX300	Linux	1 Fast Ethernet x 10/100Mbps.	Canal dedicado 15 Mbps	IPv4 / IPv6	172.30.120.117	Claro
FIBRA ÓPTICA	VCOM	VKS10025A	N/A	TX-RX	Canal dedicado 15 Mb	N/A	N/A	Claro
TELÉFONO IP	AVAYA	1603SW-I	N/A	1 Fast Ethernet x 10/100Mbps. QoS	Voz IP	IPv4 / IPv6	192.168.40.89	NT
VIDEOCONFERENCIA	POLYCOM	VSX 5000 NTSC	N/A	1 Fast Ethernet x 10/100Mbps.	Comunicación - Videoconferencia	IPv4	192.168.40.222	24817
SWITCH	3COM	2024	N/A	24 Fast Ethernet x 10/100Mbps.	Comunicación	IPv4	N/A	15433

Apéndice B

Listado Equipos con compatibilidad IPv6 para adquisición

Tipo de Equipo	Cantidad	Equipo	Sistema Operativo	Puertos Ethernet	Rol	Versión IP
Comunicaciones	1	ACCESS POINT	Linux	5 Ethernet 10/100/1000 compatibles con 802.3af/at PoE	Punto de acceso WiFi	IPv6 Ready
Comunicaciones	1	VIDEOCONFERENCIA	N/A	Ethernet 10/100/1G (x1)	Comunicación - Videoconferencia	IPv6
Comunicaciones	1	SWITCH	N/A	48 puertos Gigabit	Comunicación	IPv6
Cómputo	5	COMPUTADOR DE ESCRITORIO	Win 10 Pro	1 Fast Ethernet x 100/1000M bps.	USUARIO	IPv6

Apéndice C

Equipos de Cómputo

No.	Equipo	Marca	Modelo	Dependencia	Placa	Memoria	Procesador	Disco Duro	Sistema Operativo	Versión	Software Instalado	Rol	Versión IP
1	PORTÁTIL	LENOVO	ThinkPad Edge	COMUNITARIOS	24604	2 Gb	Core i3 M350 2,27GHz 32 bits	320 GB	Windows	7 Pro	Office Home and students 2010, Kaspersky endpoint 10	USUARIO	IPv4 / IPv6
2	ESCRITORIO	HP COMPAQ	8200 ELITE	DESPLAZADOS	25135	4 Gb	Core i3 2120 3,3GHz 64 bits	500Gb + 500Gb	Windows	10 Pro	Office 2010, Kaspersky endpoint 10	USUARIO	IPv4 / IPv6
3	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	VICTIMAS	34512	4 Gb	Intel Pentium G3450 3.40GHz 64 bits	500Gb	Windows	10 Pro	Ofiice Hogar y Empresa 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
4	ESCRITORIO	HP COMPAQ	8200 ELITE AIO	VICTIMAS	29225	4 Gb	Core i5 2400S 2,5GHz 64 bits	500 Gb	Windows	10 Pro	Office Hogar y empresa 2010, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
5	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	CRIMINALISTICA	34521	4 Gb	Intel Pentium G3450 3.40GHz 64 bits	500 Gb	Windows	10 Pro	Office Hogar y empresa 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
6	ESCRITORIO	HP COMPAQ	8200 Elite	ATQ	25153	4 Gb	Core i3 2120 3,3GHz 64 bits	500 Gb +500 Gb	Windows	10 Pro	Office Professional plus 2010, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
7	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	PROMOCIÓN Y DIVULGACIÓN	34520	4 Gb	Intel Pentium G3450 3.40GHz 64 bits	500 Gb	Windows	10 Pro	Office Hogar y Empresa 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
8	ESCRITORIO	HP	8300 Elite AIO	SAT	27792	8 Gb	Core i7 3770 3,4 GHz 64 Bits	1 Tb	Windows	10 Pro	Office Professional plus 2010, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
9	ESCRITORIO	HP COMPAQ	dC5700	PUBLICA	18863	1 Gb	Intel Pentium Dual CPU 1,6 GHz 32 Bits	80 Gb	Windows	Xp	Office Estándar 2007, Kaspersky endpoint 10	USUARIO	IPv4

10	ESCRITORIO	COMPAQ	CQ5105LA	RUP	22779	3 Gb	AMD 7550 Dual Core 2,51 GHz 32 Bits	160 Gb	Windows	Xp	Office Enterprise 2007, kaspersky endpoint 10	USUARIO	IPv4
11	ESCRITORIO	HP COMPAQ	6200 PRO	SISTEMAS	26155	8 Gb	Core i5-2400 3.10GHz 64 Bits	500 Gb	Windows	10 Pro	Office Profesional 2010, kaspersky 10	USUARIO	IPv4 / IPv6
12	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	ETNICOS	34514	4 Gb	Intel Pentium G3450 3.40GHz 64 bits	500 Gb	Windows	10 Pro	Office Hogar y empresa 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
13	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	ASUNTOS AGRARIOS	34510	4 Gb	Intel Pentium G3450 3.40GHz 64 bits	500Gb	Windows	10 Pro	Office Hogar y empresa 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
14	ESCRITORIO	HP	dx2300	PUBLICA	18457	1 Gb	Core 2 Dúo E4500 2,2GHz 32 Bits	160 Gb	Windows	Xp	Office Profesional 2010, kaspersky 10	USUARIO	IPv4
15	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	PUBLICA	34518	4 Gb	Intel Pentium G3450 3.40GHz 64 bits	500 Gb	Windows	10 Pro	Ofiice Hogar y Empresa 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
16	ESCRITORIO	HP COMPAQ	8300 Elite AIO	PUBLICA	27641	8 Gb	Core i7 3770 3,4 GHz 64 Bits	1 Tb	Windows	10 Pro	Office Professional 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
17	ESCRITORIO	HP COMPAQ	6200 PRO	FRONTERAS	26156	6 Gb	Core i5-2400 3.10GHz 64 Bits	500 Gb	Windows	10 Pro	Office Profesional 2010, kaspersky 10	USUARIO	IPv4 / IPv6
18	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	PUBLICA	34516	4 Gb	Intel Pentium G3450 3.40GHz 64 bits	500 Gb	Windows	10 Pro	Office Hogar y Empresa 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
19	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	ATQ	34519	4 Gb	Intel Pentium G3450 3.40GHz 64 bits	500 Gb	Windows	10 Pro	Office Hogar y Empresa 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
20	ESCRITORIO	COMPAQ	CQ5105LA	ATQ	22780	2 Gb	AMD 7550 Dual Core 2,51 GHz 32 Bits	250 Gb	Windows	Xp	Office Profesional 2010, kaspersky endpoint 10	USUARIO	IPv4
21	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	ATQ	34517	4 Gb	Intel Pentium G3450 3.40GHz 64 bits	500 Gb	Windows	10 Pro	Office Hogar y Empresa 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6

22	ESCRITORIO	HP COMPAQ	8300 Elite AIO	VICTIMAS	27793	8Gb	Core i7 3770 3,4 GHz 64 Bits	1 Tb	Windows	10 Pro	Office Professional 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
23	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	VICTIMAS	34513	4 Gb	Intel Pentium G3450 3.40GHz 64 bits	500 Gb	Windows	10 Pro	Office Hogar y empresa 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
24	ESCRITORIO	COMPUMAX	A68F2P-M4	AYUDANTE DE OFICINA	36816	4Gb	AMD A4-6300 3,7Ghz 64 bits	1Tb	Windows	10 Pro	Office Profesional 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
25	ESCRITORIO	COMPUMAX	A68F2P-M4	RAJ	36815	4Gb	AMD A4-6300 3,7Ghz 64 bits	1Tb	Windows	10 Pro	Office Profesional 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
26	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	PUBLICA	34189	4 Gb	Intel Pentium G3450 3.40GHz 64 bits	500 Gb	Windows	10 Pro	Office Hogar y empresa 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
27	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	PUBLICA	34515	4 Gb	Intel Pentium G3450 3.40GHz 64 bits	500 Gb	Windows	10 Pro	Office Hogar y Empresa 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
28	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	PUBLICA	34511	4 Gb	Intel Pentium G3450 3.40GHz 64 bits	500 Gb	Windows	10 Pro	Office Hogar y Empresa 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
29	ESCRITORIO	COMPAQ	CQ5105LA	ATQ	22781	2 Gb	AMD 7550 Dual Core 2,51 GHz 32 Bits	250 Gb	Windows	Xp	Office Profesional 2010, kaspersky endpoint 10	USUARIO	IPv4
30	ESCRITORIO	LENOVO	ThinkCentre M73z AIO	DESPACHO	34187	4 Gb	Intel Pentium G3450 3.40GHz 64 bits	500 Gb	Windows	10 Pro	Office Hogar y Empresa 2013, kaspersky endpoint 10	USUARIO	IPv4 / IPv6
31	ESCRITORIO	LENOVO	10NN0006LS	ORFEO	38364	4 Gb	Core i3-7100 3.90GHz 64 bits	1 Tb	Windows	10 Pro	Office Standard 2016, Windows defender	USUARIO	IPv4 / IPv6

Fuente. Autor.

Apéndice D

Equipos de Impresión

No.	Equipo	Marca	Modelo	Dependencia	Placa	Versión IP
1	MULTIFUNCIONAL	HP	LASERJET 2727nf	PUBLICA	26237	IPv4 / IPv6
2	MULTIFUNCIONAL	HP	LASERJET 2727nf	ATQ	26238	IPv4 / IPv6
3	IMPRESORA	HP	LASERJET P3005dn	SAT	18109	IPv4 / IPv6
4	IMPRESORA	LEXMARK	E360dn	DECLARACIONES	29265	IPv4 / IPv6
5	IMPRESORA	HP	LASERJET P3015	DUPLA SICOJURIDICA(victimas)	25250	IPv4 / IPv6
6	MULTIFUNCIONAL	LEXMARK	MX511de	SECRETARIA GENERAL	34879	IPv4 / IPv6
7	IMPRESORA	SAMSUNG	PROXPRESS M4030ND	DESPACHO	36552	IPv4 / IPv6

Apéndice E

Inventario de Aplicaciones

Aplicativo	Características	Tipo	Lenguaje Programación	Responsable	Componentes	Contrato	Soporte IPv6
Visión Web	Sistema de Información Misional	Aplicación Web	PHP, MySQL, Informix	Oficina Sistemas Nivel Central	RUP, ATQ, DP, RAP, RAJ y RPG	NA	Sí
SiSAT	Sistema de Alertas Tempranas	Georreferenciación, aplicación web	Georreferenciación	Oficina Sistemas Nivel Central		NA	Sí
Correo institucional	Basado en Outlook de Microsoft	mail, share, chat	HTML5, aspx	Oficina Sistemas Nivel Central	Outlook, Yammer, Skype Empresarial, OneDrive, OneNote, Office 365	Vigente	Sí
www.defensoria.gov.co	Página Web Oficial	Externo		Oficina Sistemas Nivel Central			Sí

Apéndice F

Inventario de Equipos Servidores

Tipo de Servidor	Sistema Operativo		Direccionamiento IP	Funcionalidad	Dirección IPv4
	Nombre	Versión			
Aplicación	Linux	Red Hat 6.3	IPv4/IPv6	Eliseo - Vision Web	172.31.75.151
Base de Datos	Linux	Red Hat 6.3	IPv4/IPv6	Eliseo - Vision Web	172.31.75.146
Comunicaciones	Linux	Cent OS 7	IPv4/IPv6	Intranet – Paloma Mensajera	172.31.75.139
Aplicación	Linux	Cent OS 7	IPv4/IPv6	STRATEGOS	172.31.75.139
Aplicación	Windows	Server 2012 r2 STD	IPv4/IPv6	SiSAT	172.31.75.149
Aplicación	Linux	Cent OS 7	IPv4/IPv6	ORFEO	172.31.75.131
Base de Datos	Linux	Cent OS 7	IPv4/IPv6	ORFEO	172.31.75.136

Apéndice G

Plan de Contingencias para Servidores

Servicio	Sistema Operativo		Actividad	Procedimiento Alterno			Tiempo máximo	Objetivo de Punto de Recuperación (RPO)	Objetivo del Tiempo de Recuperación (RTO)
	Nombre	Versión		(S/N)	Nombre	Descripción			
Eliseo - Vision Web	Linux	Red Hat 6.3	Aplicación	S	Habilitar el servidor respaldo	Se tienen configurados dos servidores con la técnica de discos espejos (mirrorinng) En caso de falla por conexión: Se procede a suspender el servidor principal Se enciende servidor de respaldo Se configura la dirección IP en el servidor de respaldo Se verifica el acceso a la plataforma Se habilita el acceso a todos los usuarios	4 horas	Iniciar el procedimiento de contingencia para mitigar el impacto de no contar con el acceso a la *plataforma web* Vision Web	Disponer del sistema de información misional de la Defensoría del Pueblo, Vision Web

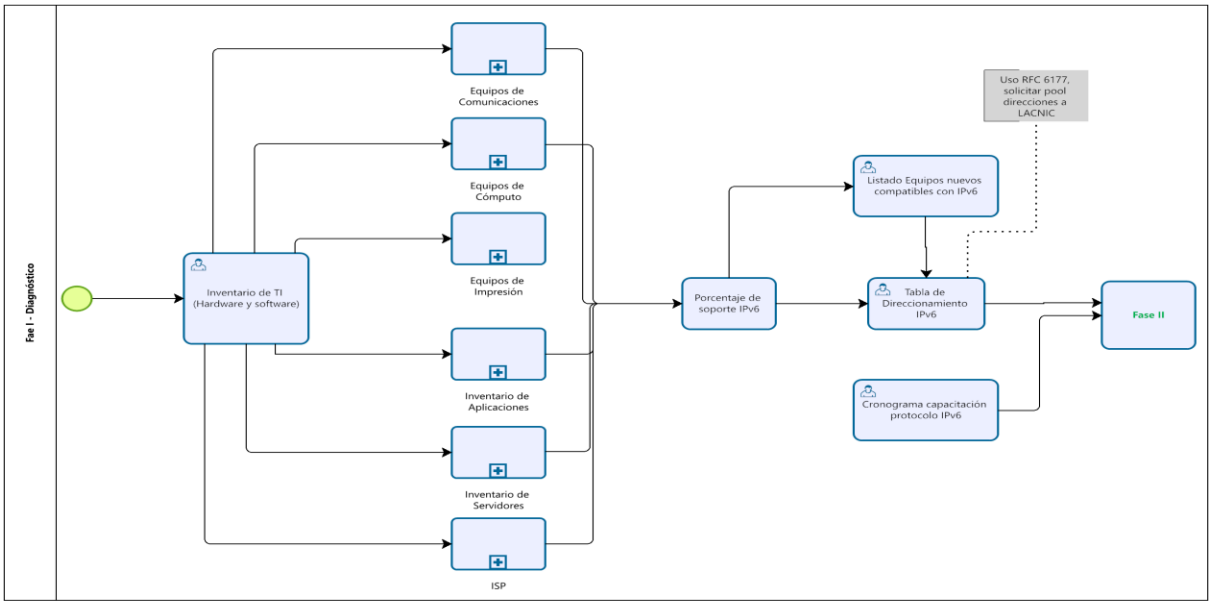
					Se configura la dirección IP temporal en el servidor principal Se realizan pruebas (test), físicas y lógicas, memoria RAM, procesadores, SO Se habilita el servidor principal			
Eliseo - Vision Web	Linux	Red Hat 6.3	Base de Datos	S	Habilitar el servidor respaldo	Se tienen configurados dos servidores con la técnica de discos espejos (mirrorinng) En caso de falla por conexión:Se procede a suspender el servidor principalSe enciende servidor de respaldoSe configura la dirección IP en el servidor de respaldoSe	4 horas	Iniciar el procedimiento de contingencia para mitigar el impacto de no contar con el acceso a la *base de datos* sistema Vision Web	Disponer del sistema de información misional de la Defensoría del Pueblo, Vision Web

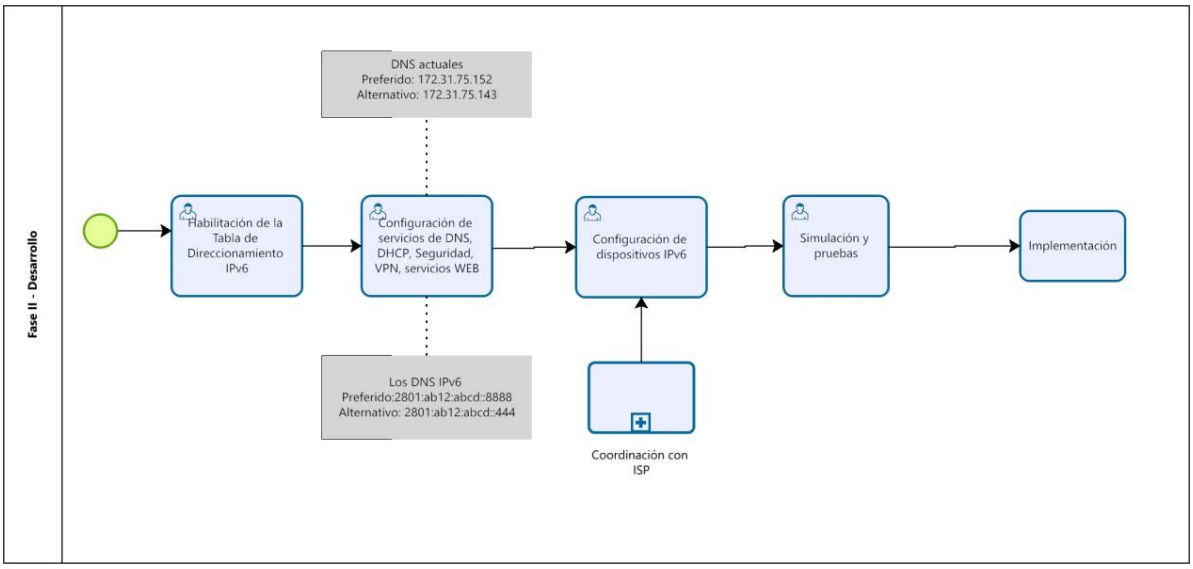
SiSAT	Windows	Server 2012 r2 STD	Aplicación y Base de Datos	S	Restaurar backup	verifica el acceso a la base de datosSe configura la dirección IP temporal en el servidor principalSe realiza un backup completo de la base de datosSe realizan pruebas (test), acceso, consultas, integridadSe habilita el servidor principal De manera preventiva, está programada para las 3 a.m. una copia de respaldo (backup) diaria de la base de datosEn caso de falla por conexión:Se procede a suspender el acceso externo al servidor SiSATSe activa el protocolo de cargue de la	6 horas	Iniciar el procedimiento de contingencia para mitigar el impacto de no contar con el acceso al *sistema de alertas temprana*	Acceder al sistema de información misional SiSAT

copia de
respaldo
más
recienteSe
realizan
pruebas
(test),
acceso,
consultas,
integridadSe
habilita el
servidor
SiSAT

Apéndice H

Prototipo Modelado

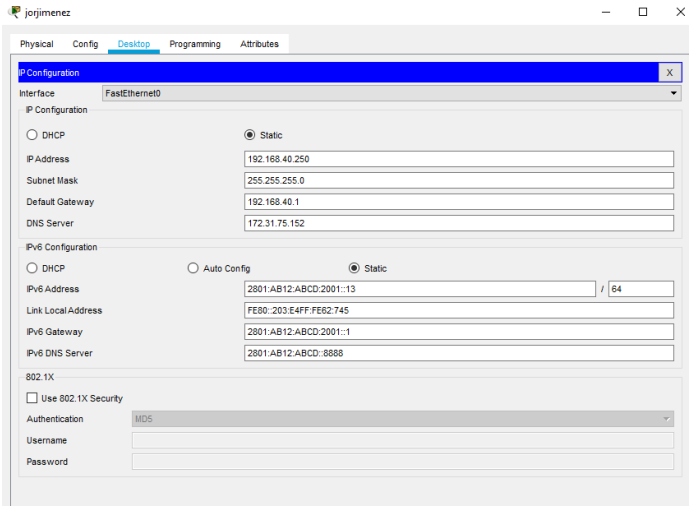




Apéndice I

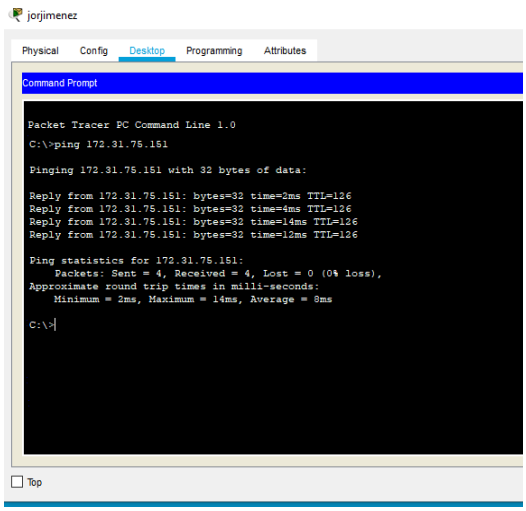
Pruebas

Prueba número uno

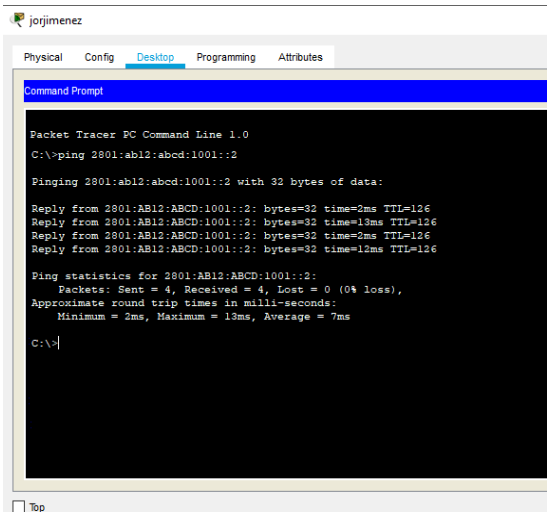


Pc “jorjimenez” configurado con IPv4 e IPv6 estática en un puerto LAN

Ping IPv4



Ping IPv6

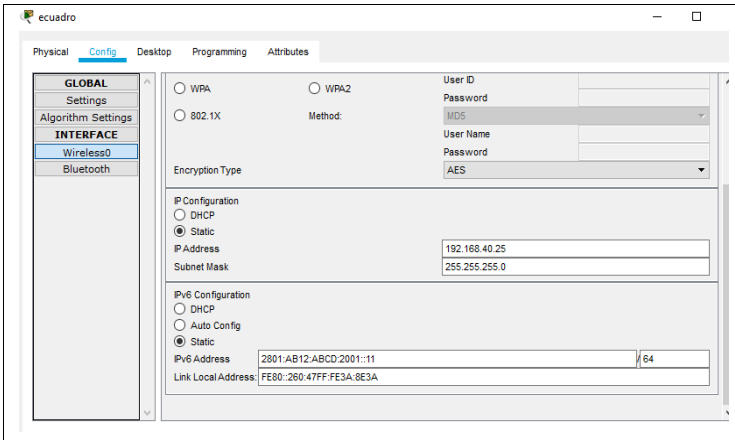


La prueba de “ping” indica que existe comunicación entre el Pc y el servidor VisionWeb tanto en IPv4 como en IPv6, es decir, que la configuración realizada a cada uno de los routers funciona como “doble pila” de manera correcta. Lo anterior, garantiza la coexistencia de ambos protocolos de comunicación y la transición “suave” requerida en la implementación.

Dirección servidor [VisionWeb] en IPv4 → 172.31.75.151

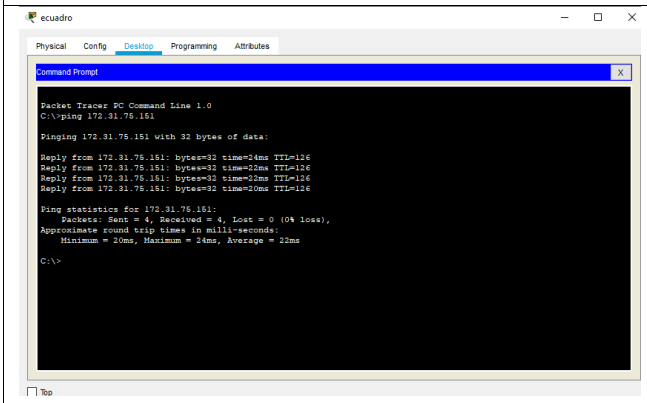
Dirección servidor [VisionWeb] en IPv6 → 2801:ab12:abcd:1001::2

Prueba número dos

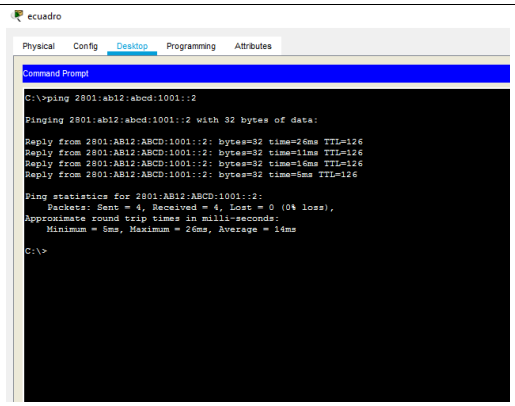


Laptop “ecuadro” configurado con IPv4 e IPv6 en un puerto WLAN

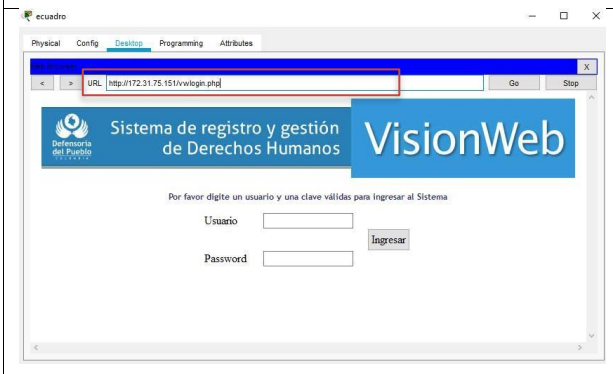
Ping IPv4



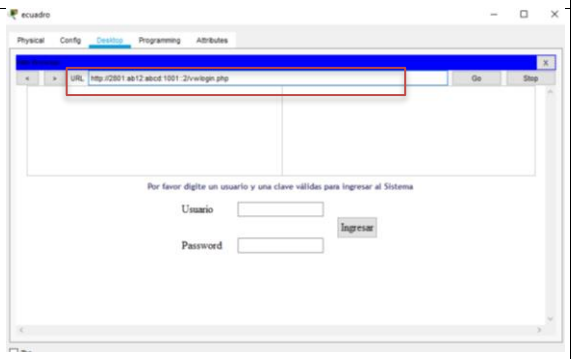
Ping IPv6



Acceso al sistema misional Vision Web con IPv4

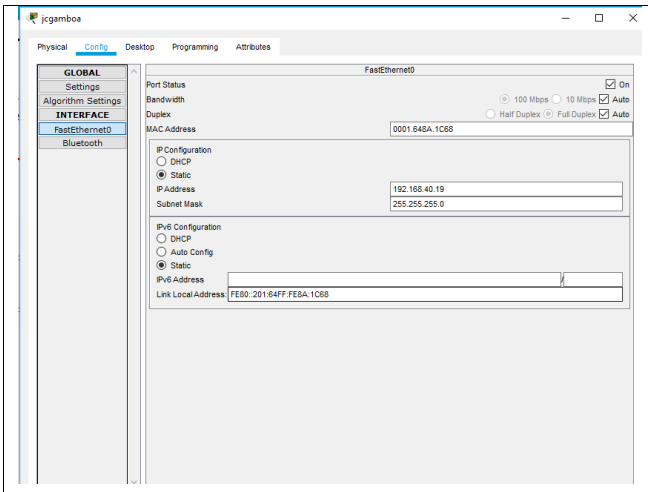


Acceso al sistema misional Vision Web con IPv6



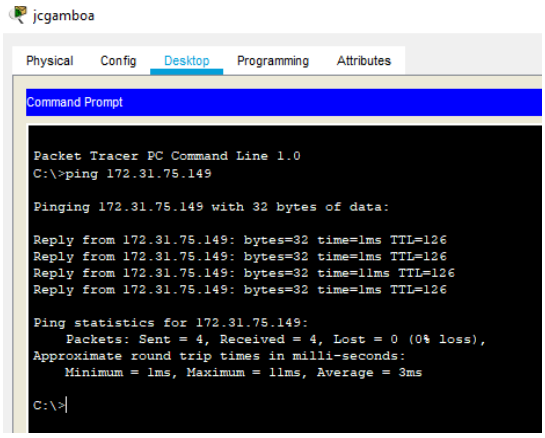
De igual manera que con el Pc de “jorjimenez”, la conexión inalámbrica desde el equipo portátil de “ecuadro” se realiza de forma exitosa.

Prueba número tres

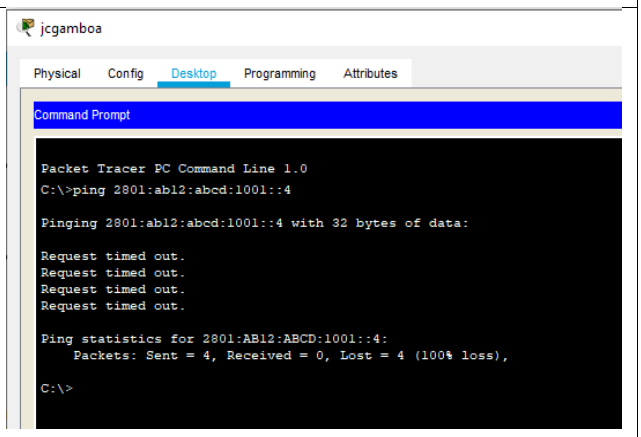


Pc “jcgamboa” configurado únicamente con una dirección IPv4 estática en un puerto LAN

Ping IPv4



Ping IPv6



La prueba de “ping” indica que existe comunicación entre el Pc y el servidor SiSAT utilizando únicamente la dirección IPv4 asignada, es decir, que la configuración realizada a cada uno de los routers funciona como “doble pila” de manera correcta.

La prueba de “ping” al servidor del aplicativo misional SiSAT, con dirección IPv6 2801:ab12:abcd:1001:0:0:0:4 resulta fallida, pues este Pc no tiene la configuración requerida para dicho acceso mediante el uso de IPv6.

Apéndice J

Configuración aplicada a los nodos de la red

Configuración router Nodo Cesar	**Configuración router Nodo Central**
interface FastEthernet0/0	interface FastEthernet0/0
ip address 192.168.40.1 255.255.255.0	ip address 172.31.75.1 255.255.255.0
ipv6 address 2801:AB12:ABCD:2001::1/52	ipv6 address 2801:AB12:ABCD:1001::1/52
no shu !activar el puerto	no shu !activar el puerto
!PUERTO SERIE COMUNICAR NodoCentral	!PUERTO SERIE COMUNICAR NodoCesar
interface Serial0/1/0	interface Serial0/1/0
ip address 192.168.3.1 255.255.255.0	ip address 192.168.3.2 255.255.255.0
ipv6 address 2801:AB12:ABCD:3000::1/52	ipv6 address 2801:AB12:ABCD:3000::2/52
no shu !activar el puerto	no shu !activar el puerto
ipv6 unicast-routing	ipv6 unicast-routing
Configurar la tabla de enrutamiento	Configurar la tabla de enrutamiento
!IPv4	!IPv4
ip route 172.31.75.0 255.255.255.0 192.168.3.2	ip route 192.168.40.0 255.255.255.0 192.168.3.1
!IPv6	!IPv6
ipv6 route ::/0 2801:AB12:ABCD:3000::2	ipv6 route ::/0 2801:AB12:ABCD:3000::1