CONSTRUCCIÓN DE ENTORNO DE PRUEBAS PARA LA EVALUACIÓN DE SERVICIOS DE RED CORPORATIVOS EN AMBIENTE BASADO EN EL MODELO DEL MINTIC PARA LA ADOPCIÓN DEL PROTOCOLO IPV6 EN COLOMBIA

VICTOR MADERA MARTÍNEZ

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MEDELLÍN

2020

CONSTRUCCIÓN DE ENTORNO DE PRUEBAS PARA LA EVALUACIÓN DE SERVICIOS DE RED CORPORATIVOS EN AMBIENTE BASADO EN EL MODELO DEL MINTIC PARA LA ADOPCIÓN DEL PROTOCOLO IPV6 EN COLOMBIA

VICTOR MADERA MARTINEZ

Trabajo de grado para optar al título de Magister en Tecnologías de la Información y la Comunicación

Asesor

CLAUDIA CARMONA RODRÍGUEZ

Magister en Ingeniería de Telecomunicaciones

UNIVERSIDAD PONTIFICIA BOLIVARIANA

ESCUELA INGENIERÍAS

FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

MEDELLÍN

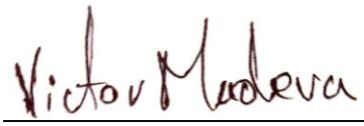
2020

2 de marzo de 2021

Víctor Hugo Madera Martínez

Declaro que este trabajo de grado no ha sido presentado con anterioridad para optar a un título, ya sea en igual forma o con variaciones, en ésta o en cualquiera otra universidad". Art. 92, parágrafo, Régimen Estudiantil de Formación Avanzada.

Firma del autor (es)



CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

GLOSARIO

DHCP Relay: Proceso mediante el cual un agente retransmite una solicitud DHCP proveniente de un cliente a un servidor DHCP que se encuentra en una subred diferente a la del cliente

DOM: Sigla para **D**ocument **O**bject **M**odel, estructura de objetos que genera el navegador cuando se carga un documento

DORA: Abreviatura para las etapas del proceso DHCP en IPv4 (**D**iscovery, **O**ffer, **R**equest, **A**ck)

IMAP: Sigla para **I**nternet **M**essage **A**ccess **P**rotocol, protocolo de aplicación que permite el acceso a mensajes almacenados en un servidor de Internet.

Kerberos: Protocolo de autenticación de redes usado por el servicio de directorio activo.

NSLOOKUP: Comando utilizado en la interfaz de línea de comandos para obtener información del servidor DNS.

RFC: Sigla para **R**equest **F**or **C**omments, memorando publicado por el Grupo de trabajo de ingeniería de Internet (IETF) que describe métodos, comportamientos, investigaciones o innovaciones aplicables al funcionamiento de Internet.

SARR: Abreviatura para las etapas del proceso DHCP en IPv6 (**S**olicit, **A**dvertise, **R**equest, **R**eply)

Script: Serie de instrucciones que se almacenan dentro de un archivo de texto generalmente pequeño que se ejecutan por medio de un intérprete en tiempo real.

SMTP: Sigla de **S**imple **M**ail **T**ransfer **P**rotocol, protocolo de red utilizado para el intercambio de mensajes de correo electrónico.

Ticket Kerberos: Elemento que posee un conjunto de información electrónica y que se utiliza para identificar a un usuario o servicio en el protocolo Kerberos.

RESUMEN

Este trabajo detalla la construcción de un entorno de pruebas para servicios de red de carácter corporativo acorde a los lineamientos de adopción del protocolo IPV6 en Colombia dados por el MINTIC. En el documento, Guía de Transición de IPv4 a IPv6 para Colombia, publicado por el MINTIC se hace referencia a algunos servicios que las empresas deben revisar, la operatividad y el rendimiento de dichos servicios bajo el modelo de transición propuesto son parámetros que deben ser medidos para identificar el comportamiento de los mismos en este nuevo escenario, ya que dichos servicios impactan directamente en la experiencia de usuario, en este trabajo se evaluará el rendimiento de algunos de estos servicios bajo un ambiente controlado con las características sugeridas por el Ministerio. En primer lugar, se realizará el diseño del entorno de pruebas, allí se hará la selección de aplicaciones que presten dichos servicios corporativos con sus respectivos protocolos de pruebas, posterior a ello se realizará la implementación y el afinamiento del entorno de pruebas con base en el diseño propuesto, por último, se harán las pruebas de funcionalidad y rendimiento. En las pruebas de rendimiento se utilizan herramientas que permiten generar el tráfico típico de los servicios evaluados desde las estaciones cliente hacía los servidores que alojan los diferentes servicios, dicho tráfico es capturado por la misma herramienta u otra específica para poder obtener las métricas de rendimiento deseados con el fin de comparar el desempeño de los servicios en los diferentes entornos. De acuerdo con los resultados obtenidos, en los cuales el rendimiento en los ambientes doble pila e IPv6 puro es similar o ligeramente superior al ambiente IPv4 puro, podemos concluir que la transición al modelo doble pila y a futuro a un modelo sólo IPv6 no implicará una degradación en el rendimiento comparado con lo que hoy experimenta un usuario en un ambiente netamente IPv4 en una red LAN.

.

PALABRAS CLAVE: servicios de red; IPV6; transición; doble pila; entorno de pruebas.

ABSTRACT

This work details the construction of a test environment for corporate network services according to the guidelines for the adoption of the IPV6 protocol in Colombia given by the MINTIC. In the document, Transition Guide from IPv4 to IPv6 for Colombia, published by the MINTIC, reference is made to some services that companies must review, the operability and performance of these services under the proposed transition model are parameters that must be measured in order to identify their behavior in this new scenario, since these services directly impact the user experience, in this work the performance of some of these services will be evaluated under a controlled environment with the characteristics suggested by the ministry . In the first place, the design of the test environment will be carried out, there will be the selection of applications that provide said corporate services with their respective test protocols, after which the implementation and fine-tuning of the test environment will be carried out based on the proposed design. Finally, the proposed design will be tested for functionality and performance. In the performance tests, tools are used that allow generating the typical traffic of the evaluated services from the client stations to the servers that host the different services, said traffic is captured by the same tool or another specific one in order to obtain the desired performance metrics to compare the performance of services in different environments. According to the results obtained, in which the performance in the dual stack and pure IPv6 environments is similar or slightly higher than the pure IPv4 environment, we can conclude that the transition to the double-stack model and in the future to an only IPv6 model will not imply a degradation in performance compared to what a user experiences today in a purely IPv4 environment on a LAN Network.

KEY WORDS: networking services; IPv6; transition; dual stack; test environment.

1 INTRODUCCIÓN

El Estado colombiano, en cabeza del MINTIC, con miras a acelerar el proceso de transición al protocolo IPv6 en Colombia, expidió la Resolución 2710 de 2017[1], en la que se dictan plazos a las entidades gubernamentales para la implementación de la tecnología IPv6 y demanda la utilización del documento Guía de Transición de IPV4 a IPV6 para Colombia [2] como referencia, allí se dispone que existen unos servicios generales tales como DNS, DHCP, Directorio Activo, Servicios WEB, correo electrónico, servicio WiFi, entre otros, a las cuales las entidades deben apuntar a planear, revisar y configurar en el marco del proceso de transición. El objeto de este trabajo es construir un entorno de pruebas acorde a las disposiciones del Ministerio donde se pueda evaluar la compatibilidad y el rendimiento de dichos servicios bajo tres escenarios; red sólo IPv4, red sólo IPv6 y doble pila.

La presentación del proyecto está dividida en capítulos, en los capítulos 2, 3 y 4 se muestra el planteamiento del problema, los objetivos y el marco referencial del proyecto. El capítulo 5 presenta la metodología utilizada y el capítulo 6 muestra los resultados obtenidos en cada fase del proyecto, planeación, ejecución y pruebas, finalizando con su correspondiente análisis. Por último, en el capítulo 7 se muestran las conclusiones del trabajo realizado y en el capítulo 8 los posibles trabajos futuros que se pueden desarrollar a partir de este proyecto.

2 PLANTEAMIENTO DEL PROBLEMA

2.1 Problema

El agotamiento de las direcciones IPv4 es una situación inminente y, por ende, la transición al protocolo IPv6 cada vez más necesaria [3][4]. En 2011, la IANA, entidad encargada de asignar las direcciones IP a nivel mundial, anunció que había entregado todos los bloques de direcciones disponibles a los diferentes Registros Regionales, en adelante RIR, los cuales están en fases de agotamiento[5]. El LACNIC, registro regional de internet para América Latina y el Caribe, el cual incluye a Colombia, está desde febrero de 2017 en la última fase del proceso de agotamiento.

Colombia actualmente cuenta con un índice de penetración de IPv6 menor al 12% según mediciones de Google, lo cual está muy por debajo de los líderes en la región como lo son Brasil y Uruguay y al promedio mundial, que están con índices superiores al 30% [6]. Con miras al proceso de transición de IPv4 a IPV6, el gobierno Nacional de Colombia, en cabeza del Ministerio de tecnologías de la información y las comunicaciones, en adelante MINTIC, expidió la Resolución 2710 de 2017 donde se dan una serie de lineamientos con miras a formalizar el proceso de adopción del protocolo IPv6 en el país [1]. En dicha resolución se dictan plazos a las entidades gubernamentales para la implementación de la tecnología IPv6, de la misma forma demanda la utilización de los documentos Guía de Transición de IPV4 a IPV6 para Colombia y Guía para el Aseguramiento del Protocolo IPV6 como referencia en el proceso de transición [1] .

El proceso de transición hacía el protocolo IPv6 genera cierta resistencia en las organizaciones, una de ellas está relacionada con las garantías de la compatibilidad de una infraestructura de servicios funcional en IPv4 con el protocolo IPv6 [7], servicios como DNS, DHCP, correo electrónico, servidores WEB, comunicación WiFi, entre otros, hacen parte de los servicios corporativos típicos existentes en las organizaciones y por ende son objeto de revisión en un escenario de transición a IPv6. Por otro lado, la estabilidad actual de la infraestructura bajo el protocolo IPv4 hace cuestionar la necesidad real de migrarse a IPv6 en muchas compañías [4].

Según el portal de LACNIC, las empresas involucradas en el proceso de migración a IPv6 en el país son en su mayoría del sector de los proveedores de servicios de internet y las universidades [8], dado el panorama actual de agotamiento IPv4, es conveniente que una mayor cantidad de organizaciones de todos los sectores, tanto de carácter público como privado, inicien sus procesos de migración.

La incertidumbre ante el proceso de adopción puede provocar dos situaciones particulares, la ejecución de un proceso de transición carente de buenas prácticas o la permanencia de

la organización en el protocolo IPv4 y en consecuencia un retraso de la transición a IPv6. En el primer escenario, nos podemos encontrar con aspectos tales como la dilatación del proceso de adopción, lo cual implica un redimensionamiento de recursos y por ende gastos extras, o problemas de compatibilidad de aplicaciones bajo el nuevo entorno por la errónea ejecución de protocolos de pruebas. Mientras tanto, en el segundo escenario, nos encontramos con situaciones como el desaprovechamiento de las capacidades de IPv6 , el incumplimiento de las directivas del ministerio, lo cual podría dar lugar a sanciones a las entidades públicas [1], o la adopción acelerada de IPv6 en el momento que la necesidad ya sea imperiosa.

2.2 Justificación

Este proyecto plantea la construcción de un entorno de pruebas basado en los lineamientos dados por el MINTIC para llevar a cabo el proceso de transición hacía IPV6 en Colombia, entendiendo entorno de pruebas como una instancia específica de una configuración con el propósito de realizar pruebas bajo condiciones controladas y conocidas[9].

La construcción y posterior evaluación del entorno de pruebas, con miras a reducir el nivel de incertidumbre en el proceso de transición, permitirá determinar si la infraestructura de red diseñada e implementada con el software y los equipos específicos para soportar los servicios analizados, son adecuados y en qué condiciones para realizar una transición al protocolo IPv6 según los lineamientos del MINTIC. Se hará especial énfasis en analizar el comportamiento de los servicios elegidos en entornos sólo IPv4, sólo IPv6 y doble pila, con el fin de comparar la experiencia que obtiene el usuario utilizando dichos servicios en los diferentes escenarios

Los servicios evaluados en este proyecto serán: DNS, DHCP, directorio activo, correo electrónico, servicio web, WiFi, estos son de gran importancia para garantizar la conectividad en una empresa, el servicio DHCP permite a los equipos cliente obtener automáticamente una dirección IP sin intervención directa del usuario final, el servicio DNS controla la traducción de nombres en direcciones IPs, el servicio de directorio activo permite gestionar las identidades de los usuarios y equipos, el servicio de correo electrónico es fundamental para la comunicación corporativa, el servicio WEB permite el funcionamiento y acceso a portales informativos, intranet u otras aplicaciones basadas en este protocolo, por su parte el servicio WiFi garantiza la conectividad de los diferentes dispositivos de forma inalámbrica. La operatividad y el rendimiento de todos los servicios antes descritos impactan en la experiencia de los usuarios conectados a una red corporativa.

La temprana adopción del protocolo IPv6 por parte de empresas, ya sean del sector público o privado, les evitará el problema actual y cada vez más evidente del agotamiento del espacio de direcciones IPv4. Los beneficiarios de este trabajo serán las diferentes entidades de carácter público, los organismos encargados de proveer servicios del programa gobierno en línea, y entidades de carácter privado que deseen adoptar el modelo propuesto.

3 OBJETIVOS

3.1 Objetivo General.

Construir un entorno de pruebas para la evaluación de la compatibilidad y el rendimiento de servicios corporativos específicos con en el modelo propuesto por el MINTIC para la adopción del protocolo IPV6 en Colombia.

3.2 Objetivos Específicos

- Diseñar el entorno de pruebas adaptado a los requerimientos del ministerio y de los servicios seleccionados.
- Realizar la instalación y configuración de la solución diseñada en infraestructura de pruebas.
- Realizar pruebas de compatibilidad y rendimiento de servicios seleccionados en IPv6 bajo el esquema doble pila.

4 MARCO REFERENCIAL

4.1 Marco contextual

Las direcciones IPv4 disponibles a nivel global se están agotando, la IANA, encargada de la coordinación a nivel mundial de los bloques de direccionamiento IPv4 informó que, en el año 2011, el bloque central de direcciones IPv4 se había agotado. Luego, cada uno de los RIR entraron en diferentes fases de agotamiento de las direcciones IPv4 que aún tienen o tenían disponibles.

El RIR LACNIC, organismo encargado de la asignación y administración de los recursos de direccionamiento, tanto en IPv4 como en IPv6 para la parte de América Latina y el Caribe, informa que en el mes de febrero de 2017 inició su tercera etapa de agotamiento. El 19 de Agosto de 2020, LACNIC informó que agotó su pool de direcciones IPv4, sólo quedan disponibles recursos recuperados y devueltos, los cuales pasan por un periodo de cuarentena de 6 meses antes de ser liberados, y una reserva destinada exclusivamente a infraestructura crítica [10].

Existen diferentes entidades que se encargan de medir el índice de penetración del protocolo IPv6 en los diferentes países, organizaciones como Google [6], y APNIC [11], sitúan a Colombia con un índice de penetración de IPv6 por debajo del 12%.

El Estado colombiano, en cabeza del MINTIC lanzó en el año 2017 la resolución 2710, en la cual se dictan una serie de lineamientos a seguir en el proceso de adopción de IPv6 en Colombia. Entre los aspectos más importantes de la resolución está que las entidades del Estado de orden nacional deberán implementar la tecnología IPv6, en coexistencia con el IPv4 a más tardar el 31 de diciembre del 2019. Para entes territoriales, el plazo dado es el 31 de diciembre del 2020. Para cumplir con lo anteriormente dispuesto, el MINTIC ha puesto a disposición de las entidades, dos documentos de apoyo titulados: Guía de Transición de IPV4 a IPV6 para Colombia [2] y Guía para el Aseguramiento del Protocolo IPV6 [1].

4.2 Marco conceptual

IPv4 es la cuarta versión en el desarrollo del protocolo IP, y actualmente la mayoría de redes de datos están operando bajo este protocolo [12]. Para establecer la comunicación entre nodos, IPv4 utiliza un direccionamiento de 32 bits, los cuales son representados por cuatro cifras decimales separadas por puntos, cada cifra representa por tanto 8 bits. Bajo este esquema, IPv4 proporciona aproximadamente 4,3 mil millones de direcciones, en el momento del diseño del protocolo y no contando con la expansión exponencial que ha tenido internet, esta cantidad de direcciones se creyó suficiente, pero la realidad muestra que las direcciones IPv4 están hace ya varios años en fases de agotamiento [5].

Para prevenir el agotamiento IPv4 se han desarrollado diferentes estrategias como el enrutamiento Inter dominio sin clase CIDR y la traducción de direcciones de red NAT [13]. NAT es un protocolo que permite conectar a internet varios dispositivos con IPs privadas, no enrutables en internet, a través de una única dirección IP pública, de esta manera se optimiza el recurso limitado de IPs públicas [13][14].

Recientemente, se han implementado otras estrategias que persiguen el objetivo común de prevenir el agotamiento IPv4, dentro de ellas destacan el NAT a gran escala o CGN, el cual consiste en conectar a través de una misma IP varios nodos independientes y dispares, este actúa como una técnica segundo nivel al ya mencionado NAT [15]. Otra opción de carácter administrativo que se ha estudiado es la posibilidad de recuperar, transferir o vender aquellos bloques de direcciones que ya han sido asignados bien sea porque nunca se han utilizado o porque ya se liberaron [4] .

Las anteriores medidas buscan optimizar la utilización del direccionamiento IPv4 y prevenir así la escasez del recurso. Ante el crecimiento acelerado de internet, Las autoridades respectivas previeron hace ya varios años que esto podría ocurrir, de tal manera que desarrollaron una nueva versión del protocolo IP, el cual serviría de sucesor de IPv4 y lo llamaron IPv6 [16]. El nuevo protocolo extiende las capacidades de direccionamiento, pasando de una dirección IP de 32 bits en IPv4 a una de 128 bits en IPv6, de esta manera se pasa de tener 2^{32} direcciones IP en IPv4 a 2^{128} direcciones IP en IPv6, es decir, alrededor de 340 sextillones de direcciones [17]. Dado el amplio número de direcciones, el uso de NAT no es necesario en IPv6 ya que cada host deberá tener su propia IP, con lo que se garantiza una conexión de extremo a extremo.

Otros cambios introducidos por la nueva versión fueron la simplificación del formato del encabezado, en la que unos campos del encabezado IPv4 se suprimieron o se dejaron como opcionales, con el objetivo de disminuir el costo del procesamiento de paquete y para optimizar el tema del ancho de banda; el soporte reformado de extensiones y opciones, los cuales van orientados a un reenvío más efectivo modificando la forma de codificación de las opciones en el encabezado, flexibilidad para la longitud de las opciones y para admitir la posibilidad de introducción de otras opciones adicionales en años venideros. La

capacidad de etiquetado de flujo es otra característica que se adiciona para permitir marcar un tipo específico de paquete y de esta manera manejar calidad de servicio para aplicaciones que así lo requieran [16].

La arquitectura de direccionamiento IPv6 está definida por la IETF en la RFC 4291, estas direcciones de 128 bits se representan dividiéndolas en 8 grupos y cada grupo en números hexadecimales de 4 dígitos separados por el símbolo de dos puntos [18]. La anterior notación, permite que una misma dirección IPv6 pueda ser escrita de múltiples maneras, por tal razón la IETF en la RFC 5952 define un formato canónico de representación textual de las direcciones IPv6, esto con el fin de evitar problemas o confusiones a ingenieros y demás usuarios del protocolo [19].

El protocolo IPv6 define tres tipos de direcciones: unicast, este tipo de direcciones cuenta con una dirección por interfaz, cuando un paquete es enviado a una dirección de este tipo, este simplemente es reenviado a la interfaz de red que está registrada con esa dirección; multicast, en este tipo de direcciones se usa una dirección para un grupo de interfaces de distintos nodos normalmente, cuando un paquete es enviado a direcciones de este tipo, este es transmitido a todas las interfaces de red que estén registradas con esa IP en específico; y anycast, en la cual un identificador es para un grupo de interfaces de red típicamente perteneciente a distintos nodos, cuando un paquete se envía a una dirección de este tipo, el paquete se entrega a la interfaz más cercana, según la medida de distancia dada por los protocolos de enrutamiento, identificado por esa dirección. Los dos primeros tipos ya existían en IPv4, mientras que anycast es un nuevo tipo de dirección definida en IPv6. A diferencia de IPv4, las direcciones de broadcast desaparecen en IPv6, las direcciones multicast asumen esta función. Los prefijos y su representación textual en direcciones IPv6 son similares a la forma en que los prefijos de las direcciones IPv4 están escritos en notación CIDR [18].

Las direcciones unicast IPv6 según su ámbito de operación pueden ser globales, de enlace local o ULA (Unique Local Address), las direcciones globales son las que se pueden enrutar en internet, es decir, el equivalente de las direcciones públicas en IPv4, las direcciones ULA operan dentro de un ámbito local a la organización y no deben ser enrutadas en internet, su uso es similar al que se le da a las direcciones privadas en IPv4, por último, las direcciones de enlace local son usadas para la conexión dentro de una misma LAN, no son enrutables [20][18].

Servicios de red presentes en entornos corporativos como DNS y DHCP existentes en IPv4, son redefinidos en IPv6, entendiendo servicio de red como una composición de funciones que facilitan una operación en la red. El servicio de nombres de dominio DNS es utilizado para realizar un mapeo entre nombres de host y direcciones IP, de esta manera, un usuario no se deberá aprender una dirección de 24 bits sino un nombre que le es más familiar. El servicio de configuración dinámica de host DHCP permite asignar una configuración de direccionamiento de manera automática a los dispositivos que se conectan a una red en particular [21], de esta manera el direccionamiento lo recibe el host de manera automática

sin necesidad de intervenciones manuales del usuario. Los protocolos antes mencionados persisten en IPv6 con sus respectivas adaptaciones.

En redes IPv4, DNS utiliza los registros A para asociar este tipo de direcciones con un nombre específico. En IPv6 se define la creación del tipo de registro AAAA para almacenar una dirección IPv6, de esta manera, una dirección IPv6 de 128 bits está codificada en la porción de datos de un registro de recursos AAAA [22]. En IPv6 el proceso de configuración automática de direccionamiento se puede dar de varias maneras, dependiendo si los parámetros se obtendrán a través de un mecanismo sin estado, un mecanismo con estado, o ambos [23]. En el mecanismo sin estado, abreviado SLAAC, cada host genera sus propias direcciones usando una combinación de información de su propia interfaz e información anunciada por los dispositivos encargados de realizar el enrutamiento, en ausencia de dichos dispositivos, un host solo puede generar direcciones de enlace local, sin embargo, éstas permiten que nodos que hacen parte del mismo enlace obtengan comunicación [23]. El mecanismo con estado es un esquema cliente/servidor donde el servidor entrega la información de direccionamiento e información adicional al host para su configuración, este mecanismo es conocido como DHCPv6 [24]. En un esquema mixto, un host puede hacer uso del mecanismo SLAAC para configurar su propio direccionamiento, pero usar DHCPv6 para conseguir otra información.

Además de los ya previamente mencionados, otro de los servicios importantes en un entorno de red corporativo es el servicio de directorio activo, este se encarga de proveer un repositorio central de información de todos los recursos de una organización existentes en la red, como empleados, grupos, dispositivos, impresoras, programas y documentos de tal manera que los administradores del directorio activo pueden gestionar eficientemente la información de la empresa, permitiéndole ejecutar acciones como agregar usuarios, establecer políticas de red, controlar la autenticación, entre otros [25]. Los tres servicios descritos anteriormente junto con los servicios de correo electrónico, WEB y WiFi, ampliamente conocidos, son los que se evaluarán en este trabajo en el entorno propuesto por el MINTIC.

Una de las dificultades de la transición de IPv4 a IPv6 es que los protocolos no son compatibles entre sí por las diferencias de su encabezado, es por ello que se debe implementar un mecanismo con el que sea posible una transición que permita la coexistencia de ambos protocolos y que las aplicaciones continúen funcionando mientras se actualiza la red [26].

Diferentes técnicas de transición son usadas para hacer posible la comunicación entre IPv4 e IPv6, dichas técnicas se pueden clasificar en tres grandes grupos de acuerdo a su forma de hacer la transición: Túneles, Doble Pila y Traducción de protocolos [26] [3].

El mecanismo doble pila está diseñado para que los equipos de la red soporten ambos protocolos IPv4 e IPv6, en este entorno se necesita que cada equipo disponga de al menos una dirección por cada protocolo, lo que implica que dicho mecanismo no resuelve el

problema de la escasez de direcciones IPv4 [27], pero si permite que se pueda evolucionar de forma gradual de una red dominante IPv4, pasando por una red dual IPv4/IPv6 para llegar finalmente a una red dominante o exclusiva IPv6 [12].

En el entorno doble pila, cuando se genera una conexión hacia un host que sólo permite IPv4, se utilizará el protocolo específico, al igual si la conexión es hacia un host que sólo permita IPv6. En el caso de que el host remoto admita tanto IPv4 como IPv6, se priorizará la conexión a través de IPv6 y en caso de que ésta no cumpla ciertos parámetros se realizará la conexión a través de IPv4 [28], para ello se ha desarrollado el algoritmo Happy Eyeballs, el cual calcula un tiempo para establecer la conexión TCP a través de IPv6, si en ese tiempo específico la conexión no es establecida, se intentará una nueva conexión a través del protocolo IPv4 [29]. La técnica de doble pila es la sugerida por el gobierno nacional en cabeza del MINTIC para hacer la transición [2].

En la mayoría de los escenarios de implementación, la infraestructura de enrutamiento IPv6 se construirá a lo largo del tiempo. Se espera que el mecanismo doble pila se complemente con el mecanismo de túneles en las primeras etapas de la transición, mientras aumenta la cantidad de dispositivos que utilizan el mecanismo doble pila, los túneles encapsulan paquetes IPv6 dentro de paquetes IPv4 con lo que permiten que dos redes IPv6 aisladas se comuniquen sin necesidad de que haya conectividad IPv6 entre ellos. En las últimas etapas de la transición, cuando se espera que IPv4 se apague gradualmente, se espera que IPv4 se encapsule dentro de un túnel IPv6 hasta que finalmente ya no fuera necesario [30].

En líneas generales, en los mecanismos tipo túnel, los paquetes son transmitidos hasta cierto nodo haciendo uso del protocolo con el que fueron generados, más allá de ese nodo, la red no soporta el protocolo inicial por lo que los paquetes son encapsulados para poder ser transportados en la parte de red que no admite dicho protocolo, finalmente, al llegar al nodo de la red que nuevamente soporta el protocolo inicial, se retira el encabezado y se envía al destino final en forma nativa [31]. Existen diferentes técnicas de transición basadas en la arquitectura de túneles, ISATAP, 6to4, 6RD, GRE, son algunos de los mecanismos más comunes, la selección de uno en especial dependerá de los requerimientos de cada proyecto de transición [26].

La técnica de traducción de protocolos se basa en convertir un paquete IPv4 en un paquete IPv6 y viceversa haciendo uso de algún equipo, generalmente un enrutador, que sea capaz de cumplir con ambas funciones [32]. La clave del mecanismo está en la conversión del encabezado, similar al NAT usado en IPv4 en el cual se realiza la traducción entre direcciones públicas y privadas, aquí lo que se busca es realizar la traducción entre un encabezado IPv4 y uno IPv6 [26]. El mecanismo de traducción de protocolos implica un nivel alto de procesamiento en la red, toda vez que el dispositivo encargado de hacer la traducción deberá remover el encabezado IPv4 y colocar un nuevo encabezado IPv6 o viceversa según sea el caso. Este mecanismo es especialmente útil cuando la mayoría de la internet se haya movido a IPv6, pero algunos sistemas todavía utilicen IPv4. El remitente

desea usar IPv6, pero el receptor no comprende IPv6, por lo que necesitará un dispositivo capaz de realizar la traducción [3].

4.3 Marco legal

El proceso de adopción del protocolo IPv6 en Colombia está reglamentado en la resolución 2710 de 2017, ésta sólo afecta a las entidades de carácter público y entre otras cosas se les obliga a culminar el proceso de transición a más tardar el 31 de diciembre de 2019 para las entidades nacionales y a las de carácter territorial a más tardar el 31 de diciembre 2020. Dicha resolución también exige a los ISPs preparar sus troncales de acceso a internet para permitir el enrutamiento de los prefijos IPv6 nativos de las diferentes entidades que efectúen la adopción [1].

Durante el proyecto se hará uso de diferentes tipos de aplicaciones, el uso de software legal para Colombia está reglamentado en la ley 603 de 2000, en la cual se obliga a las empresas a presentar un informe de gestión donde se debe resaltar el tipo de software que se usa y su respectivo licenciamiento con el fin de proteger la propiedad intelectual y prevenir el incremento de la piratería [33].

4.4 Estado del arte

El mundo se está quedando sin direcciones IPv4, particularmente LACNIC, el RIR que cobija a Latinoamérica y por ende Colombia anunció el agotamiento de sus direcciones IPv4 en agosto de 2020 [10]. En busca de prevenir el agotamiento IPv4, históricamente se han desarrollado técnicas como NAT y CIDR. Actualmente, el NAT a gran escala o CGN se viene utilizando para optimizar aún más el espacio de direcciones IPv4, esta técnica permite compartir una IP pública entre varios terminales lo que conlleva a vacíos en temas como listas negras basadas en IP, reputación de direcciones, análisis del uso de la web, fallas en aplicaciones VoIP, entre otros. Otra técnica que ha emergido para evitar el agotamiento IPv4 son los llamados mercados de transferencia, donde direcciones IPv4 previamente asignadas son revendidas en el mercado, sin embargo, [34] y [30] coinciden en que los ISPs prefieren optar por técnicas como CGN antes de acudir a este tipo de operaciones.

Por otro lado, como respuesta definitiva al agotamiento de direcciones, la IETF específica el protocolo IPv6 como sucesor de IPv4, en el cual se amplía el tamaño de una dirección IP de 32 bits a 128 bits, pasando a un universo de 340 sextillones de direcciones [16]. Las estadísticas muestran que el despliegue de IPv6 ha ido creciendo ininterrumpidamente situándose el porcentaje de adopción a Abril de 2020 para el mundo, Suramérica y Colombia en valores por encima del 25%, 20% y 5% respectivamente [6], [11], de hecho [34] muestra que aunque el uso de CGN es popular entre los ISPs, esto no parece estar afectando el despliegue de IPv6, incluso el porcentaje de sistemas autónomos con IPv6 desplegado es mayor en aquellos que utilizan CGN frente a los que no lo utilizan.

La transición de internet a IPv6 ha sido objeto de varios estudios, dentro de las partes interesadas que hacen parte de la adopción de IPv6 se encuentran los desarrolladores de tecnología de internet IDT, los proveedores de servicios de internet ISP, los proveedores de contenido ICP y los usuarios [35][4]. Los IDT son una pieza importante debido a que son los encargados de fabricar los equipos que soportarán el tráfico IPv6, por ende deberán garantizar la disponibilidad y estabilidad de dichos dispositivos [4]. Los ISPs son los encargados de proporcionar el servicio de internet a los usuarios, hallazgos indican que un proceso no coordinado en los ISP, donde cada proveedor toma las decisiones de forma independiente puede afectar negativamente la adopción de IPv6, agregando incertidumbre, lo cual ralentiza la decisión de adopción de las partes interesadas de Internet [35], en el caso de Colombia, según la resolución 2710 de 2017, Los ISPs deberán preparar la troncal de acceso a internet para permitir el enrutamiento de los prefijos IPv6 nativos en Colombia [1]. Los ICPs proporcionan los contenidos que compensan en gran parte el valor de internet a los usuarios, los ICPs más populares pueden hacer una diferencia en la dirección de adopción de IPv6, ya que alojan el contenido más popular consumido por los usuarios, y su transición puede incentivar a los ISPs a ofrecer IPv6 a sus usuarios [35], en esta línea [36] advierte que en los últimos años ha habido avances, mientras que en 2012 sólo el 1% de los sitios web dentro del top 1 millón de Alexa anunciaban entradas AAAA, en 2019 este

porcentaje estaba por encima del 19% y en cuanto a rendimiento encontraron que de los sitios web dentro del top 10 mil de Alexa que tenían capacidades doble pila, un 54% de estos eran más rápidos sobre IPv6. En cuanto a los usuarios, dentro de la transición a IPv6 no hay un beneficio real que los afecte directamente, en cambio esta transición debe garantizar la experiencia del usuario con las diferentes aplicaciones, la configuración totalmente automática del host y una experiencia similar o superior a la obtenida con IPv4 [37] [4].

A la hora de implementar IPv6 se debe optar por algún mecanismo de transición que permita la convivencia simultánea de los protocolos IPv4 e IPv6, en secciones anteriores se mostraron las generalidades de estos mecanismos enfocadas en tres categorías según la técnica utilizada: Túneles, doble pila y traducción de protocolos. La IETF sugiere una guía para el despliegue de IPv6 en un ambiente corporativo en la RFC 7381 [38], en ella sugiere el mecanismo de doble pila para la transición a IPv6 al interior de las compañías siempre que se pueda y mecanismos tipo túnel sólo cuando se deba, argumentando que el esquema doble pila es más robusto en comparación con los túneles, los cuales son más difíciles de soportar y diagnosticar ante algún problema, y que además pueden presentar problemas de escalabilidad y rendimiento; dicho documento también contempla elementos como la elaboración de inventarios, planes de direccionamiento, consideraciones de seguridad, estos elementos también aparecen referenciados en la guía del MINTIC para la transición en Colombia [2].

Publicaciones que realizan análisis que miden la eficiencia de la red bajo diferentes sistemas de transición, señalan que el mecanismo de doble pila presenta los mejores resultados ante mediciones de RTT y throughput, en comparación con otros mecanismos de tipo túnel y traducción [26], [39]. Los análisis muestran que el mecanismo de doble pila sólo es superado por una implementación de IPv6 nativa [26], por su parte [17] y [3] proponen la selección del mecanismo doble pila para la transición hacía IPv6. Una razón del mejor rendimiento de doble pila con respecto a los otros mecanismos es su bajo procesamiento del encabezado de los paquetes IPv6 [3].

A pesar de lo mencionado anteriormente, existen algunas objeciones ante el mecanismo de transición de doble pila, una de las criticas apunta a que el mecanismo ofrece una falsa esperanza a la conservación de direcciones IPv4, toda vez que su implementación permite el uso continuo de direcciones IPv4, lo cual no lo convierte en una solución a la escasez de direcciones e incluso ponen en duda la efectividad de este mecanismo para alcanzar el objetivo final de tener una red donde IPv6 sea el protocolo dominante [30].

Por otra parte, a nivel de recursos, señalan que el mecanismo de doble pila consume un porcentaje más alto de utilización de CPU, por el hecho de mantener y administrar dos tablas de enrutamiento, en comparación con mecanismos tipo túnel y versiones nativas de IPv4 e IPv6, los cuales tienen consumos similares [17].

Otra desventaja de los ambientes doble pila se observa cuando el servicio al que quiere

acceder un usuario dispone de IPv4 pero no de IPv6, en este caso, el usuario percibe un retraso mucho mayor en comparación de un usuario con IPv4 nativo, tratando de mitigar esta situación, la IETF expidió las RFC 6555 y 8305 [40], en las que se define la primera y segunda versión del algoritmo Happy Eyeballs, apuntando a que el retraso mencionado sea mucho menos perceptible a la vez que se promueve la coexistencia de ambos protocolos [29]. Análisis hechos a este algoritmo muestran que implementar la primera versión del algoritmo Happy Eyeballs, el cual tiene un valor de temporizador predefinido de 300 ms tiende a preferir conexiones IPv6 más lentas en alrededor del 90% de los casos y explica que, al bajar el valor del temporizador a 150 ms, se obtienen mejores resultados manteniendo los mismos niveles de preferencia sobre IPv6, la segunda versión permite configurar el tiempo sugiriendo un valor de 0,25s [41],[29], [40]. Los resultados en [36] confirman que el tiempo de 150 ms no afecta el porcentaje de preferencia de IPv6 (96% para el top 10K de Alexa) y sugiere el cambio en el estándar para seguir dando ventaja a IPv6 pero al mismo tiempo reducir el tiempo de espera cuando la conexión bajo IPv6 sea considerablemente lenta, señala también que bajar el tiempo a 0 ms afectaría considerablemente la preferencia de IPv6 (56% para el top 10K de Alexa).

Según LACNIC, campus como la Universidad Pontificia Bolivariana, Universidad del Atlántico y Universidad Distrital ya han realizado la transición de parte de sus servicios al protocolo IPv6, el MINTIC como entidad del estado responsable de las telecomunicaciones también ha efectuado la adopción. En cuanto a los ISPs como UNE, Claro, entre otros ya ofrecen sus servicios de IPv6 en modalidad doble pila a clientes corporativos [8].

En los diferentes estudios antes mencionados también se comparan los escenarios nativos de IPv4 e IPv6, en donde se muestra que IPv6 es más rápido que IPv4 debido principalmente a su estructura de encabezado simplificada[17][42], el encabezado IPv4 contiene 13 campos en comparación con solo 8 campos están presentes en el encabezado IPv6.

En cuanto a los servicios corporativos, se encontraron algunos estudios relacionados con los servicios DNS, WEB y DHCP. [43] advierte sobre configuraciones erróneas en el servicio DNS, tales como registros con direcciones de enlace local o direcciones IPv4 en formato HEX, las cuales no son perceptibles por la operación doble pila pero que provocarían fallas en un entorno IPv6 puro, por su parte [44] propone un mecanismo donde sólo se envíen consultas de registros A o AAAA en vez de ambos para los sitios que no sean doble pila, optimizando los tiempos de respuesta y/o el volumen de tráfico en la red.

[36] muestra el mejoramiento en términos de disponibilidad y latencia de los principales sitios WEB frente al protocolo IPv6, también advierte sobre los distintos métodos de los navegadores frente a un entorno doble pila, mientras Chrome utiliza el algoritmo Happy Eyeballs ya tratado, otros como Firefox u Opera optan por defecto por preferir la conexión más rápida sin ninguna preferencia, [45] por su parte advierte sobre el hecho de que si bien muchas páginas WEB son accesibles a través de IPv6, algunos de sus contenidos tales como imágenes, CSS y JavaScript fallan bajo IPv6 y deben ser accedidos bajo IPv4. [46]

muestra la factibilidad del proceso de auto configuración de direcciones IPv6 bien sea por las técnicas SLAAC + RDNSS o DHCPv6 en un entorno LAN, mientras tanto [47], [48] basan su investigación en proponer mecanismos que proporcionen esquemas de seguridad y privacidad de los que no dispone el protocolo DHCPv6.

El escenario actual de IPv6 muestra una aceleración clara en el despliegue de la tecnología, aunque IPv4 sigue a la cabeza como protocolo de conectividad IP se observa una clara tendencia a un escenario donde los dos protocolos coexisten con una adopción de IPv6 cada vez mayor, el escenario de tener una red completamente IPv6 aún no es claro. Se vienen utilizando varios mecanismos buscando optimizar el espacio de direccionamiento IPv4 para así evitar su agotamiento, sin embargo, los estudios muestran que estos mecanismos tienen varias dificultades a nivel técnico y económico, pero, sobre todo, no son una solución a largo plazo para el problema de la escasez de direccionamiento IP, en ese caso, solo la adopción de IPv6 ofrece una solución concreta al problema, brindando un espacio de direccionamiento en teoría infinito.

Los análisis y mediciones realizadas frente al nivel de adopción de IPv6 muestran un claro crecimiento en los últimos años e identifican a los proveedores de tecnología, los ISPs y los proveedores de contenido como fichas clave para continuar el proceso de transición, estos últimos han demostrado avances importantes en los últimos años. En Colombia, aunque no se observa un nivel de adopción significativo, si se muestra que a partir de 2018 el porcentaje de adopción ha crecido situándose por encima del 5% influyendo seguramente las medidas del gobierno que impactan tanto a las organizaciones de carácter público como a los ISPs, lo anterior demuestra que las políticas públicas pueden influir de forma importante en la adopción de una tecnología.

En materia de mecanismos de transición, la mayoría de los estudios apuntan a mecanismos tipo túnel y de doble pila, la tecnología de traducción de protocolo es vista como un mecanismo útil para dar acceso a internet a redes IPv4 en el momento que IPv6 sea la tecnología dominante que hoy no es. El mecanismo doble pila es el recomendado en entornos LAN corporativos por la IETF y el gobierno nacional, debido en parte a su mejor rendimiento en comparación con los otros mecanismos y a que ofrece una transición suave ya que permite la coexistencia de IPv4 e IPv6 en un mismo entorno, dando prioridad al protocolo IPv6, pero permitiendo la comunicación a través de IPv4 cuando IPv6 no esté disponible o su rendimiento sea deficiente. Este trabajo pretende confirmar la operatividad del mecanismo doble pila en un entorno corporativo típico evaluando el rendimiento de algunos de los servicios de red más comunes.

Algunos de los servicios a evaluar en este trabajo como DNS, DHCP y WEB han sido objeto de estudio en diversos artículos, con enfoques diversos como funcionalidad, rendimiento, nivel de adopción, seguridad, entre otros, en cambio no se encuentra literatura previa enfocada en servicios como directorio activo y correo electrónico. Este trabajo se centra en verificar funcionalidad y medir rendimiento de los servicios previamente mencionados.

5 METODOLOGÍA

Este trabajo estará dividido por etapas. En una etapa preliminar se eligieron los servicios y las aplicaciones que prestarán dichos servicios. El documento del ministerio sugiere la revisión y configuración de los siguientes servicios: DNS, DHCP, Directorio Activo, Correo electrónico, Mensajería Instantánea, Video Conferencia, Servicio de respaldo, Servicio de Voz sobre IP, Servicio WiFi, Servicio de repositorio compartido de archivos, Servicios en la nube, Servicio Web y Acceso a Internet, Canal de comunicaciones de internet. En este trabajo serán evaluados los servicios de DNS, DHCP, Directorio Activo, Correo electrónico, servicio Wifi, servicio WEB; las aplicaciones que soportarán estos servicios serán Windows DNS Server, Windows DHCP server, Active Directory, Hmail Server, Unifi AP y Microsoft IIS respectivamente; la evaluación de cualquier otro servicio está fuera del alcance de este trabajo.

Cada servicio se someterá posteriormente a las pruebas de funcionalidad y rendimiento, las pruebas de funcionalidad deberán evidenciar que los servicios medidos funcionan en los tres entornos, sólo IPv4, sólo IPv6 y doble pila, las pruebas de rendimiento por su parte incluirán métricas objetivo para medir el desempeño de los servicios en cada uno de los tres entornos citados. Para la obtención de las métricas objetivo, en primer lugar, se utilizarán o se diseñarán herramientas encargadas de generar el tráfico específico hacía cada uno de los servicios, el tráfico generado será capturados desde las estaciones cliente por una herramienta analizadora de paquetes, dichos datos serán posteriormente organizados en un software de hoja de cálculo para finalmente utilizar una aplicación de análisis y visualización de datos para la presentación de resultados, en caso de que la herramienta generadora de tráfico utilizada para un servicio específico se encargue de brindar las métricas y/o graficar los resultados se aprovechará dicha funcionalidad.

Después de la selección de servicios y pruebas a realizar para cada uno de ellos, se procederá a una segunda etapa de diseño de la infraestructura de red que cumpla con los requisitos exigidos tanto por el MINTIC como por los proveedores de los servicios seleccionados. En esta etapa se estudiarán diferentes topologías, en busca de seleccionar una que se adecúe a los requerimientos propios del proyecto, definida la topología se analizarán los elementos, observando las características de cada uno de ellos, para escoger el que genere mejores prestaciones para el proyecto a desarrollar, enfatizando claramente en la necesidad de que cada elemento, salvo excepciones previamente definidas, sea compatible con el protocolo IPv6, esto será validado con las hojas de datos de los fabricantes y corroborado en la plataforma de configuración de los diferentes elementos que harán parte de la infraestructura.

Una tercera etapa será definida para la fase de implementación, en la cual se llevará a cabo la instalación y configuración de cada uno de los componentes del sistema, esto incluye elementos de hardware y software, de este último hacen parte claramente las aplicaciones

que darán soporte a los servicios elegidos en la primera etapa. La configuración estará orientada a un entorno doble pila, donde coexistan IPv6 e IPv4, tal como lo indican los lineamientos del ministerio.

Finalmente, en una última etapa se realizarán las pruebas de funcionalidad y rendimiento definidas en la primera etapa con su correspondiente análisis de resultados.

6 PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

Los resultados serán presentados en forma secuencial, de acuerdo con las etapas previamente definidas de planeación y presentación de la propuesta, montaje y configuración del entorno de pruebas, aplicación de pruebas y análisis de resultados.

La primera etapa denominada fase de planeación contempla el inventario de equipos que harán parte del entorno de pruebas a construir, el correspondiente diseño de red que incluye el plan de direccionamiento y el diagrama topológico de la red a implementar, y el protocolo de pruebas a los diferentes servicios, incluyendo las herramientas que se utilizarán para la generación del tráfico específico. En la segunda etapa se llevará acabo la implementación de la solución, se configurará cada uno de los equipos de red de acuerdo con el plan de direccionamiento, la interconexión de estos según la topología y la instalación y parametrización de los servicios a evaluar en el servidor contemplado para ello. En la tercera y última etapa se llevarán a cabo los tests de acuerdo con el protocolo de pruebas estipulado en la etapa 1. Luego de poner en marcha los generadores de tráfico y realizar la captura de información necesaria del lado del cliente para el cálculo de las métricas estimadas, se hará un análisis de los resultados según los hallazgos encontrados bajo los tres escenarios a evaluar: IPv4 Puro, IPv6 Puro y Doble pila.

6.1 Fase de planeación

El documento del MINTIC “Guía de Transición de IPv4 a IPv6 para Colombia” [2] propone en la fase de planeación las siguientes actividades: Inventario de activos de TI (Hardware y Software) indicando la compatibilidad de estos con el protocolo IPv6, diseño de red que incluye plan de direccionamiento y topología de red, protocolos de pruebas a llevar a cabo para los servicios a probar. Estas actividades se detallan a continuación.

6.1.1 Inventario de activos

El documento del MINTIC “Guía de Transición de IPv4 a IPv6 para Colombia” [2] propone en la fase de planeación elaborar un inventario de los equipos y el software de la infraestructura de TI de la organización que requiere la transición al protocolo IPv6. En este se debe indicar cuales de ellos soportan el nuevo protocolo, cuáles deben actualizarse para garantizar el cumplimiento y cuales definitivamente no soportan el protocolo.

En este trabajo se hará un inventario de los equipos y el software que van a intervenir en la implementación del entorno de pruebas, haciendo uso de los formatos sugeridos por el documento en mención. Para los equipos de cómputo, tanto equipos de escritorio como servidores, se utilizarán sistemas operativos Windows, esta decisión se tomó debido a la alta presencia de dicho sistema operativo para equipos de escritorio y servidores [49], [50] . Como plataforma de virtualización de servidores se eligió el fabricante VMware, líder del mercado global en según la consultora G2 [51]. La **Tabla 1** muestra los equipos de cómputo utilizados en el proyecto, indicando sus recursos, versión de sistema operativo y otras características: la **Tabla 2** muestra los equipos de comunicaciones a utilizar, detallando el modelo y la versión de firmware entre otras características.

Equipos de cómputo

Equipo	**Memoria**	**CPU**	**Disco**	**SO**	**Versión**	**Software instalado**	**Rol**	**Versión IP**
Lenovo E460	8GB	Intel core i5-6200u	1x500 GB	Windows	10 build 18362	Office 365 Pro, Power BI, Silk Performer	Cliente	IPv4/IPv6
HP	24GB	Intel Xeon E5504	2x300 GB	Vsphere	6.0.0	NA	Server	IPv4/IPv6
Máquina Virtual (alojada	8GB	4 core	1x100 GB	Windows 10	build 18362	Silk Performer, Wireskark,	Cliente	IPv4/IPv6

Equipo	Memoria	CPU	Disco	SO	Versión	Software instalado	Rol	Versión IP
en server HP)						Network Monitor		
Máquina Virtual (alojada en server HP)	8GB	4 core	1x100 GB	Windows	Server 2016	DNS Server DHCP Server IIS Hmail ADDS	Server	IPv4/IPv6

Tabla 1. Inventario de equipos de cómputo.
Fuente: Elaboración propia

Equipos de comunicaciones:

Equipo	Marca	Modelo	SO	Puertos Ethernet	Rol	Versión IP
Firewall UTM	Fortinet	Fortigate 60E	Forti OS	10 GE	Firewall perimetral/ Enrutador	IPv4/IPv6
Switch	Aruba HPE	2530	YA 16.02	48 GE	Conmutador	IPv4/IPv6
Punto de acceso	Cisco Meraki	MR42	MR 25.13	1 GE	Punto de acceso	IPv4/IPv6

Tabla 2. Inventario de equipos de comunicaciones.
Fuente: Elaboración propia

El documento “Guía de Transición de IPv4 a IPv6 para Colombia” [2] sugiere que el firmware/SO de los dispositivos que hagan parte de la infraestructura tengan el certificado IPv6 Ready Logo como forma de garantizar que dichos equipos cumplen con los requisitos básicos de IPv6, en caso de no disponer del logo, los dispositivos y sus correspondientes firmwares/SO deberán demostrar el cumplimiento de diversos RFC relacionados con el cumplimiento de IPv6 según la categoría del equipo.

Los equipos que hacen parte del diseño tienen el certificado IPv6 ready Logo, a excepción del punto de acceso, la **Tabla 3** muestra el nombre que se le asignó a cada equipo en el diseño de red junto con los detalles de la certificación IPv6. Para el punto de acceso, el

fabricante garantiza funcionalidad limitada del protocolo, sin embargo, la característica del paso de tráfico IPv6 de los clientes, que es la necesaria en este proyecto si está avalada.

Nombre de dispositivo	**Dispositivo**	**Firmware/Sistema Operativo**	**IPV6 Ready -Logo ID**
CLI-W10	Máquina virtual	Windows 10	02-C-001328
PC-W10	Lenovo E460	Windows 10	02-C-001328
DCIPv6	Máquina virtual	Windows server 2016	02-C-001887
SVR_HV	HPE Proliant	ESXi 6.0.0	02-C-001482
FW_FG60E	Fortigate 60 E	Forti OS 6.2	02-C-000615
SW_HPL2	Aruba HPE 2530	YA 16.02	02-C-001628

Tabla 3. Compatibilidad de equipos con IPv6.
Fuente: Elaboración propia

6.1.2 Diseño de red

El documento del MINTIC “Guía de Transición de IPv4 a IPv6 para Colombia” [2] estima que se debe proponer un diseño de red en la cual coexistan los protocolos IPv4 e IPv6 en un entorno doble pila. En esta sección se detallan aspectos del plan de direccionamiento de ambos protocolos, topología de red y proceso de enrutamiento.

Plan de direccionamiento

En un escenario ideal, el plan de direccionamiento IPv6 se debe hacer con el prefijo global asignado por el RIR o el ISP, por motivos meramente económicos no es viable hacerlo para este proyecto, en su lugar, el plan de direccionamiento de IPv6 se hará utilizando el rango ULA, de acuerdo con las buenas prácticas recomendadas por la IETF en su RFC 7381 [38] y el documento “Guía de Transición de IPv4 a IPv6 para Colombia” [2].

En caso de que se quiera obtener un prefijo IPv6 global en Colombia, se deberá verificar el cumplimiento de los prerrequisitos de LACNIC [52], entre los cuales están proyectar la utilización del bloque en el tiempo, entregar la topología de red y realizar descripción del plan de enrutamiento a implementar, una vez estén cubiertos los prerrequisitos, se deberá hacer la solicitud ante LACNIC de un prefijo /48 como mínimo, esto implica el registro de la organización si no se ha efectuado previamente y el pago de una tarifa en caso de que se apruebe la solicitud, el enrutamiento del prefijo y el acceso a internet deberá ser negociado con un ISP local. Otra opción para tener un prefijo IPv6 global es solicitarlo directamente al ISP, esto por un lado evita el trámite ante LACNIC pero implica que el prefijo está licenciado

para uso del ISP y en caso de cambiar de proveedor se deberá cambiar de prefijo, por lo anterior, lo recomendado es solicitar un bloque ante LACNIC.

Para la elaboración del plan de direccionamiento con direcciones ULA se tuvieron en cuenta los siguientes lineamientos:

- Tomar como base un bloque de direccionamiento /48 para realizar la segmentación IPv6.
- Realizar el direccionamiento a partir del segmento ULA FC00::/7.
- Realizar la segmentación IPv6 asignando subredes /64.
- Asignar una subred para los siguientes servicios: WIFI Usuarios para la conectividad inalámbrica de los equipos cliente, LAN Usuarios para la conectividad cableada de los equipos cliente, LAN Servidores para el equipo servidor que aloja los servicios a probar, LAN Administración para los equipos de comunicaciones.
- Asignar segmentos IPv6 no consecutivos para las diferentes subredes.
- Asignar direccionamiento privado para las subredes en IPv4.
- Establecer una equivalencia entre los direccionamientos IPv4 e IPv6 adoptados.
- Asignar una VLAN para cada subred.

Cálculo de prefijo IPv6

Teniendo en cuenta las anteriores consideraciones se realiza el cálculo del prefijo de red a usar para la implementación IPv6 siguiendo las recomendaciones dadas en el RFC 4193 para direcciones ULA. Este proceso se hace para fines demostrativos recalcando que en un entorno productivo el prefijo generalmente /48 es directamente asignado por el RIR o el ISP, se recomienda gestionar el prefijo ante el RIR, de tal manera que el segmento asignado sea propiedad de la organización, independiente del ISP que se quiera elegir para enrutar el prefijo en internet.

Segmento de red:

$$FC00::/7$$

El bit 8 se debe establecer a 1, de tal manera tenemos:

$$FD00::/8$$

Los otros 40 bits los obtenemos de la siguiente forma.

Obtenemos el tiempo en formato NTP 64 bits, para un cálculo durante el día 02/05/2020 tenemos la fecha en formato Hexadecimal:

$$E25872A1876F3800$$

Obtenemos el EUI 64 de una interfaz específica y la transformamos a binario, con lo cual tenemos:

$$CA5B76FFFED89EAA$$

Concatenamos los dos resultados anteriores y calculamos un HASH basados en el algoritmo SHA 1

$$56cbde77404957a8b7ef0686e3b79f551b94c90a$$

Utilizamos los últimos 40 bits para completar el prefijo /48

$$FD55:1B94:C90A::/48$$

Asignación de prefijos IPv4

Para el rango de direcciones IPv4 se escoge la subred 192.168.0.0/16 como base para diseñar el direccionamiento de subredes con máscara /24. En el tercer octeto se escogen los valores de 30, 40, 120 y 140 para las diferentes subredes. La **Tabla 4** muestra el resumen del plan de direccionamiento detallando el nombre asignado a la subred, el ID de la VLAN y los segmentos IPv4 e IPv6 respectivos.

Diseño de subredes

Nombre de subred	VLAN ID	Subred IPv4	Subred IPv6
WiFi	20	192.168.30.0/24	FD55:1B94:C90A:30::/64
LAN Usuarios	40	192.168.40.0/24	FD55:1B94:C90A:40::/64
LAN Servidores	120	192.168.120.0/24	FD55:1B94:C90A:C0::/64
LAN Administración	140	192.168.140.0/24	FD55:1B94:C90A:E0::/64

Tabla 4. Plan de direccionamiento
Fuente: Elaboración propia

Topología de red

En la **Figura 1** se muestra la topología física de red propuesta, el switch está encargado de interconectar los demás dispositivos. Los enlaces entre el switch y los equipos de cómputo se hacen a través de la VLAN correspondiente, mientras que los enlaces del switch con el

punto de acceso y el firewall se hacen a través de enlaces troncales por donde se propagan las VLANs de interés en cada enlace y con la VLAN de administración como VLAN Nativa.

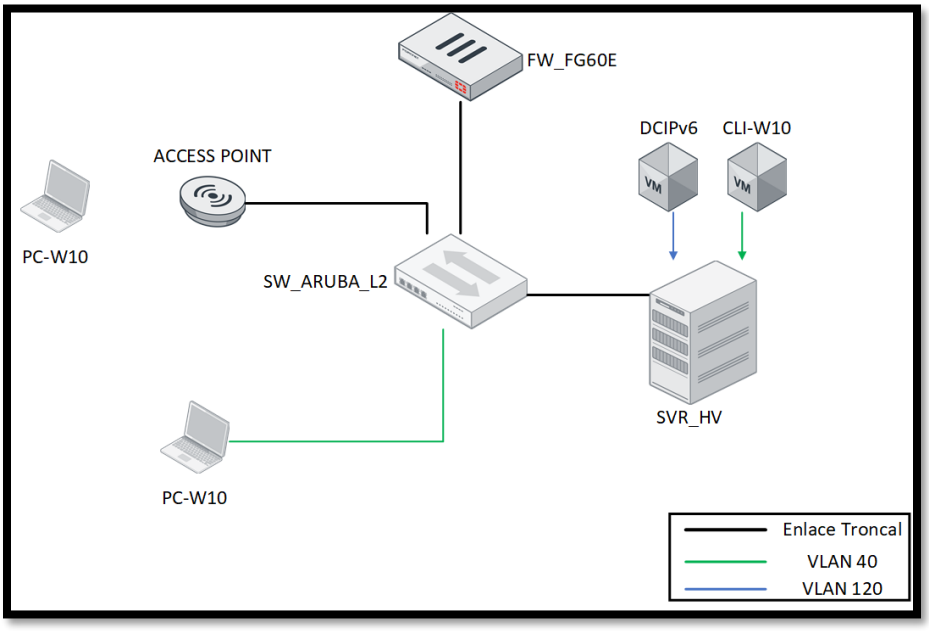


Figura 1. Topología física de diseño de red

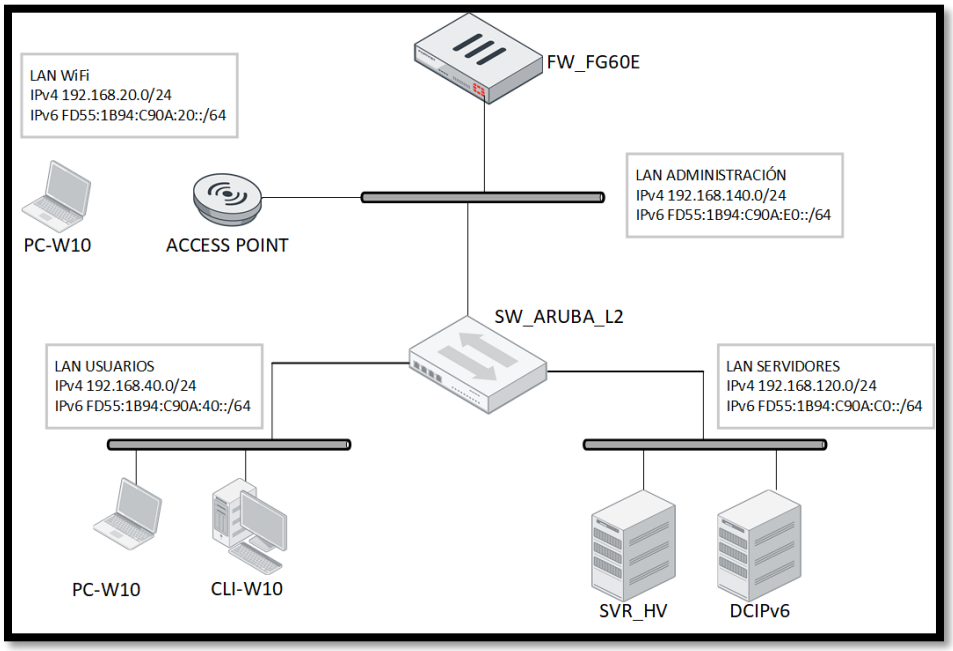


Figura 2. Topología lógica de diseño de red

En la **Figura 2** se muestra la topología lógica de red propuesta, en ella se observan los diferentes segmentos de red contemplados en el plan de direccionamiento, las funciones de enrutamiento dentro del diseño planteado están a cargo del firewall, donde se configurará una VLAN para cada segmento de red.

6.1.3 Protocolo de pruebas

El documento “Guía de Transición de IPv4 a IPv6 para Colombia” [2] sugiere que se deben establecer protocolos de pruebas de validación que permitan determinar la correcta operación de las aplicaciones y servicios que soporten IPv6 en coexistencia con IPv4, tal como lo contempla el escenario doble pila.

Inicialmente, se realizarán pruebas funcionales, las cuales permitirán determinar la correcta operación de los servicios evaluados bajo tres entornos: sólo IPv4, sólo IPv6 y doble pila. Superadas las pruebas funcionales se realizarán pruebas de rendimiento donde se utilizarán herramientas y/o scripts para generación de tráfico específico de cada servicio desde los dispositivos cliente hacía los servidores de la infraestructura implementada nuevamente bajo los tres entornos anteriormente citados. Se tomarán métricas evaluadas desde el lado del cliente para conocer tiempos de respuesta de operaciones típicas soportadas por los diferentes servicios. Los resultados serán producto de los datos recolectados por las herramientas de generación de tráfico para cada uno de los casos evaluados. Para el caso del servicio WiFi, se evaluarán las métricas del entorno cableado.

Para la recolección de datos se utilizará el software Wireshark, los datos serán tabulados en la herramienta Microsoft Excel y serán procesados para su visualización utilizando la herramienta Power BI.

La **Tabla 5** muestra detalle de las métricas a evaluar por servicio en las pruebas de rendimiento, indicando las herramientas de generación de tráfico utilizadas y la acción desarrollada.

Servicio Medido	Aplicación	Herramienta	Acción	Métrica
DNS	Microsoft DNS	Powershell Script	Envío de solicitudes iterativas de consultas DNS	Tiempo de respuesta a consultas DNS sobre registros A y AAAA
DHCP	Microsoft DHCP	PowerShell Script	Liberación y renovación iterativa de dirección IPv6 en interfaz de red	Medición de tiempo de adquisición de dirección IPv6 (Proceso SARR)
DHCP	Microsoft DHCP	Powershell Script	Petición de direccionamiento IPv4 iterativo previo cambio de dirección MAC en interfaz de red	Medición de tiempo de adquisición de dirección IPv6 (Proceso DORA)
DHCP	Microsoft DHCP	Powershell Script	Restablecimiento iterativo de interfaz de red para simular una nueva conexión a la red	Medición de tiempo de renovación de direccionamiento IPv4 o IPv6
Correo electrónico	Hmail Server	Powershell Script	Envío iterativo de correo electrónico por protocolo SMTP	Medición de tiempo de envío de correo de cliente a servidor
Correo electrónico	Hmail Server	Powershell Script	Envío iterativo de correo electrónico con archivo adjunto por protocolo SMTP	Medición de tiempo de envío de correo de cliente a servidor
Directorio activo	MS Active Directory	Powershell Script	Envío iterativo de inicios de sesión que requieren autenticación en el AD	Medición del tiempo de verificación de autenticación en el directorio activo.
WEB	Microsoft IIS	Silk Performer	Generación de script de carga de página para posterior reproducción con carga de trabajo variable	DOM interactivo: tiempo transcurrido desde la solicitud hasta que el navegador ha completado el análisis de todos los elementos HTML y la

Servicio Medido	Aplicación	Herramienta	Acción	Métrica
				construcción del DOM
WEB	Microsoft IIS	Silk Performer	Generación de script de carga de página para posterior reproducción con carga de trabajo variable	DOM Completo: período de tiempo desde la solicitud hasta que el navegador ha completado la descarga y el procesamiento de todos los recursos
WEB	Microsoft IIS	Silk Performer	Generación de script de carga de página para posterior reproducción con carga de trabajo variable	Carga finalizada: período de tiempo desde la solicitud hasta que el navegador ha completado la ejecución de la función OnLoad.

Tabla 5. Métricas de rendimiento por servicio
Fuente: Elaboración propia

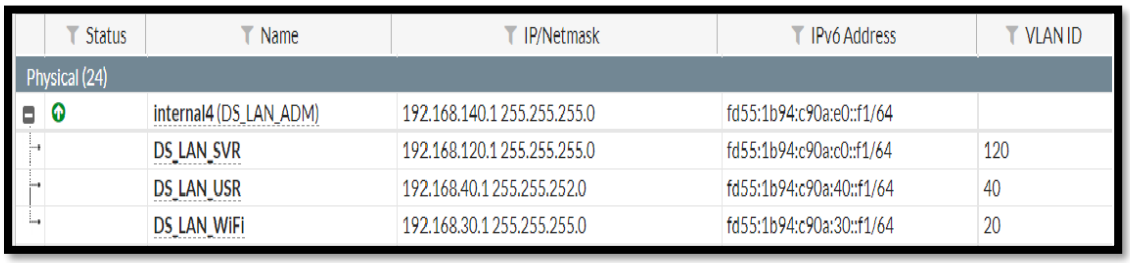
6.2 Fase de implementación

El documento del MINTIC “Guía de Transición de IPv4 a IPv6 para Colombia” [2] propone en la fase de planeación las siguientes actividades: Configuración y habilitación de protocolo IPv6 en cada uno de los componentes de hardware y software de la infraestructura de red, incluyendo servicios y aplicaciones. Estas actividades se detallan a continuación.

6.2.1 Configuración de equipos de comunicaciones

Configuración de firewall

El firewall Fortigate 60E cumplirá las funciones de enrutador entre las diferentes subredes, la configuración de las interfaces de red hecha en el dispositivo se muestra en la **Figura 3** , la VLAN de administración funciona como VLAN nativa en la interfaz seleccionada y las demás VLAN son etiquetadas en dicha interfaz para su enrutamiento. Además de lo anterior, se deben configurar las interfaces para advertir el prefijo IPv6 e indicarle al firewall que el servicio DHCPv6 será proporcionado por otro dispositivo.



Status	Name	IP/Netmask	IPv6 Address	VLAN ID
Physical (24)				
	internal4 (DS_LAN_ADM)	192.168.140.1 255.255.255.0	fd55:1b94:c90a:e0::f1/64	
	DS_LAN_SVR	192.168.120.1 255.255.255.0	fd55:1b94:c90a:c0::f1/64	120
	DS_LAN_USR	192.168.40.1 255.255.252.0	fd55:1b94:c90a:40::f1/64	40
	DS_LAN_WiFi	192.168.30.1 255.255.255.0	fd55:1b94:c90a:30::f1/64	20

Figura 3. Configuración de interfaces de red en firewall

Configuración de switch

El switch Aruba HPE 2530 cumplirá la función de conmutador capa 2, en él se define la IP de administración en los protocolos IPv4 e IPv6 y se crean las VLANs predefinidas, las cuales se asignan a los puertos troncales y de acceso de acuerdo con el diseño previo. La configuración de las diferentes VLAN del switch se muestra en la **Figura 4**.

Figura 4. Configuración VLAN de switch

Configuración de punto de acceso

El punto de acceso Meraki MR 42 cumplirá la función de permitir la conectividad inalámbrica a los equipos de cómputo del proyecto, este se configura en el dashboard del fabricante. Se verifica que la característica de paso de tráfico IPv6 esté habilitada y se configura el SSID “Test IPv6” asociado con la VLAN predeterminada en el diseño para la conexión WiFi

6.2.2 Configuración de equipos de cómputo

Configuración de plataforma de virtualización

Las plataformas de virtualización de servidores permiten ejecutar en un solo servidor físico múltiples sistemas operativos de forma simultánea. Cada sistema operativo se aloja en un contenedor de software denominado máquina virtual, las cuales funcionan totalmente independientes unas de otras. Debido a la limitación de recursos y a la optimización de estos que ofrecen las plataformas de virtualización, se recurre a su implementación como

base para el montaje de los diferentes sistemas operativos que albergarán los servicios a medir en este trabajo.

Se elige la plataforma Vsphere 6.0 del fabricante VMware para el montaje de las diferentes máquinas virtuales, la **Figura 5** muestra las máquinas virtuales instaladas sobre este.

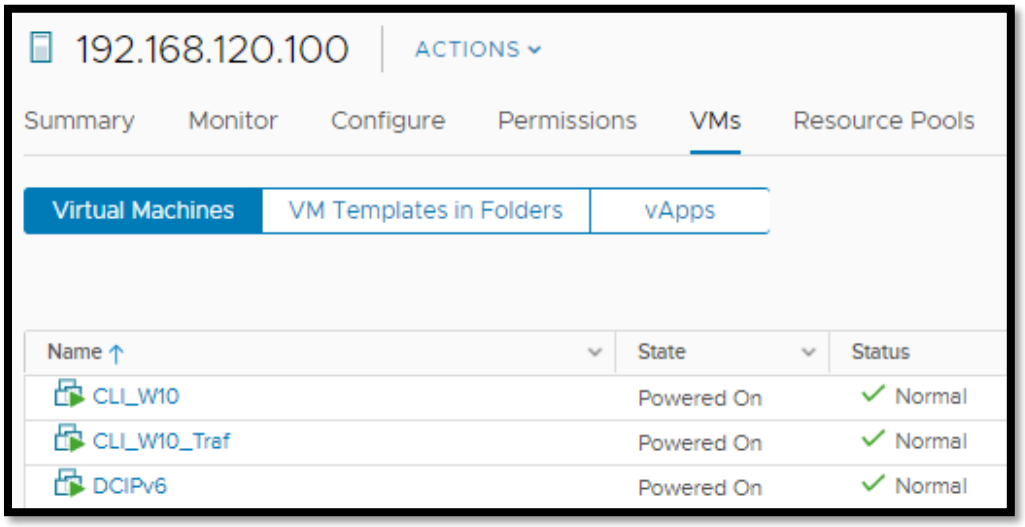


Figura 5. Máquinas virtuales en plataforma VMware

Configuración de servidores

Se configura una máquina virtual para albergar el servidor que hará parte del entorno de pruebas, el servidor DCIPv6, estará encargado de alojar los servicios de Directorio Activo, DNS, DHCP, WEB, Hmail. La **Tabla 6** muestra la configuración de la máquina, se presentan los componentes físicos, la configuración de red y el sistema operativo utilizado.

Item	**DCIPv6**
Sistema Operativo	Windows Server 2016
Núcleos de CPU	4
Memoria RAM	6 GB
Disco	40 GB
Dirección IPv4	192.168.120.50
Puerta de enlace IPv4	192.168.120.1

Item	DCIPv6
DNS IPv4	192.168.120.50
Dirección IPv6	FD55:1B94:C90A:C0::AA
Puerta de enlace IPv6	FD55:1B94:C90A:C0::F1
DNS IPv6	FD55:1B94:C90A:C0::AA
Servicios	AD, DHCP, DNS, WEB

Tabla 6. Características de máquina virtual servidor
Fuente: Elaboración propia

6.2.3 Configuración de servicios

Configuración de servicio de directorio activo

El servicio de Directorio Activo se activó en el servidor DCIPv6 agregando el rol de servicios de dominio de Active Directory en un entorno Windows Server 2016. El nombre de dominio definido fue DSIPv6.local y la máquina DCIPv6 fue promovida como controlador de dominio. Posterior a la activación, una máquina cliente fue agregada al dominio para verificar la correcta unión de equipos a este servicio.

Configuración de servicio DNS

El servicio DNS se instala como rol de Windows Server junto con el servicio de directorio activo. Luego de la instalación se procede a verificar la presencia de la zona DSIPv6.local en el administrador del servicio y se configura la zona de búsqueda inversa.

Configuración de servicio DHCP

El servicio DHCP es configurado como rol en el servidor DCIPv6, luego de autorizar dicho servicio, se configuran los ámbitos IPv4 e IPv6 para las subredes. En el caso de las subredes diferentes a la subred de servidores, se habilita el firewall Fortinet como DHCP Relay para las interfaces específicas, especificándole la dirección IPv4 e IPv6 a la cual debe reenviar las peticiones DHCP provenientes de dichas interfaces, en este caso particular al servidor DCIPv6. En la **Figura 6** se muestran los ámbitos IPv4 e IPv6 de las subredes de servidores y usuarios LAN.

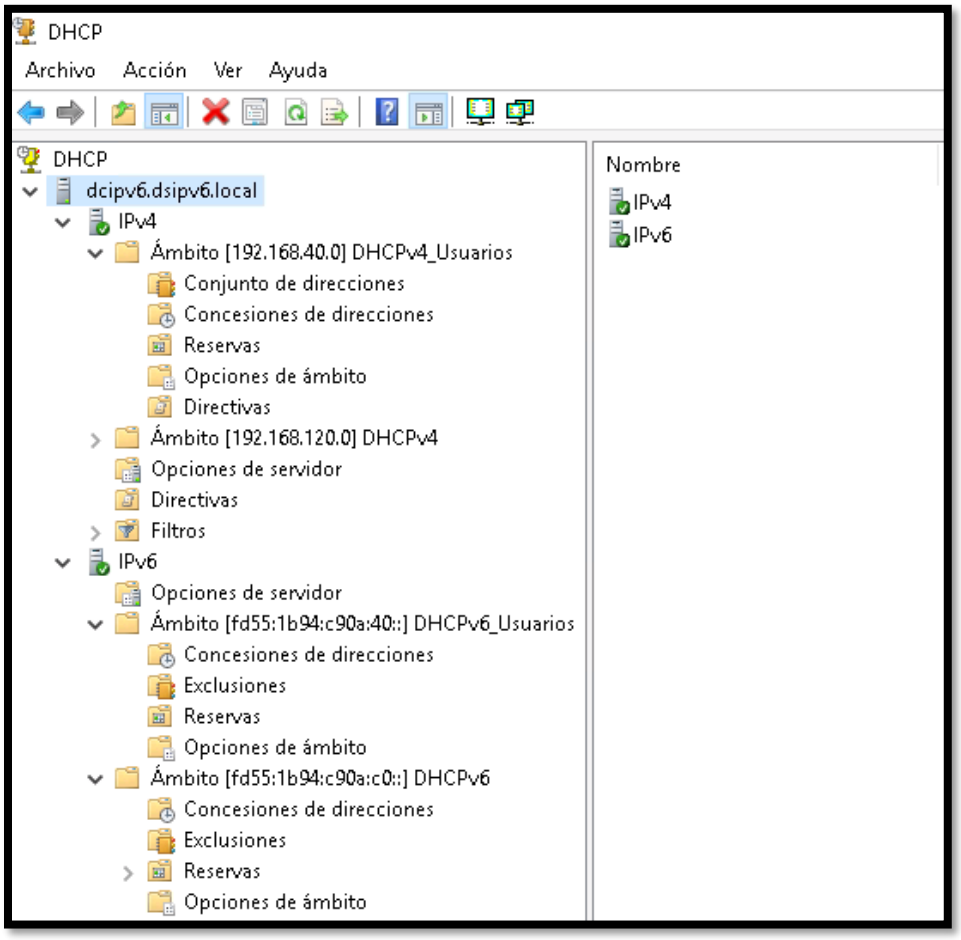


Figura 6. Ámbitos en servidor DHCP

Configuración de servicio WEB

El servicio WEB se activa a través del rol IIS (Internet Information Services) en la plataforma Windows Server. Después de habilitar el módulo, se procede a configurar un nuevo sitio WEB y posteriormente cargar una plantilla WEB en dicho sitio, la plantilla en mención es descargada de [53] bajo licencia de uso libre.

Configuración de servicio de correo electrónico

El servicio de correo electrónico se configura a través de la aplicación hMail server, la cual es de tipo *free open source* para ambientes Windows [54], ésta se instala en el servidor

DCIPv6. El dominio adoptado para el correo es el mismo dominio principal dsipv6.local, dos usuarios de prueba, user1 y user2, son creados en el directorio activo, los cuales son sincronizados en la plataforma de administración de hMail. En la **Figura 7** se muestra la la plataforma de administración hMail server.

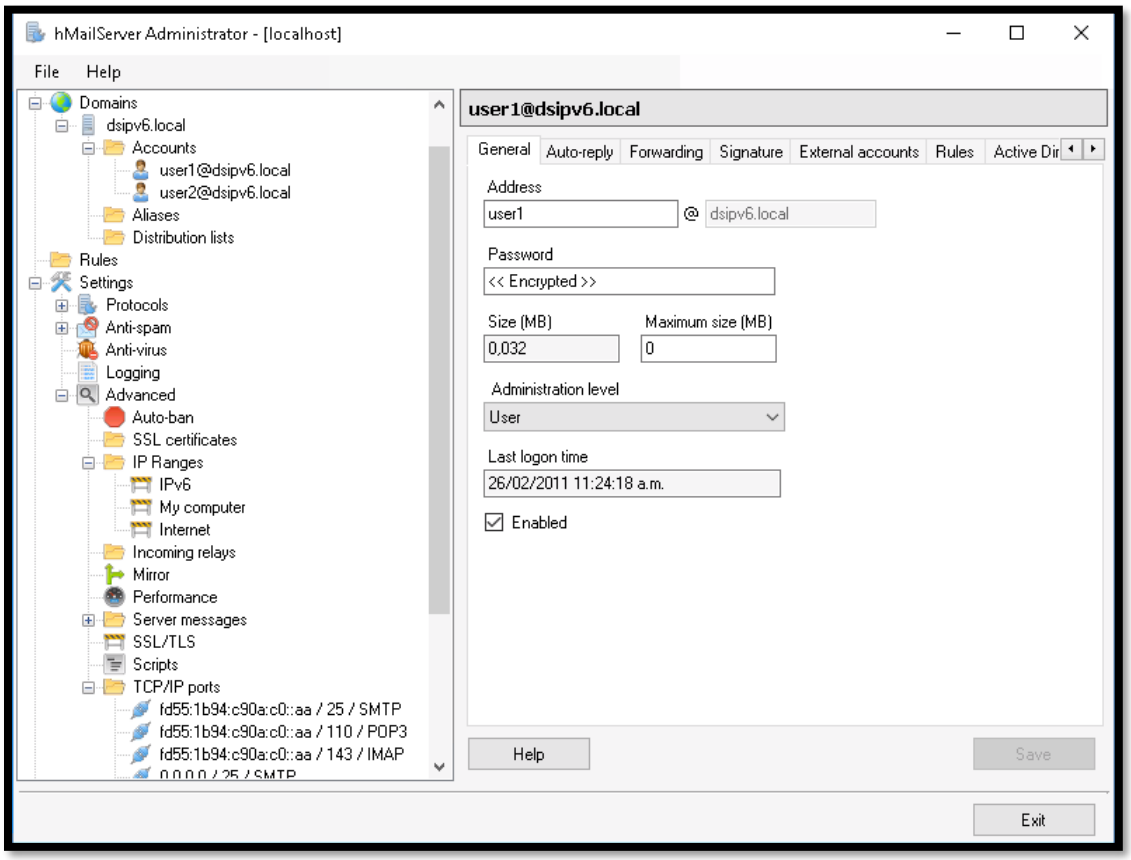


Figura 7. Plataforma de administración hMail

6.2.4 Configuración de equipos cliente

Para la realización de pruebas se utilizarán dos clientes, uno de ellos es una máquina virtual con sistema operativo cliente alojado en el mismo servidor donde se aloja la máquina virtual que cumple funciones de servidor, a diferencia de esta última que está en la VLAN de Servidores, la interfaz de red de la máquina cliente se encuentra en la VLAN de usuarios. La segunda máquina cliente es un dispositivo portátil del fabricante Lenovo. Las características de las máquinas cliente se muestran en la **Tabla 7**, indicando el tipo, recursos de hardware y sistema operativo.

Item	PC-W10	CLI-W10
Tipo de equipo	Portátil	Máquina virtual
Sistema Operativo	Windows 10	Windows 10
Núcleos de CPU	2	2
Memoria RAM	8 GB	8 GB
Disco	500 GB	32 GB
Interfaces de red	LAN, WiFi	LAN

Tabla 7. Características de equipos cliente
Fuente: Elaboración propia

6.3 Fase de pruebas

El documento del MINTIC “Guía de Transición de IPv4 a IPv6 para Colombia” propone en la fase de pruebas las siguientes actividades: Realización de pruebas y monitoreo de la funcionalidad del protocolo IPv6 en los servicios y/o aplicaciones instaladas, afinamiento de configuraciones de hardware, software y servicios. Además de las pruebas de funcionalidad, este trabajo abarca las pruebas y el análisis del rendimiento de los diferentes servicios instalados en los escenarios sólo IPv4, sólo IPv6 y doble pila, todo esto de acuerdo con los protocolos de pruebas establecidos en la fase 1.

6.3.1 Pruebas de funcionalidad

Las pruebas de funcionalidad están orientadas a garantizar la operatividad de los servicios implementados en el entorno de pruebas bajo tres escenarios: sólo IPv4, sólo IPv6 y doble pila; todas las pruebas se realizarán haciendo solicitudes del servicio desde una máquina cliente a la máquina donde se encuentra alojado el servicio, las evidencias de las pruebas de funcionalidad están detalladas en el Anexo 1. La **Tabla 8** muestra la descripción de las pruebas realizadas para cada servicio indicando la métrica a tomar.

Tipo de servicio	**Prueba**	**Métrica**
Conectividad	Envío de paquetes ICMP	Respuesta satisfactoria
DNS	Solicitud DNS de registro local	Solicitud satisfactoria
DHCP	Solicitud de direccionamiento IP	Solicitud satisfactoria
Active Directory	Solicitud de autenticación	Solicitud satisfactoria
Active Directory	Solicitud de permisos	Solicitud satisfactoria
Hmail	Envío de correo electrónico	Envío satisfactorio
Hmail	Recepción de correo electrónico	Recepción satisfactoria
IIS	Acceso a página WEB	Acceso satisfactorio

Tabla 8. Pruebas de funcionalidad realizadas
Fuente: Elaboración propia

Pruebas de conectividad

Se realizan pruebas de conectividad a través del protocolo ICMP desde la máquina cliente CLI-W10 al servidor DCIPv6. Se ejecuta con respuesta exitosa el comando PING en los escenarios sólo IPv4, sólo IPv6 y doble pila respectivamente, esto se hace deshabilitando las pilas de las diferentes versiones del protocolo IP según corresponda. Para el escenario doble pila se envían tres peticiones, en la primera se verifica conectividad a través de la dirección IPv4, en la segunda a través de la dirección IPv6 y en la última petición se hace la solicitud por nombre para verificar la preferencia del protocolo IPv6 como lo indica el enfoque doble pila.

Pruebas de servicio DNS

Las pruebas de funcionalidad del servicio DNS se hacen utilizando el comando NSLOOKUP, a través del cual se realizan consultas para obtener las direcciones IPv4 e IPv6 correspondientes a un host en específico. Además de lo anterior se hacen consultas DNS inversas, verificando que el servidor es capaz de identificar el nombre de un equipo en la red a través de la dirección IPv4 o IPv6 dada.

Pruebas de servicio DHCP

Las pruebas del servicio DHCP se realizan desde el equipo cliente CLI-W10, se configuran las tarjetas de red en modo DHCP para ambos protocolos. Se observa la asignación correcta de direccionamiento IP en la interfaz de línea de comandos del equipo y posteriormente se confirma la asignación de parte del servidor DHCP en la consola de administración del servicio de la máquina DCIPv6.

Pruebas del servicio de Directorio Activo

Las pruebas del servicio de directorio activo se realizan desde el equipo cliente CLI-W10, se inicia sesión con dos usuarios previamente creados en el directorio activo, dichos inicios de sesión son satisfactorios, también se realiza acceso por escritorio remoto al servidor donde nuevamente se confirma el funcionamiento exitoso de la autenticación. Las pruebas anteriormente citadas se realizan en los ambientes sólo IPv4, sólo IPv6 y Dual Stack.

Pruebas de servicio WEB

Las pruebas para este servicio se hacen cargando el sitio WEB, previamente alojado en el servicio IIS en DCIPv6, desde un explorador instalado en la máquina cliente CLI-W10. Las pruebas se hacen cargando el sitio a través de la dirección IPv4 e IPv6 del servidor y a través del nombre de dominio. Las pruebas se ejecutan satisfactoriamente.

Pruebas de servicio de correo electrónico

Para realizar las pruebas de este servicio se configura la aplicación Microsoft Outlook como cliente de correos y en cada uno de los perfiles de los usuarios creados se configura la cuenta de correos respectiva bajo protocolo IMAP.

Se realizan pruebas bajo ambientes sólo IPv4, sólo IPv6 y Dual Stack de forma satisfactoria. Las pruebas consisten en el envío de un correo desde el usuario user1@dsipv6.local al usuario user2@dsipv6.local y viceversa.

Pruebas de servicio WIFI

Para las pruebas del servicio WiFI se realizaron los mismos procedimientos anteriormente descritos en cada uno de los servicios con resultados satisfactorios, la conexión se hace en la banda de 5Ghz.

6.3.2 Pruebas de rendimiento y análisis de resultados

Las pruebas de rendimiento se realizan teniendo en cuenta las métricas predefinidas que nos permitan comparar el rendimiento de los diferentes servicios en los ambientes sólo IPv4, sólo IPv6 y doble pila. Los resultados para los diferentes servicios se muestran a través de gráficas que exhiben los tiempos de respuesta en las diferentes iteraciones acompañados de medidas que apoyan la interpretación de los datos obtenidos.

Pruebas de servicio DNS

Para las pruebas de rendimiento del servicio DNS, se elabora un script en PowerShell para la generación de tráfico, dicho script genera una consulta iterativa a un registro presente en el servidor DNS, de acuerdo con el entorno en el que estemos realizando la prueba, la consulta obtiene un registro A (IPv4), un registro AAAA (IPv6) o ambos (Doble Pila), la métrica está enfocada en medir el tiempo que tarda el cliente en obtener dichos registros luego de generada la consulta. Para capturar el tráfico generado por el script se utiliza la herramienta de captura de paquetes WireShark.

La **Figura 8** muestra los tiempos de respuesta de las consultas DNS medidas en ambientes independientes (sólo IPv4 o sólo IPv6), del comportamiento de la gráfica y las medidas de tendencia se evidencian claramente los mejores tiempos de respuesta en las consultas de registros AAAA con respecto a registros tipo A.

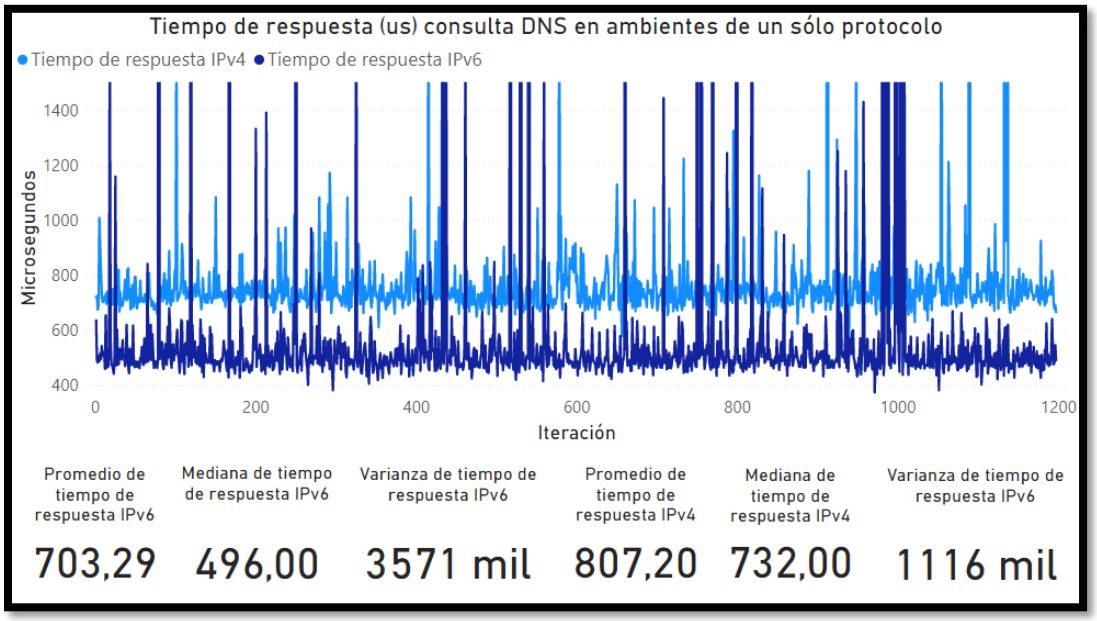


Figura 8. Tiempo de respuesta de consulta DNS en ambientes puros

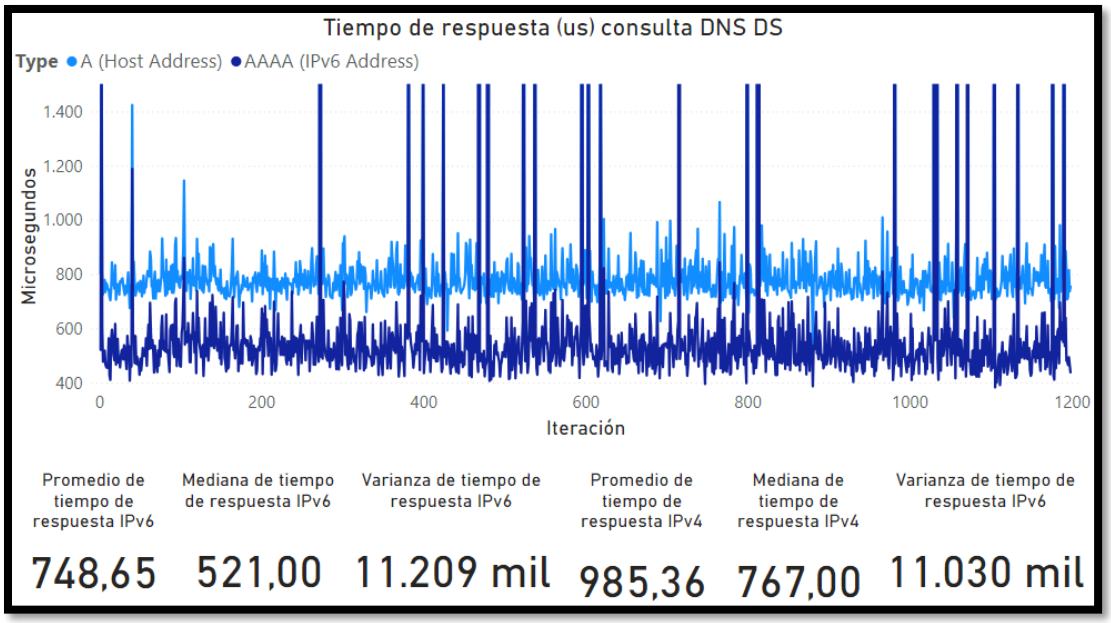


Figura 9. Tiempo de respuesta de consulta DNS en ambiente Dual Stack

La **Figura 9** muestra los tiempos de respuesta de las consultas DNS en ambiente Dual Stack categorizándolas por tipo de registro, similar a las mediciones en ambientes independientes, se observa una respuesta más rápida de la consulta para el registro AAAA, dicha respuesta se calcula como la diferencia de tiempo entre el envío de la consulta y la recepción de esta. Sin embargo, haciendo un análisis más detallado, se observa que pese

a que la consulta se hace para ambos registros (A y AAAA), el registro AAAA es consultado con un tiempo de retardo frente al registro A, esta situación es ilustrada en la **Figura 10** donde se observa un promedio de retardo de 295 microsegundos. La **Figura 11** exhibe los tiempos de respuesta haciendo el ajuste antes mencionado y evidencia que el cliente obtiene el registro A en promedio 58 microsegundos antes que el registro AAAA.

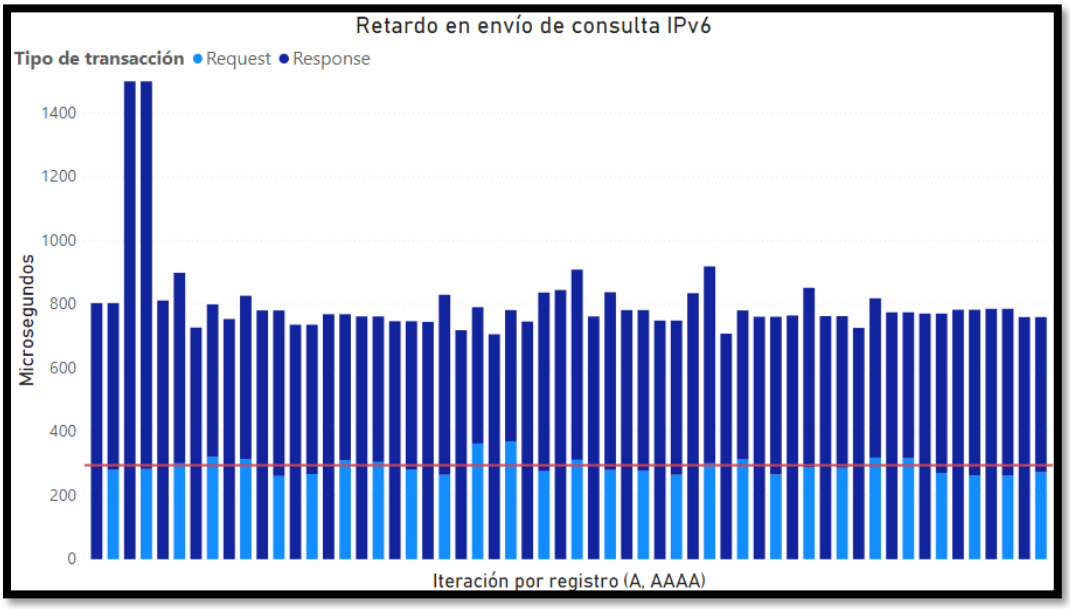


Figura 10. Retardo en envío de consulta de registro AAAA

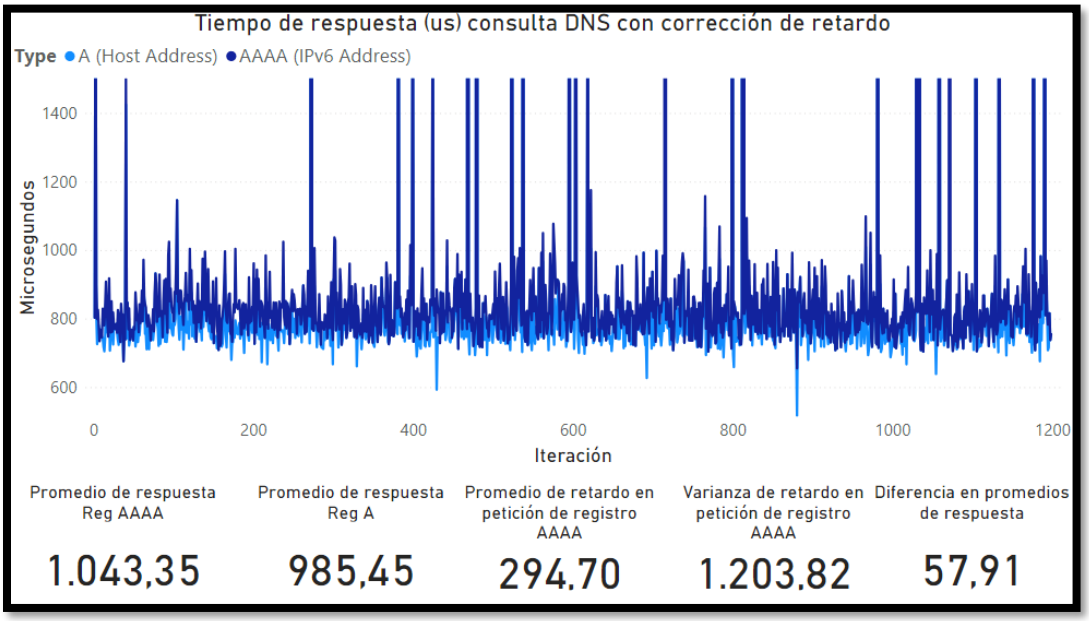


Figura 11. Tiempo de consulta DNS en Dual Stack con corrección de retardo

Pruebas de servicio DHCP

Las pruebas de servicio DHCP se dividen en dos escenarios típicos de operación del servicio, adquisición de un nuevo direccionamiento y renovación de un direccionamiento previamente adquirido. En el primer escenario, para el direccionamiento IPv4 se genera un script que cambia la dirección MAC de la interfaz de red, con esto se obliga a que se inicie el proceso de adquisición en cada iteración, en el caso de IPv6, el script realiza una liberación de la dirección actual y petición de una nueva dirección. Para el segundo caso, renovación de direccionamiento, un script emula la desconexión de la tarjeta de red y su posterior conexión, de esta forma se inicia un proceso de renovación de dirección IPv4 o IPv6 previamente adquirida. Todos los scripts mencionados son elaborados en PowerShell, para la captura de tráfico se utiliza la herramienta Network Monitor. Las métricas se enfocan en el tiempo que demora el cliente en obtener o renovar una dirección IP luego de hacer la petición. La **Figura 12** muestra el tiempo de adquisición de direccionamiento IPv4 (DORA) en ambientes puro y doble pila y la **Figura 13** muestra ese mismo tiempo para el direccionamiento IPv6 (SARR) en ambientes IPv6 puro y doble pila, en ellas se observa que el tiempo de adquisición de direccionamiento IPv6 es significativamente más elevado que el de IPv4, y si observamos en las diferentes medidas evidenciamos que la diferencia está marcada principalmente en la aceptación del direccionamiento de parte del cliente, es decir, el tiempo que tarda el cliente en enviar el paquete request en IPv4 después de haber recibido el paquete offer es significativamente menor al tiempo que tarda el mismo cliente en enviar el paquete request en IPv6 después de haber recibido el paquete advertise, haciendo mucho más lento el proceso DHCP en IPv6. Comparativamente, En los procesos de adquisición en ambientes de una sola pila (sólo IPv4 o sólo IPv6) notamos que el comportamiento es similar al evidenciado en el ambiente doble pila.

Para obtener las métricas del proceso de renovación de direccionamiento hicimos pruebas en un ambiente doble pila cuyo resultado se muestra en la **Figura 14** y en ambientes de una sólo pila cuyo resultado se muestra en la **Figura 15**, comparando ambos resultados podemos evidenciar que el proceso de renovación IPv6 es más rápido que el proceso de renovación IPv4, midiendo esta diferencia a través de las medianas, la cual no es tan sensible a valores extremos como la media, observamos que esta diferencia está alrededor del 20% a favor del protocolo IPv6.

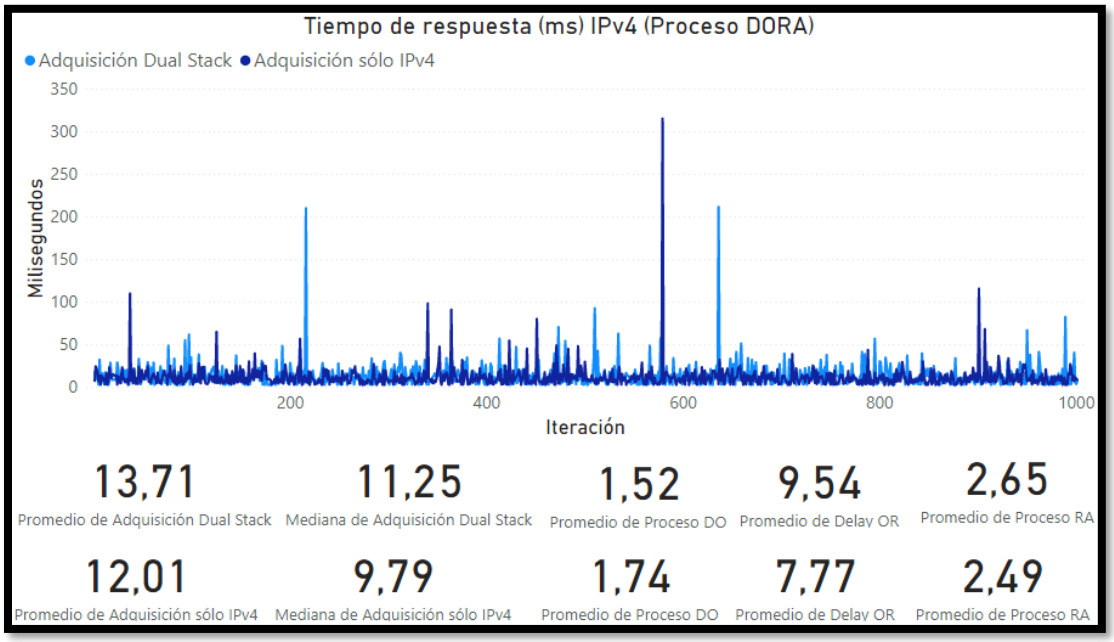


Figura 12. Proceso de direccionamiento DHCPv4 (DORA)

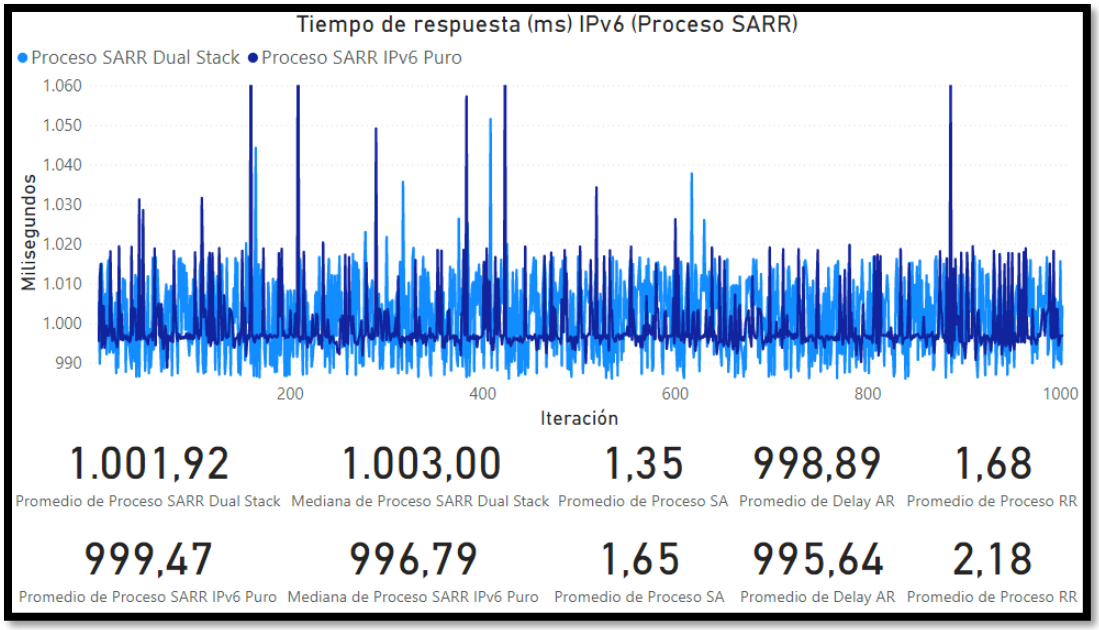


Figura 13. Proceso de direccionamiento DHCPv6 (SARR)

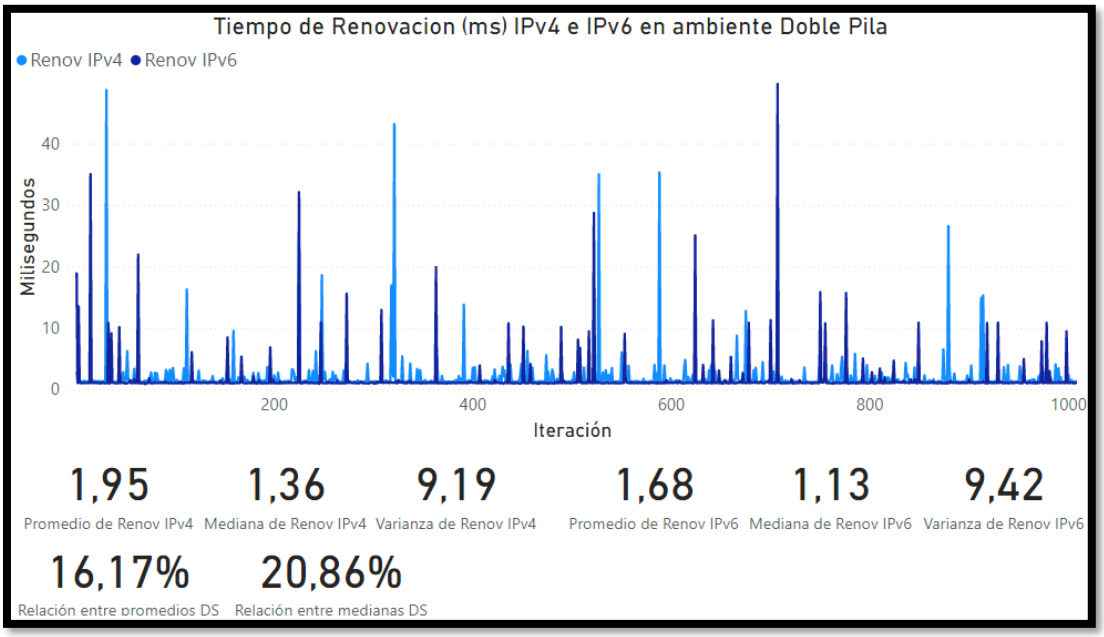


Figura 14. Proceso de renovación DHCP Dual Stack

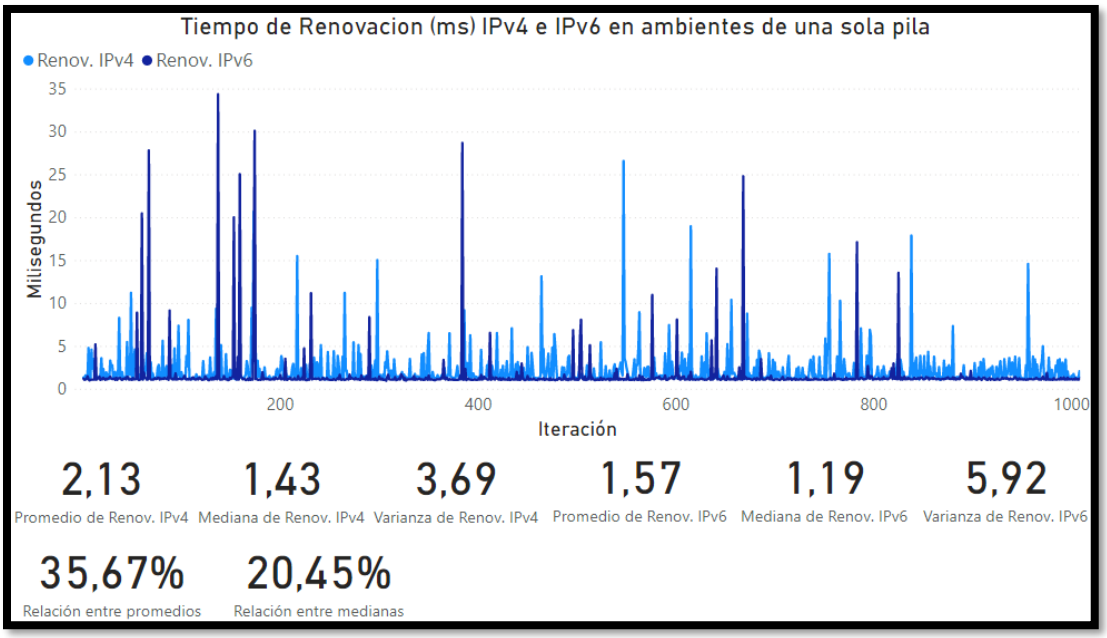


Figura 15. Proceso de renovación DHCP en ambientes de una sola pila

Pruebas de servicio de correo electrónico

Las pruebas del servicio se focalizan en el envío de un correo electrónico a través del protocolo SMTP, en esta se mide el tiempo desde que el cliente inicia la solicitud de envío hasta que recibe la notificación del servidor que el correo fue enviado. Aquí se consideran dos escenarios, el primero contempla el envío sin archivos adjuntos y el segundo incluye en el correo un archivo adjunto de formato JPG con un peso de 149 KB. El tráfico fue generado a través de un script de PowerShell y fue capturado a través de la herramienta WireShark.

La **Figura 16** muestra los resultados del envío de un correo sin adjunto en los tres ambientes (sólo IPv4, sólo IPv6, Dual Stack). La **Figura 17** exhibe los resultados del ejercicio anterior para un correo con archivo adjunto.

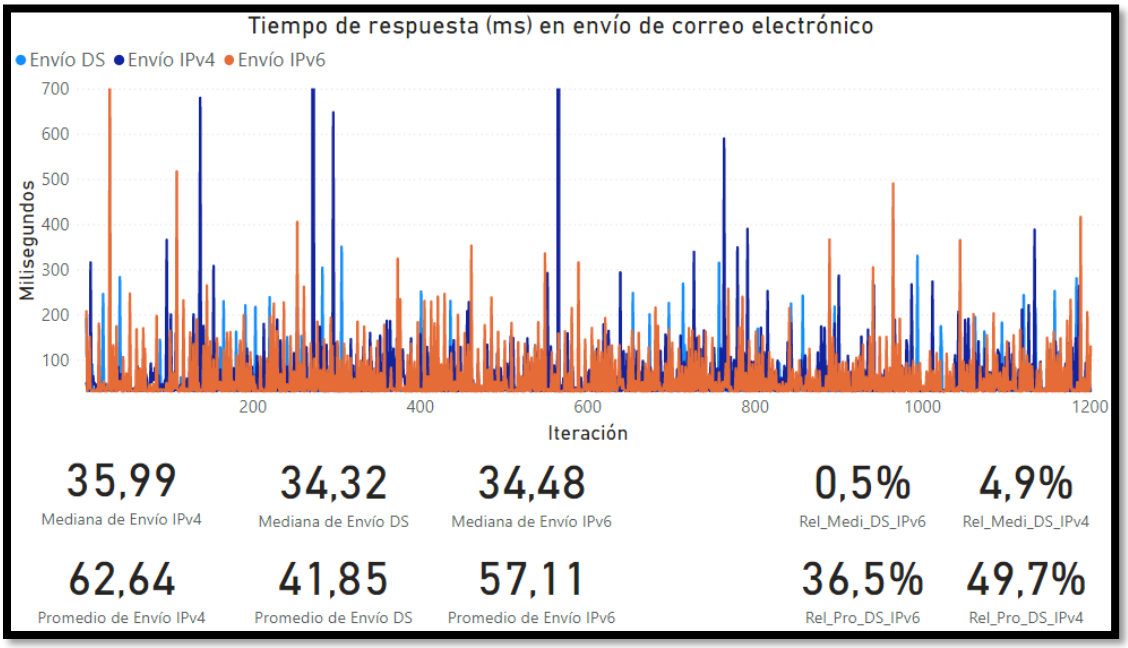


Figura 16. Envío de correo sin archivo adjunto

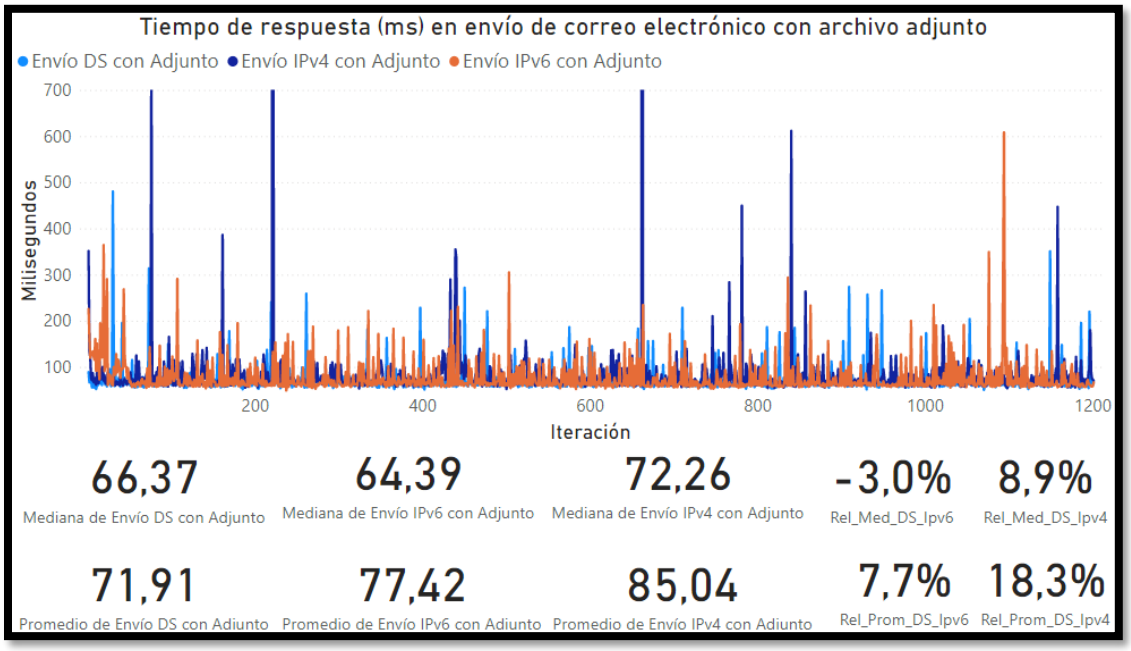


Figura 17. Envío de correo con archivo adjunto

Observando los resultados, evidenciamos mejores tiempos de respuesta para el protocolo IPv6, ya sea en Dual Stack (IPv6 Preferido) o en ambiente sólo IPv6 frente a los tiempos de IPv4, esto es común en ambos escenarios, con y sin archivo adjunto. Comparando las medianas, notamos diferencias menores entre los ambientes doble pila y sólo IPv6, lo cual es lógico al utilizar ambos IPv6. Al realizar la misma comparación del ambiente doble pila con el ambiente sólo IPv4, notamos diferencias mayores, entre un 5% y un 10% a favor del primer escenario.

Pruebas de servicio de directorio activo

Las pruebas de rendimiento para este servicio se enfocaron en el proceso de autenticación. Se simula de manera iterativa la autenticación de un usuario que demanda un inicio de sesión en el directorio activo para acceder a una estación remota a través del protocolo WinRM, en cada iteración se hace una limpieza de los tickets almacenados en la estación cliente para garantizar que el proceso de autenticación se lleva a cabo en su totalidad sin información almacenada en caché.

La **Figura 18** muestra los resultados de los tiempos de autenticación en el directorio activo del usuario en los tres entornos evaluados. El rendimiento es muy similar en todos los entornos, siendo los tiempos ligeramente mejores en IPv6 (Ipv6 puro y Dual Stack). Como en las pruebas anteriores, el promedio es muy sensible a los valores extremos lo que hace que las diferencias sean mucho mayores en esta medida de tendencia.

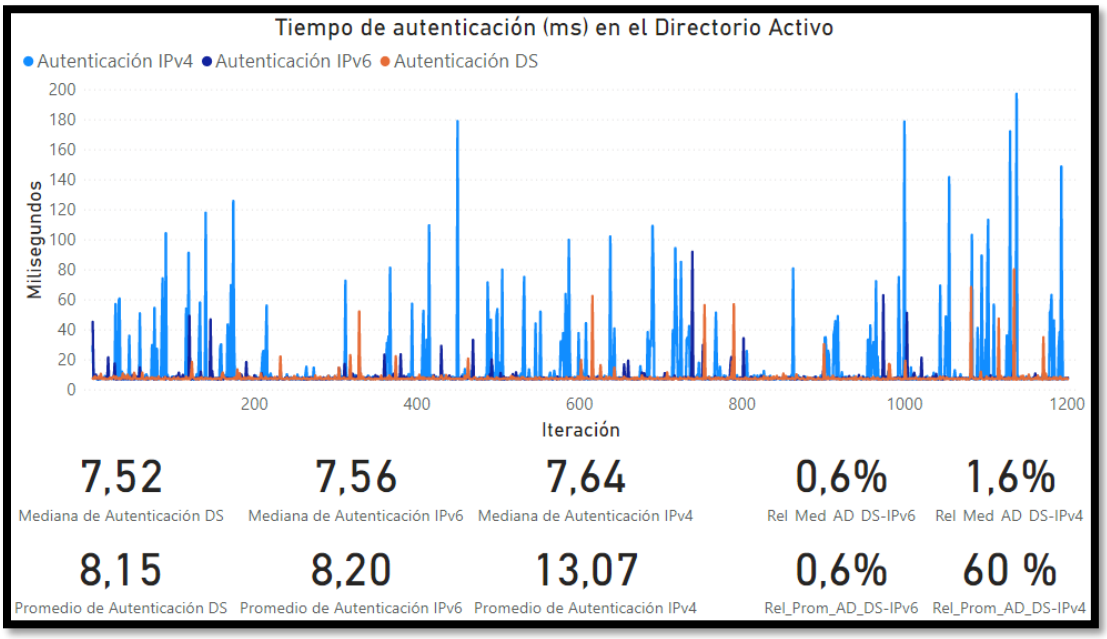


Figura 18. Tiempo de respuesta de autenticación contra el Directorio Activo

Pruebas de servicio WEB

Las pruebas del servicio WEB se hacen a través de la herramienta Silk Performer de Micro Focus, el modelo se basa en “grabar” la carga de la página web utilizada para el proyecto, la cual ha sido alojada previamente en el servidor IIS. Después de realizar la acción de grabación, el software genera un script que se puede replicar en forma de carga de trabajo iterativamente. El navegador utilizado para las pruebas es internet explorer, la versión del software disponible permite simular hasta 10 usuarios virtuales, las pruebas se realizan en este escenario de 10 usuarios. En esta prueba se analizan tres métricas, la primera, llamada DOM Interactivo, mide el tiempo transcurrido desde la solicitud del usuario hasta que el explorador WEB ha completado el análisis de la página y construido el DOM, entendiendo este último como la estructura de objetos que genera el explorador para la carga de la página; la segunda, llamada DOM completo, mide el tiempo entre el envío de la solicitud hasta que tiene lugar el procesamiento de todos los recursos y la página carga completamente en el navegador; por último, la métrica carga finalizada indica el tiempo pasado desde la solicitud hasta que el navegador completa la a ejecución de la función onLoad. Como paso final en cada proceso de carga de la página, el navegador envía un evento onLoad, que activa la función onLoad. Una vez que se ejecutan las funciones onLoad, se puede ejecutar alguna lógica adicional en la aplicación. La **Figura 19** muestra los resultados de la métrica DOM interactivo en los tres ambientes (IPv4 Puro, IPv6 Puro y

Dual Stack), la **Figura 20** y la **Figura 21** muestran los resultados de la métrica DOM Completo y Carga Finalizada en los mismos tres ambientes citados.

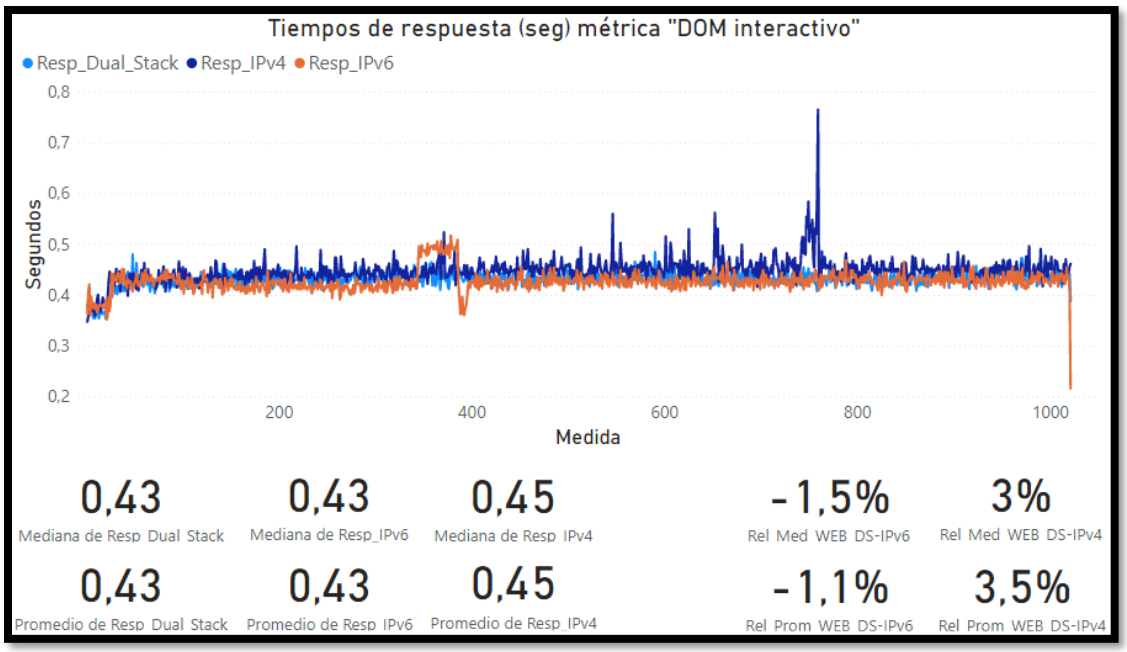


Figura 19. Tiempos de respuesta "DOM interactivo"

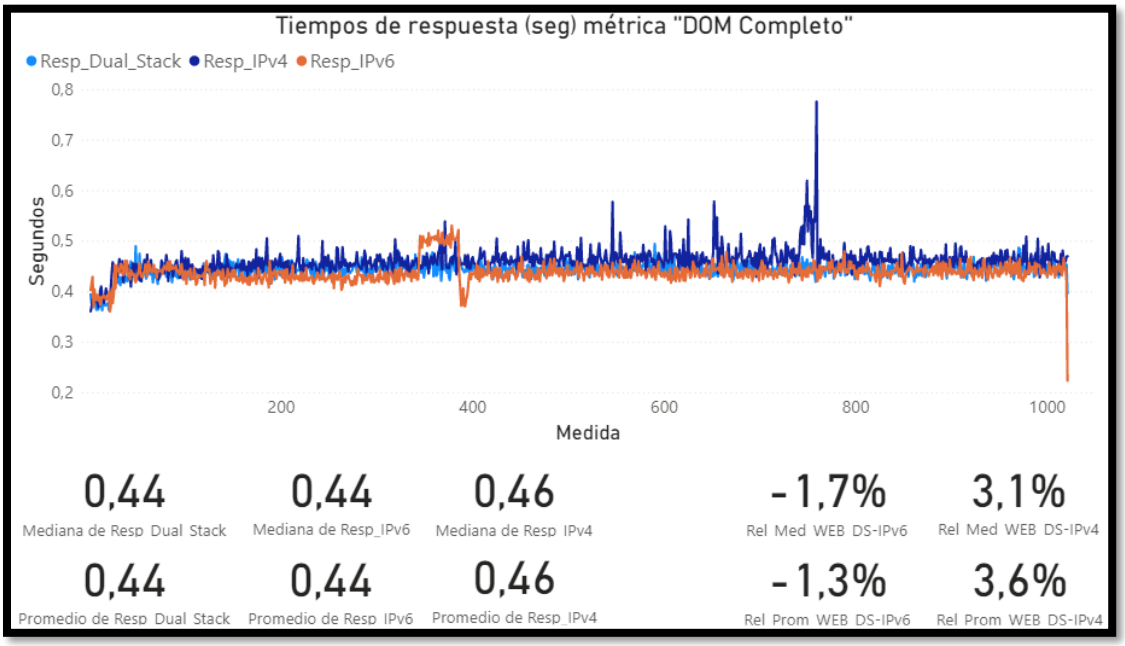


Figura 20. Tiempos de respuesta "DOM Completo"

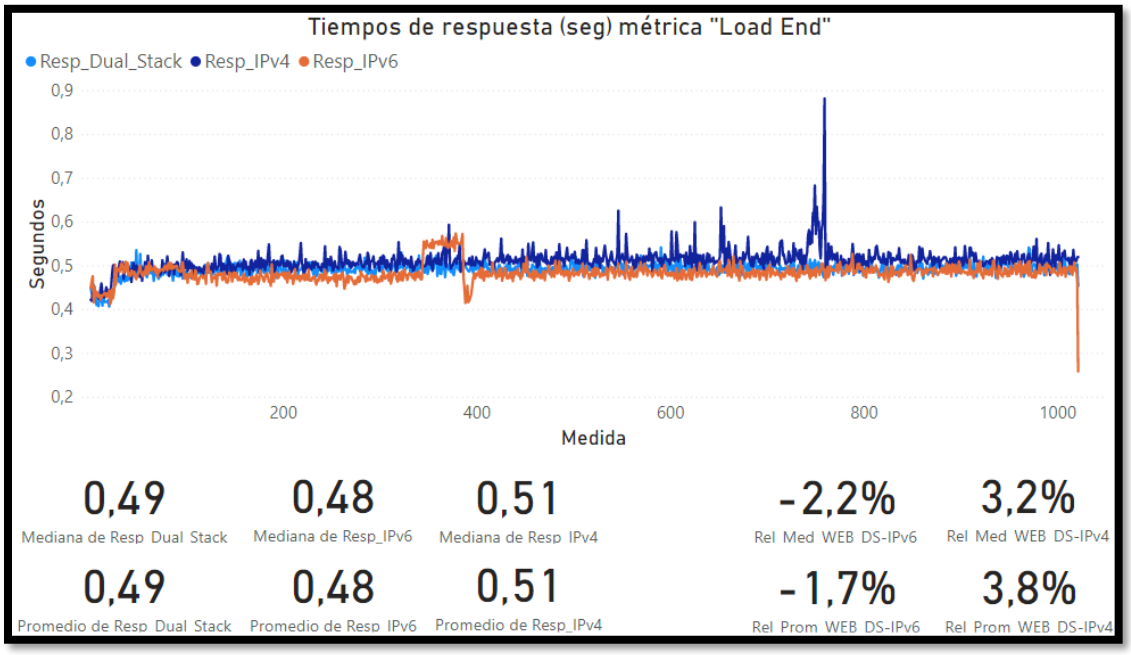


Figura 21. Tiempos de respuesta "Carga Finalizada"

La **Tabla 9** y la **Tabla 10** muestran un resumen de los promedios y las medianas respectivamente obtenidas en las métricas de los servicios evaluados en el ambiente cableado.

Servicio Medido	**Métrica**	**Media (ms)**			**Comparativa con doble pila**	
		Sólo IPv4	**Sólo IPv6**	**Doble Pila**	**Sólo IPv4**	**Sólo IPv6**
DNS	Consulta de registro	0,81	0,70	1,04	-22,1%	-32,7%
DHCP	Renovación de IP	2,13	1,57	1,95	9,2%	-19,4%
Mail	Envío sin adjunto	62,64	57,11	41,85	49,7%	36,5%
Mail	Envío con adjunto	85,04	77,42	71,91	18,3%	7,7%
Directorio activo	Autenticación	13,07	8,20	8,15	60%	0,6%
WEB	DOM interactivo	448	428	432	3,5%	-1,1%
WEB	DOM Completo	460	438	444	3,6%	-1,3%
WEB	Carga finalizada	511	484	493	3,8%	-1,7%

Tabla 9. Promedios en tiempos de respuesta de métricas en ambiente cableado
Fuente: Elaboración propia

Servicio Medido	Métrica	Mediana (ms)			Comparativa con doble pila	
		Sólo IPv4	Sólo IPv6	Doble Pila	Sólo IPv4	Sólo IPv6
DNS	Consulta de registro	0,73	0,50	0.82	-11,0%	-39,0%
DHCP	Renovación de IP	1,43	1,19	1,36	5,1%	-12,5%
Mail	Envío sin adjunto	35,99	34,48	34,32	4,9%	0,5%
Mail	Envío con adjunto	72,26	64,39	66,37	8,9%	-3,0%
Directorio activo	Autenticación	7,64	7,56	7,52	1,6%	0,6%
WEB	DOM interactivo	446	426	433	3,0%	-1,5%
WEB	DOM Completo	458	437	445	3,1%	-1,7%
WEB	Carga finalizada	510	483	494	3,2%	-2,2%

Tabla 10. Medianas en tiempos de respuesta de métricas en ambiente cableado
Fuente: Elaboración propia

Pruebas de servicio WiFi

Para las pruebas del servicio WiFi se repiten las pruebas que se hicieron en entorno cableado para los servicios de DNS, DHCP, WEB, Directorio Activo y Correo Electrónico. Las gráficas con los resultados de cada prueba se muestran en el Anexo 2. La **Tabla 11** muestra los promedios en los tiempos de respuesta para las diferentes métricas evaluadas en un ambiente WiFi. Haciendo un análisis comparativo con los resultados en ambiente cableado se notan tiempos de respuesta mayores en cada métrica, esto se puede explicar por el cambio a un medio compartido como es el inalámbrico. En lo que respecta a la comparación de las métricas en los diferentes escenarios, se evidencia un comportamiento similar al entorno cableado, tiempos similares entre los ambientes y con una ligera ventaja para el tráfico IPv6 (ya sea en ambiente IPv6 puro y/o en ambiente doble pila con IPv6 preferido) frente a IPv4 en los servicios de directorio activo, WEB y correo electrónico.

Servicio Medido	Métrica	Media (ms)			Comparativa con doble pila	
		Sólo IPv4	Sólo IPv6	Doble Pila	Sólo IPv4	Sólo IPv6
DNS	Consulta de registro	6,82	6,33	6,43	6,1%	-1,5%
DHCP	Renovación de IP	7,66	5,73	6,05	26,6%	-5,2%
Mail	Envío sin adjunto	87,04	70,63	70,81	22,9%	-0,3%
Mail	Envío con adjunto	108,80	92,35	96,93	12,2%	-4,7%
Directorio activo	Autenticación	268,6	279,4	253,9	6%	10%
WEB	DOM interactivo	446	435	443	0,6%	-1,9%
WEB	DOM Completo	456	445	455	0,4%	-2,1%
WEB	Carga finalizada	511	494	508	0,6%	-2,8%

Tabla 11. Promedios en tiempos de respuesta de métricas en ambiente WiFi
Fuente: Elaboración Propia

7 CONCLUSIONES

Después de realizar la implementación del entorno de pruebas para los test de compatibilidad y rendimiento de características típicas de los servicios DNS, DHCP, correo electrónico, directorio activo, WEB y WiFI podemos evidenciar que estos son totalmente funcionales en el ambiente doble pila sugerido por el Ministerio. El proceso de adquisición de direccionamiento DHCP muestra una clara diferencia a favor del protocolo IPv4, sin embargo, el usuario final sólo hace esto una vez para conectarse a una red nueva o si el tiempo de arrendamiento configurado para alguna red conocida se ha vencido, por lo que no representa una amenaza para la experiencia del usuario final. En lo que respecta al protocolo DNS se observan mejores tiempos de respuesta en IPv6, pero haciendo un análisis más detallado se encuentra que el sistema operativo de los equipos usados para el proyecto envía la consulta IPv6 con un tiempo de retardo con respecto a la consulta IPv4 lo cual a la postre le da una ligera ventaja a la recepción del registro para el protocolo IPv4, esto es del orden de microsegundos según los resultados.

En los protocolos de Directorio Activo, correo electrónico y WEB se evidencian rendimientos muy similares en los tres ambientes, los ambientes IPv6 puro y doble pila, donde IPv6 es preferido, muestran una ligera ventaja con respecto a los tiempos de respuesta del protocolo IPv4.

Las pruebas de servicio WiFI mostraron tiempos de respuesta mayores al ambiente cableado, lo cual se puede explicar debido al menor ancho de banda disponible en la red WLAN; al margen de los tiempos de respuesta más elevados, se observó un comportamiento similar a los del entorno cableado comparando los tres escenarios de medida (sólo IPv6, sólo IPv4 y doble pila), los tiempos de respuesta fueron similares en todas las medidas y en servicios como directorio activo, WEB y correo electrónico se observaron nuevamente mejores tiempos cuando el protocolo IPv6 era utilizado.

La ligera ventaja obtenida por IPv6 puede obedecer a su estructura de encabezado más simplificado, el cual necesitaría menor tiempo de procesamiento. En todo caso, las diferencias notadas en los tres ambientes no son considerablemente altas para afirmar que alguno de los tres ambientes ofrezca una clara diferencia de rendimiento que redunde en una experiencia diferenciada para el usuario final, sin embargo, debido al alcance limitado de este proyecto sólo a redes LAN, no fue evaluado el procesamiento NAT, el cual puede aumentar la diferencia a favor de IPv6 de cara al acceso a la WAN toda vez que en IPv4 es común y en IPv6 no es necesario. Con base en los resultados obtenidos en la medición de los diferentes servicios podemos concluir que la transición al modelo doble pila y a futuro a un modelo sólo IPv6 no implicará diferencia marcada en el rendimiento comparado con lo que hoy experimenta un usuario en un ambiente netamente IPv4, esto claro está, en un ambiente LAN ya que el acceso WAN está fuera del alcance de este proyecto.

El entorno de pruebas generado puede ser replicado por organizaciones que requieran probar la funcionalidad y el rendimiento de los servicios y aplicaciones que hagan parte de su red bajo el modelo sugerido por el gobierno nacional, dentro de los aspectos importantes a tener en cuenta está procurar que los equipos usados, sobre todo servidores y equipos de comunicación, dispongan del logo IPv6 Ready, de lo contrario se tendrá que verificar un listado de RFCs por cada tipo de dispositivo, lo cual haría el proceso de transición mucho más dispendioso; el plan de direccionamiento deberá adaptarse completamente a la topología elegida para la transición y cada VLAN dentro de la red local deberá tener su subred IPv4 e IPv6 asociada, el prefijo IPv6 se recomienda ser solicitado ante LACNIC para no depender del ISP.

En cuanto a la etapa de pruebas, lo que recomiendan los lineamientos es garantizar la compatibilidad de los servicios y aplicaciones en IPv6 en un ambiente doble pila, pero más allá de esto, se sugiere, como se hizo en este proyecto, hacer pruebas de rendimiento donde se repliquen los procesos críticos de cada servicio o aplicación, dichas pruebas se deberán hacer en los tres ambientes y garantizar rendimientos similares o superiores bajo IPv6 en comparación con IPv4, si esto no ocurre, se recomienda buscar alternativas a la aplicación o servicio específico bajo el plan de manejo de excepciones, las cuales pueden ir desde la actualización del software hasta el cambio de la aplicación por otra similar que garantice un rendimiento adecuado en IPv6, mientras tanto dicha aplicación o servicio deberá seguir funcionando bajo IPv4 para no afectar la experiencia de usuario.

Las herramientas específicas para testear aplicaciones o en su defecto las herramientas de generación y captura de tráfico nos permiten realizar mediciones más precisas con el fin de comparar el rendimiento de los servicios o aplicaciones bajo ambos protocolos, se recomienda su uso para determinar si los procesos críticos de las aplicaciones tienen un rendimiento similar en IPv6 al experimentado en IPv4.

8 TRABAJOS FUTUROS

Este trabajo se orientó a servicios implementados On Premise, una posible extensión de este trabajo es recrear este escenario en un ambiente de nube pública o privada, siempre que se tenga un canal WAN y aplicaciones específicas que soporten IPv6. Servicios como WEB, Correo Electrónico y Active Directory son cada vez más comunes en un escenario nube y sería importante medir el rendimiento en este escenario.

Las métricas consideradas en este trabajo se obtuvieron del lado del cliente y se enfocaron en determinar la experiencia de usuario en un ambiente donde el volumen de tráfico generado no afectara de sobremanera el rendimiento del servidor. Un posible trabajo que se puede desarrollar es evaluar el rendimiento de un servidor con recursos específicos y observar si su rendimiento y capacidad de respuesta ante una carga elevada difiere de acuerdo con el protocolo IP utilizado. Para lo anterior se hace necesario el uso de simuladores de carga con soporte para los servicios específicos en ambos protocolos. Soluciones como TRex de Cisco e IXLoad de Ixia pueden ser candidatas para dichas simulaciones, pero debería considerarse si su costo se ajusta al presupuesto del proyecto.

Otros proyectos que se pueden desarrollar a partir de este trabajo son las pruebas de compatibilidad y rendimiento en ambientes doble pila de aplicaciones corporativas específicas de cada organización tales como CRM, ERP, entre otros que utilicen los servicios base analizados en este proyecto como Directorio Activo, DNS y WEB.

9 REFERENCIAS

[1] MINTIC, *Resolución 2710 de 2017*. Colombia, 2017, p. 4.

[2] MINTIC, “Guía de Transición de IPv4 a IPv6 para Colombia,” 2017. Accessed: May 06, 2020. [Online]. Available: http://www.mintic.gov.co/gestionti/615/articles-5482_G20_Transicion_IPv4_IPv6.pdf.

[3] F. Siddika, M. A. Hossen, and S. Saha, “Transition from IPv4 to IPv6 in Bangladesh: The competent and enhanced way to follow,” *Proc. 2017 Int. Conf. Networking, Syst. Secur. NSysS 2017*, pp. 174–179, 2017, doi: 10.1109/NSysS.2017.7885821.

[4] M. Nikkhah, R. Guerin, and M. Nikkhah, “Migrating the Internet to IPv6: An Exploration of the When and Why,” *IEEE/ACM Trans. Netw.*, vol. 24, no. 4, pp. 2291–2304, Aug. 2016, doi: 10.1109/TNET.2015.2453338.

[5] LACNIC, “Portal IPv6 - LACNIC,” 2020. https://www.lacnic.net/2942/1/lacnic/ (accessed May 06, 2020).

[6] GOOGLE, “IPv6 – Google,” 2020. https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption. (accessed Dec. 06, 2020).

[7] A. Baig, “IPv6 Campus Network Deployment Guidelines,” *Telecommun. Networks Appl. Conf. (ITNAC), 2016 26th Int.*, pp. 237–242, 2016.

[8] LACNIC, “Portal IPv6 - LACNIC,” 2020. https://www.lacnic.net/3042/1/lacnic/quienes-implementan (accessed May 06, 2020).

[9] IBM, “IBM Knowledge Center - Glosario,” 2018. https://www.ibm.com/support/knowledgecenter/es/SSBLQQ_9.0.0/com.ibm.rational.rit.ref.doc/topics/rit_glossary.html#gloss_E (accessed Apr. 10, 2018).

[10] LACNIC, “LACNIC Inicio,” 2020. https://www.lacnic.net/agotamiento (accessed May 06, 2020).

[11] APNIC, “IPv6 Measurement Maps,” 2020. https://stats.labs.apnic.net/ipv6 (accessed Dec. 06, 2020).

[12] Y. C. Kao, J. C. Liu, Y. Q. Ke, S. C. Tsai, and Y. B. Lin, “Dual-Stack Network Management through One-Time Authentication Mechanism,” *IEEE Access*, vol. 8, pp. 34706–34716, 2020, doi: 10.1109/ACCESS.2020.2974659.

[13] G. Huston, “In defence of NATs: An opinion,” in *2017 IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS 2017*, Nov. 2017, pp. 625–628, doi: 10.1109/INFCOMW.2017.8116449.

[14] P. Srisuresh and M. Holdrege, “IP Network Address Translator (NAT) Terminology and Considerations,” no. 2663. RFC Editor, Fremont, CA, USA, pp. 1–30, 1999, doi:

10.17487/RFC2663.

[15] P. Richter *et al.*, “A Multi-perspective Analysis of Carrier-Grade NAT Deployment,” in *Proceedings of the 2016 ACM on Internet Measurement Conference - IMC ’16*, 2016, pp. 215–229, doi: 10.1145/2987443.2987474.

[16] S. Deering and R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” no. 8200. RFC Editor, Fremont, CA, USA, pp. 1–42, 2017, doi: 10.17487/RFC8200.

[17] Y. Sookun and V. Bassoo, “Performance analysis of IPv4/IPv6 transition techniques,” *2016 IEEE Int. Conf. Emerg. Technol. Innov. Bus. Pract. Transform. Soc. EmergiTech 2016*, pp. 188–193, 2016, doi: 10.1109/EmergiTech.2016.7737336.

[18] R. Hinden and S. Deering, “IP Version 6 Addressing Architecture,” no. 4291. RFC Editor, Fremont, CA, USA, pp. 1–25, 2006, doi: 10.17487/RFC4291.

[19] S. Kawamura and M. Kawashima, “A Recommendation for IPv6 Address Text Representation,” no. 5952. RFC Editor, Fremont, CA, USA, pp. 1–14, 2010, doi: 10.17487/RFC5952.

[20] R. Hinden and B. Haberman, “Unique Local IPv6 Unicast Addresses,” no. 4193. RFC Editor, Fremont, CA, USA, pp. 1–16, 2005, doi: 10.17487/RFC4193.

[21] R. Droms, “Dynamic Host Configuration Protocol,” no. 2131. RFC Editor, Fremont, CA, USA, pp. 1–45, 1997, doi: 10.17487/RFC2131.

[22] S. Thomson, C. Huitema, V. Ksinant, and M. Souissi, “DNS Extensions to Support IP Version 6,” no. 3596. RFC Editor, Fremont, CA, USA, pp. 1–8, 2003, doi: 10.17487/RFC3596.

[23] S. Thomson and T. Narten, “IPv6 Stateless Address Autoconfiguration,” no. 2462. RFC Editor, Fremont, CA, USA, pp. 1–25, 1998, doi: 10.17487/RFC2462.

[24] R. Droms (Ed.), J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6),” no. 3315. RFC Editor, Fremont, CA, USA, pp. 1–101, 2003, doi: 10.17487/RFC3315.

[25] A. Binduf, H. O. Alamoudi, H. Balahmar, S. Alshamrani, H. Al-Omar, and N. Nagy, “Active Directory and Related Aspects of Security,” in *21st Saudi Computer Society National Computer Conference, NCC 2018*, Dec. 2018, pp. 4474–4479, doi: 10.1109/NCG.2018.8593188.

[26] S. Singalar and R. M. Banakar, “Performance Analysis of IPv4 to IPv6 Transition Mechanisms,” in *Proceedings - 2018 4th International Conference on Computing, Communication Control and Automation, ICCUBEA 2018*, Jul. 2018, pp. 1–6, doi: 10.1109/ICCUBEA.2018.8697539.

[27] Y. Yang, Z. Wei, and B. Hong, “Research on IPv6 Transition Technology for Digital Ocean,” in *2018 IEEE 4th International Conference on Computer and Communications (ICCC)*, Dec. 2018, pp. 317–320, doi:

10.1109/CompComm.2018.8780871.

[28] “Dual stack o pila doble,” 2020. https://www.lacnic.net/3091/1/lacnic/dual-stack-o-pila-doble (accessed May 07, 2020).

[29] D. Schinazi and T. Pauly, “Happy Eyeballs Version 2: Better Connectivity Using Concurrency,” no. 8305. RFC Editor, Fremont, CA, USA, pp. 1–15, 2017, doi: 10.17487/RFC8305.

[30] P. Dell, “On the dual-stacking transition to IPv6: A forlorn hope?,” *Telecommunications Policy*, vol. 42, no. 7. Elsevier Ltd, pp. 575–581, Aug. 01, 2018, doi: 10.1016/j.telpol.2018.04.005.

[31] LACNIC, “Túneles/Encapsulamiento,” 2020. https://www.lacnic.net/3092/1/lacnic/ (accessed May 15, 2020).

[32] LACNIC, “Traducción,” 2020. https://www.lacnic.net/3093/1/lacnic/traduccion (accessed May 07, 2020).

[33] M. Pinedo Vidal, “Ley 603 de 2000,” 2000, Accessed: May 07, 2020. [Online]. Available: http://derechodeautor.gov.co/documents/10181/182597/603.pdf/42c15f4a-afe5-4339-97ca-a61026450307.

[34] I. Livadariu, K. Benson, A. Elmokashfi, A. Dhamdhere, and A. Dainotti, “Inferring Carrier-Grade NAT Deployment in the Wild,” in *Proceedings - IEEE INFOCOM*, Oct. 2018, vol. 2018-April, pp. 2249–2257, doi: 10.1109/INFOCOM.2018.8486223.

[35] M. Nikkhah, “Maintaining the progress of IPv6 adoption,” *Comput. Networks*, vol. 102, pp. 50–69, 2016, doi: 10.1016/j.comnet.2016.02.027.

[36] V. Bajpai and J. Schonwalder, “A Longitudinal View of Dual-Stacked Websites - Failures, Latency and Happy Eyeballs,” *IEEE/ACM Trans. Netw.*, vol. 27, no. 2, pp. 577–590, Apr. 2019, doi: 10.1109/TNET.2019.2895165.

[37] A. Hamarsheh and Y. Abdalaziz, “Transition to IPv6 Protocol, Where We Are?,” in *2019 International Conference on Computer and Information Sciences, ICCIS 2019*, May 2019, pp. 1–6, doi: 10.1109/ICCISci.2019.8716482.

[38] K. Chittimaneni, T. Chown, L. Howard, V. Kuarsingh, Y. Pouffary, and E. Vyncke, “Enterprise IPv6 Deployment Guidelines,” no. 7381. RFC Editor, Fremont, CA, USA, pp. 1–34, 2014, doi: 10.17487/RFC7381.

[39] R. K. Cv and H. Goyal, “IPv4 to IPv6 Migration and Performance Analysis using GNS3 and Wireshark,” in *Proceedings - International Conference on Vision Towards Emerging Trends in Communication and Networking, ViTECoN 2019*, Mar. 2019, pp. 1–6, doi: 10.1109/ViTECoN.2019.8899746.

[40] D. Wing and A. Yourtchenko, “Happy Eyeballs: Success with Dual-Stack Hosts,” no. 6555. RFC Editor, Fremont, CA, USA, pp. 1–15, 2012, doi: 10.17487/RFC6555.

[41] V. Bajpai and J. Schönwälder, “Measuring the Effects of Happy Eyeballs,” in

Proceedings of the 2016 workshop on Applied Networking Research Workshop - ANRW 16, 2016, pp. 38–44, doi: 10.1145/2959424.2959429.

[42] W. M. N. W. Mahmud, R. A. Rahman, M. Kassim, and M. I. Yusof, “Performance comparison analysis of E2E Dual-Stack IP protocol method over wired and Wi-Fi broadband access,” *Proc. 2016 6th Int. Conf. Syst. Eng. Technol. ICSET 2016*, pp. 7–12, 2017, doi: 10.1109/FIT.2016.7857509.

[43] L. Hendriks, P. De Boer, and A. Pras, “IPv6-specific Misconfigurations in the DNS,” 2017.

[44] S. Malay and S. Kuncha, “Q-DNS: Optimized Network Lookup for Dual Stack Devices,” in *2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, 2018, pp. 992–997, doi: 10.1109/HPCC/SmartCity/DSS.2018.00164.

[45] S. J. Eravuchira, V. Bajpai, J. Schonwalder, and S. Crawford, “Measuring web similarity from dual-stacked hosts,” in *2016 12th International Conference on Network and Service Management, CNSM 2016 and Workshops, 3rd International Workshop on Management of SDN and NFV, ManSDN/NFV 2016, and International Workshop on Green ICT and Smart Networking, GISN 2016*, Jan. 2017, pp. 181–187, doi: 10.1109/CNSM.2016.7818415.

[46] G. E. Jerez, V. J. López, and V. M. Longo, “Técnicas para el despliegue de ipv6 en redes lan: laboratorios de auto-configuración utilizando RDNSS y DHCPV6,” *Rev. Difusiones*, vol. 17, pp. 273–286, 2019.

[47] L. Li, G. Ren, Y. Liu, and J. Wu, “Secure DHCPv6 mechanism for DHCPv6 security and privacy protection,” *Tsinghua Sci. Technol.*, vol. 23, no. 1, pp. 13–21, Feb. 2018, doi: 10.26599/TST.2018.9010020.

[48] A. Al-Ani, M. Anbar, I. H. Hasbullah, R. Abdullah, and A. K. Al-Ani, “Authentication and Privacy Approach for DHCPv6,” *IEEE Access*, vol. 7, pp. 73144–73156, 2019, doi: 10.1109/ACCESS.2019.2919966.

[49] Stat Counter, “Desktop Operating System Market Share Worldwide | StatCounter Global Stats,” *2020*. https://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-201904-202004 (accessed May 14, 2020).

[50] Statista, “Global server share by OS 2018-2019,” 2020. https://www.statista.com/statistics/915085/global-server-share-by-os/ (accessed May 11, 2020).

[51] “Best Server Virtualization Software in 2020 | G2.” https://www.g2.com/categories/server-virtualization#grid (accessed May 14, 2020).

[52] LACNIC, “LACNIC Solicitar Recursos.” https://www.lacnic.net/978/1/lacnic/solicitar-recursos (accessed Feb. 15, 2021).

[53] OS-TEMPLATES.COM, “Pentwist Website Template | Free Website Templates | OS Templates,” 2020. https://www.os-templates.com/free-website-templates/pentwist (accessed Jun. 07, 2020).

[54] “hMailServer - Free open source email server for Microsoft Windows.” https://www.hmailserver.com/ (accessed Jun. 16, 2020).

ANEXO 1

RESULTADOS PRUEBAS DE FUNCIONALIDAD

Pruebas de conectividad

```
C:\Users\administrador.DSIPV6>ping 192.168.120.50 -n 2

Haciendo ping a 192.168.120.50 con 32 bytes de datos:
Respuesta desde 192.168.120.50: bytes=32 tiempo<1m TTL=127
Respuesta desde 192.168.120.50: bytes=32 tiempo=1ms TTL=127

Estadísticas de ping para 192.168.120.50:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\administrador.DSIPV6>ping FD55:1B94:C90A:C0::AA -n 2

Haciendo ping a fd55:1b94:c90a:c0::aa con 32 bytes de datos:
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.

Estadísticas de ping para fd55:1b94:c90a:c0::aa:
    Paquetes: enviados = 2, recibidos = 0, perdidos = 2
    (100% perdidos),
```

```
C:\Users\administrador.DSIPV6>ping FD55:1B94:C90A:C0::AA -n 2

Haciendo ping a fd55:1b94:c90a:c0::aa con 32 bytes de datos:
Respuesta desde fd55:1b94:c90a:c0::aa: tiempo<1m
Respuesta desde fd55:1b94:c90a:c0::aa: tiempo<1m

Estadísticas de ping para fd55:1b94:c90a:c0::aa:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\administrador.DSIPV6>ping 192.168.120.50 -n 2

Haciendo ping a 192.168.120.50 con 32 bytes de datos:
PING: error en la transmisión. Error general.
PING: error en la transmisión. Error general.

Estadísticas de ping para 192.168.120.50:
    Paquetes: enviados = 2, recibidos = 0, perdidos = 2
    (100% perdidos),
```

```
C:\Users\administrador.DSIPV6>ping 192.168.120.50 -n 2

Haciendo ping a 192.168.120.50 con 32 bytes de datos:
Respuesta desde 192.168.120.50: bytes=32 tiempo<1m TTL=127
Respuesta desde 192.168.120.50: bytes=32 tiempo<1m TTL=127

Estadísticas de ping para 192.168.120.50:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\administrador.DSIPV6>ping FD55:1B94:C90A:C0::AA -n 2

Haciendo ping a fd55:1b94:c90a:c0::aa con 32 bytes de datos:
Respuesta desde fd55:1b94:c90a:c0::aa: tiempo<1m
Respuesta desde fd55:1b94:c90a:c0::aa: tiempo<1m

Estadísticas de ping para fd55:1b94:c90a:c0::aa:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\administrador.DSIPV6>ping DCIPV6 -n 2

Haciendo ping a DCIPv6.DSIPv6.local [fd55:1b94:c90a:c0::aa] con 32 bytes de datos:
Respuesta desde fd55:1b94:c90a:c0::aa: tiempo<1m
Respuesta desde fd55:1b94:c90a:c0::aa: tiempo<1m

Estadísticas de ping para fd55:1b94:c90a:c0::aa:
    Paquetes: enviados = 2, recibidos = 2, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

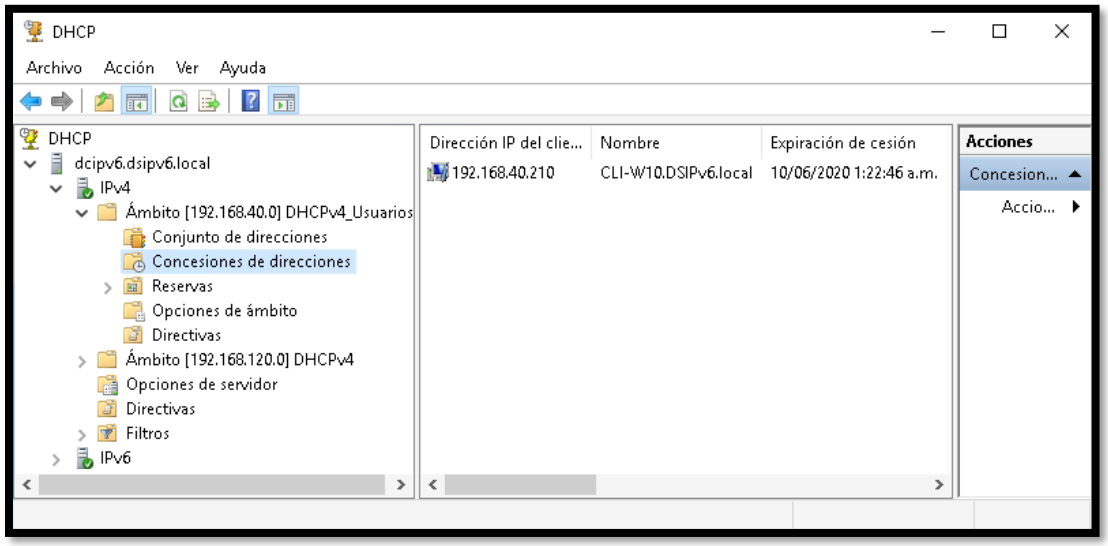
Pruebas de servicio DNS

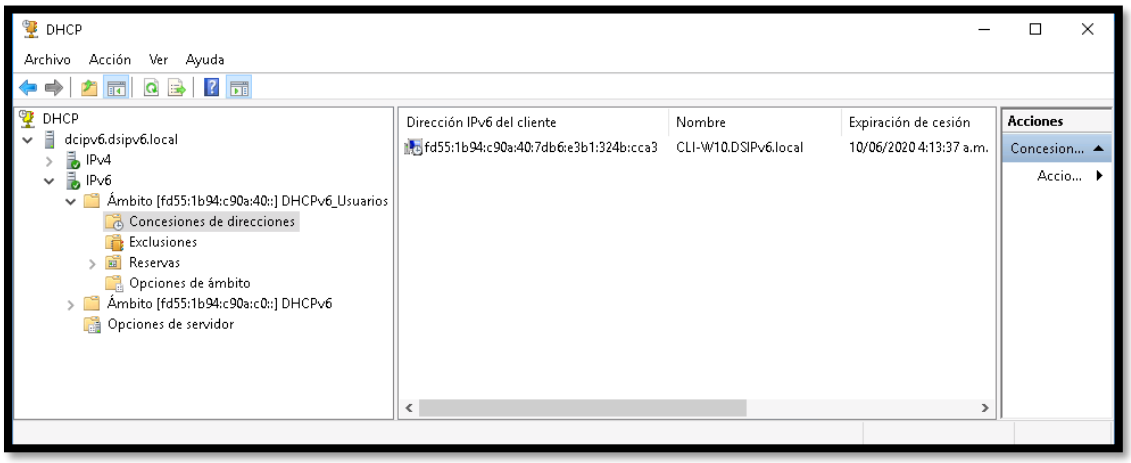
```
C:\Users\administrador.DSIPV6>nslookup
Servidor predeterminado:  dcipv6.DSIPv6.local
Address:  fd55:1b94:c90a:c0::aa

> dcipv6
Servidor:  dcipv6.DSIPv6.local
Address:  fd55:1b94:c90a:c0::aa

Nombre:  dcipv6.DSIPv6.local
Addresses:  fd55:1b94:c90a:c0::aa
          192.168.120.50

> 192.168.120.50
Servidor:  dcipv6.DSIPv6.local
Address:  fd55:1b94:c90a:c0::aa

Nombre:  DCIPv6.DSIPv6.local
Address:  192.168.120.50

> fd55:1b94:c90a:c0::aa
Servidor:  dcipv6.DSIPv6.local
Address:  fd55:1b94:c90a:c0::aa

Nombre:  dcipv6.DSIPv6.local
Address:  fd55:1b94:c90a:c0::aa
```

```
C:\Users\administrador.DSIPV6>ping dcipv6 -4

Haciendo ping a DCIPV6.DSIPv6.local [192.168.120.50] con 32 bytes de datos:
Respuesta desde 192.168.120.50: bytes=32 tiempo<1m TTL=127
Respuesta desde 192.168.120.50: bytes=32 tiempo<1m TTL=127
Respuesta desde 192.168.120.50: bytes=32 tiempo<1m TTL=127
Respuesta desde 192.168.120.50: bytes=32 tiempo<1m TTL=127

Estadísticas de ping para 192.168.120.50:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\administrador.DSIPV6>ping dcipv6 -6

Haciendo ping a dcipv6.DSIPv6.local [fd55:1b94:c90a:c0::aa] con 32 bytes de datos:
Respuesta desde fd55:1b94:c90a:c0::aa: tiempo<1m
Respuesta desde fd55:1b94:c90a:c0::aa: tiempo<1m
Respuesta desde fd55:1b94:c90a:c0::aa: tiempo<1m
Respuesta desde fd55:1b94:c90a:c0::aa: tiempo<1m

Estadísticas de ping para fd55:1b94:c90a:c0::aa:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

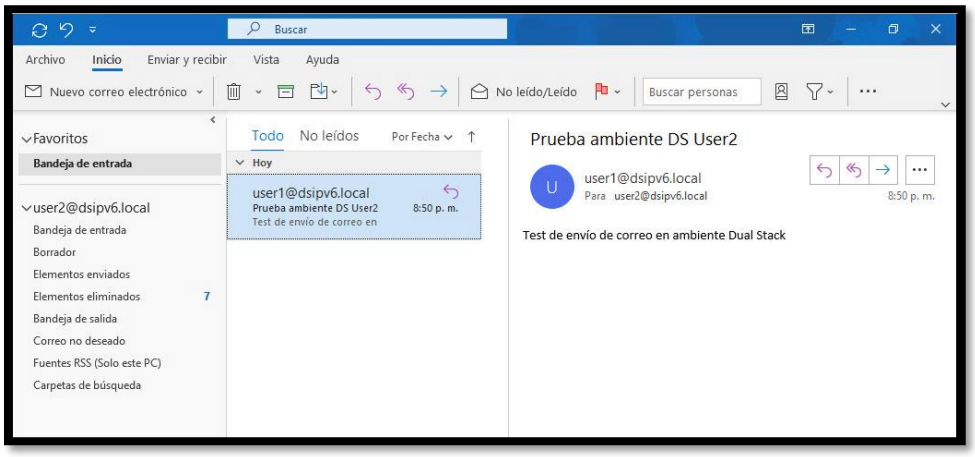
Pruebas de servicio DHCP

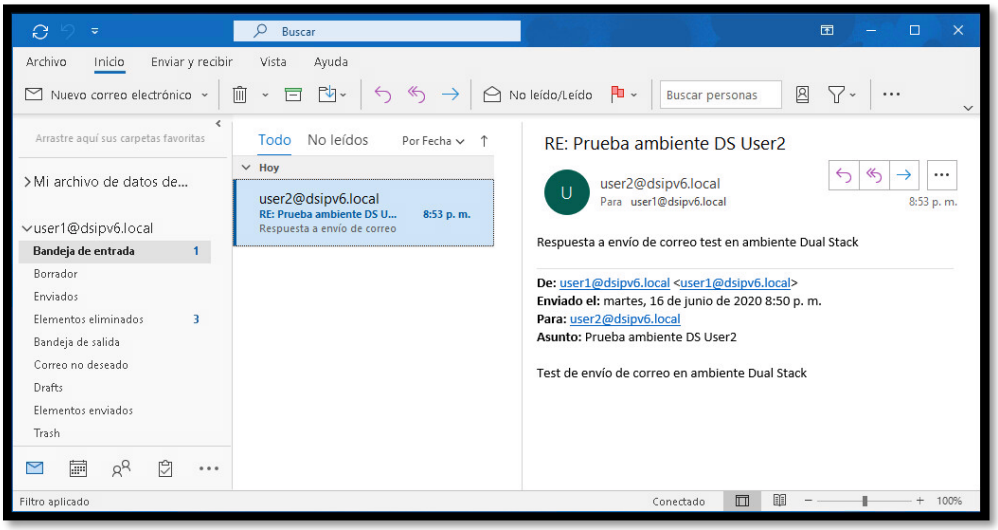
```
C:\Users\administrador.DSIPV6>ipconfig

Configuración IP de Windows


Adaptador de Ethernet Ethernet1:

   Sufijo DNS específico para la conexión. . : DSIPv6.local
   Dirección IPv6 . . . . . . . . . . . . . : fd55:1b94:c90a:40:7db6:e3b1:324b:cca3
   Vínculo: dirección IPv6 local. . . . . . : fe80::f586:d6e3:965e:6d94%6
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.40.210
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::926c:acff:febc:8c7a%6
                                               192.168.40.1

Adaptador de túnel isatap.DSIPv6.local:

   Estado de los medios. . . . . . . . . . . : medios desconectados
   Sufijo DNS específico para la conexión. . : DSIPv6.local
```


DHCP
Archivo Acción Ver Ayuda
DHCP
dcipv6.dsipv6.local
IPv4
Ámbito [192.168.40.0] DHCPv4_Usuarios
Conjunto de direcciones
Concesiones de direcciones
Reservas
Opciones de ámbito
Directivas
Ámbito [192.168.120.0] DHCPv4
Opciones de servidor
Directivas
Filtros
IPv6
Dirección IP del clie...
Nombre
Expiración de cesión
192.168.40.210
CLI-W10.DSIPv6.local
10/06/2020 1:22:46 a.m.
Acciones
Concesion...
Accio...

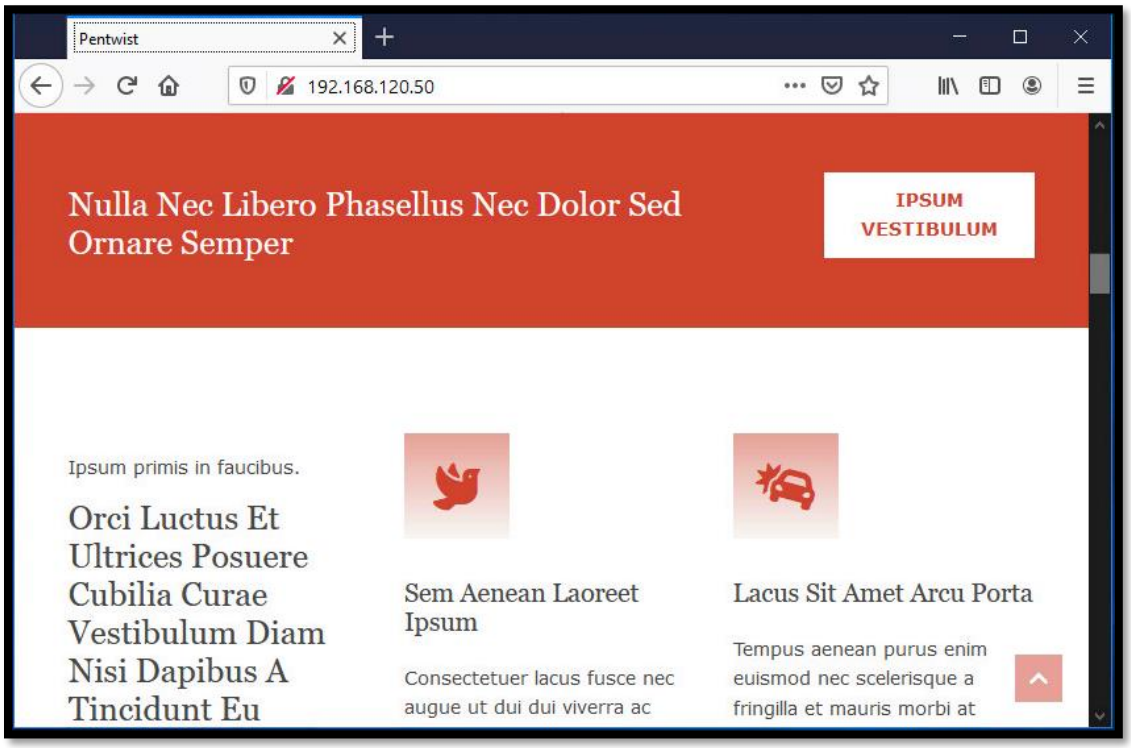

DHCP
Archivo Acción Ver Ayuda
DHCP
dcipv6.dsipv6.local
IPv4
IPv6
Ámbito [fd55:1b94:c90a:40::] DHCPv6_Usuarios
Concesiones de direcciones
Exclusiones
Reservas
Opciones de ámbito
Ámbito [fd55:1b94:c90a:c0::] DHCPv6
Opciones de servidor
Dirección IPv6 del cliente
Nombre
Expiración de cesión
fd55:1b94:c90a:40:7db6:e3b1:324b:cca3
CLI-W10.DSIPv6.local
10/06/2020 4:13:37 a.m.
Acciones
Concesion...
Accio...

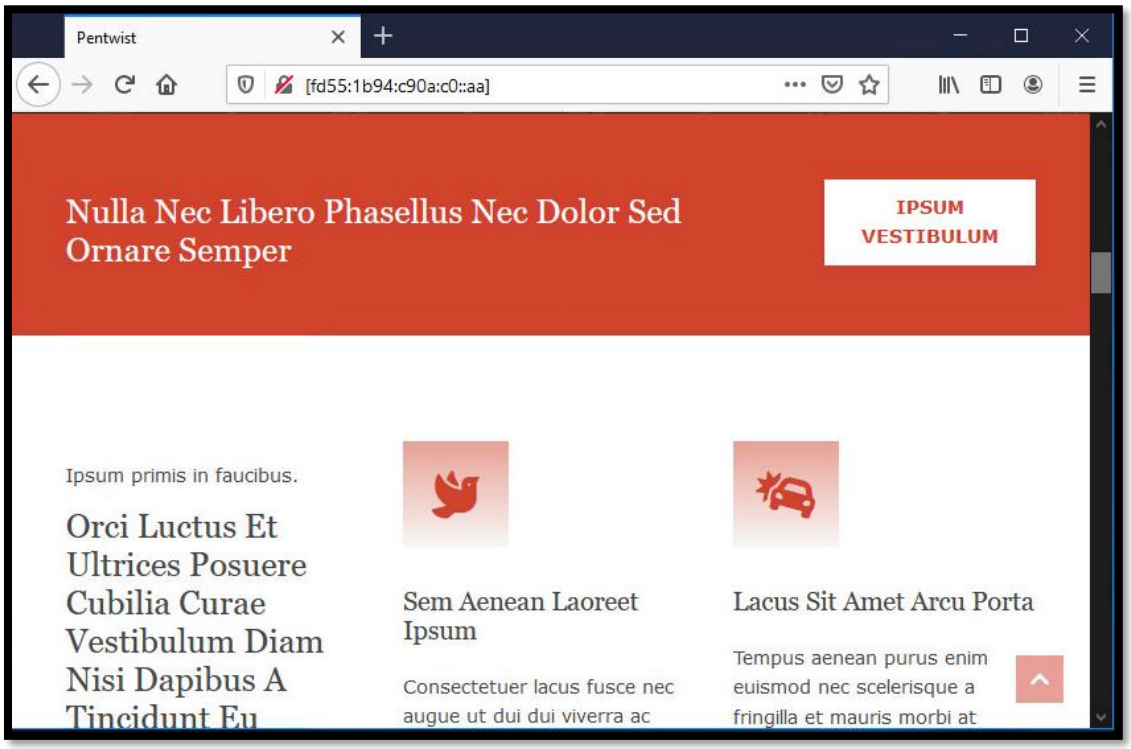
Pruebas de servicio de correo electrónico

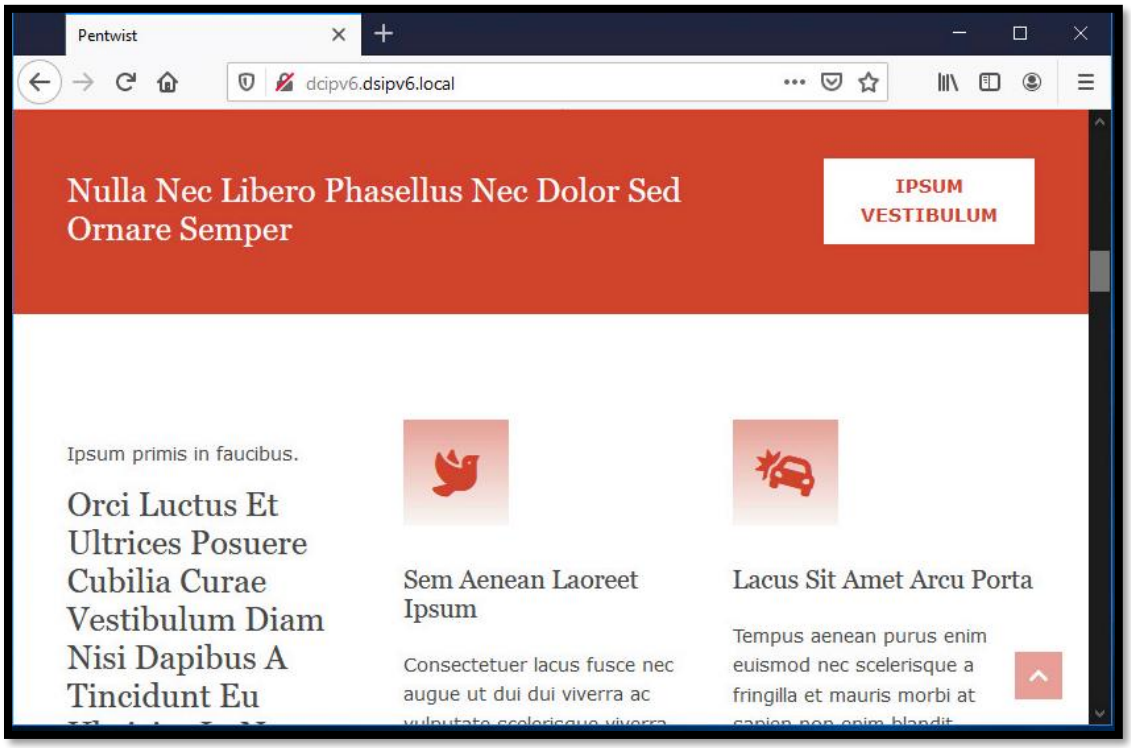




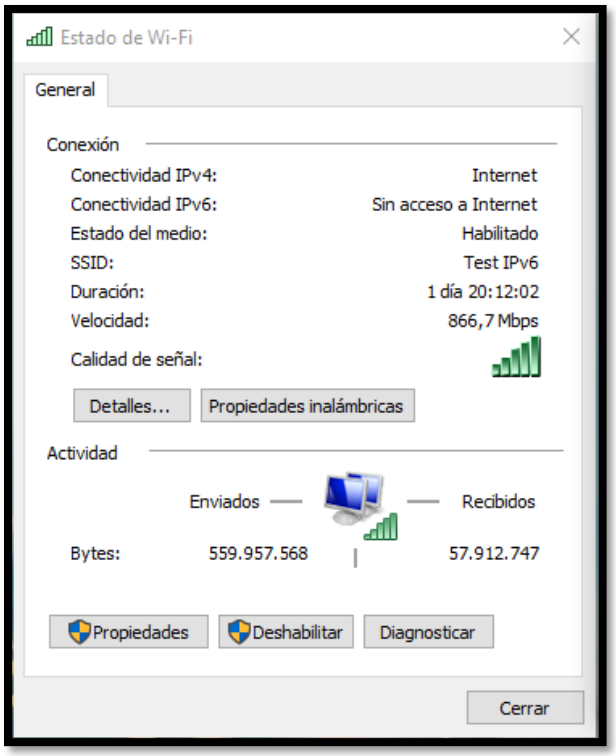
Pruebas de servicio WEB

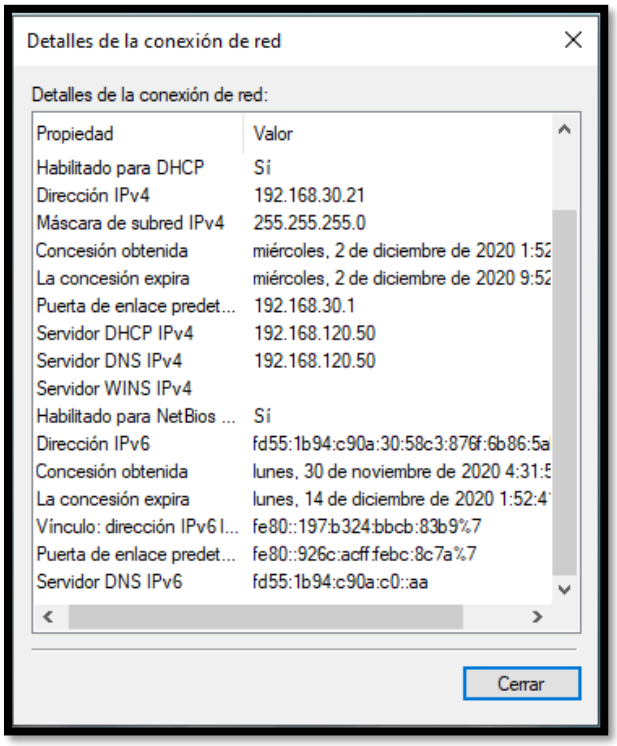


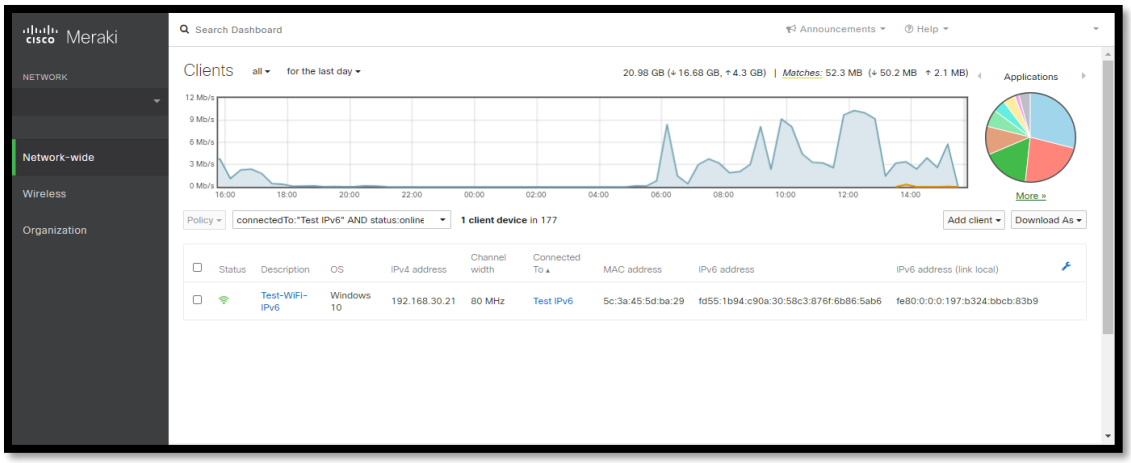




Prueba de servicio WiFi



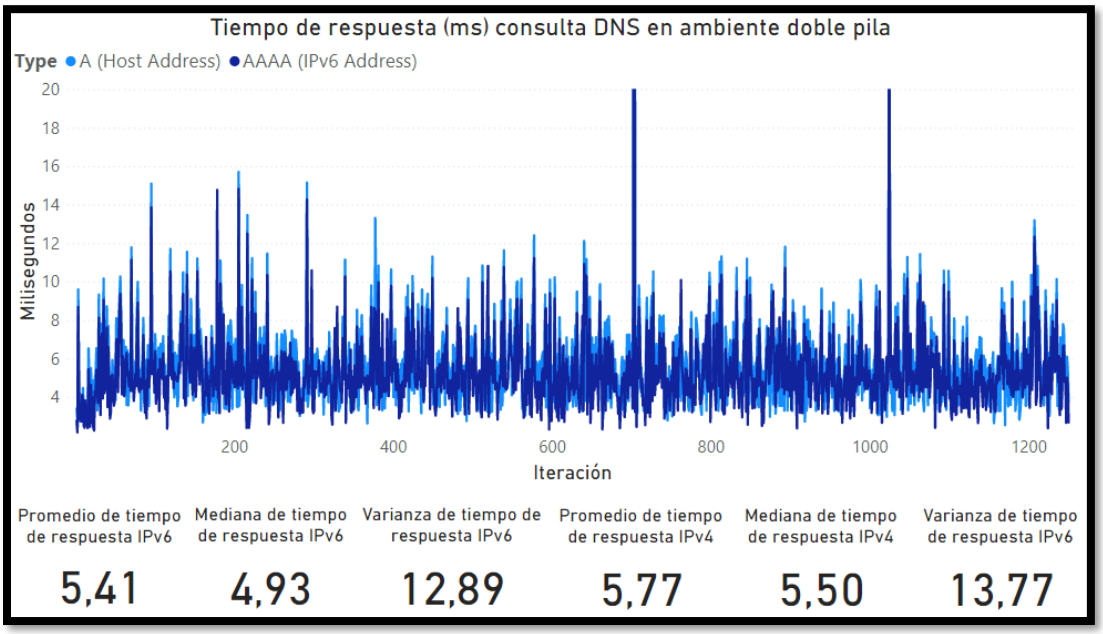

Detalles de la conexión de red
Detalles de la conexión de red:
Propiedad
Valor
Habilitado para DHCP
Sí
Dirección IPv4
192.168.30.21
Máscara de subred IPv4
255.255.255.0
Concesión obtenida
miércoles, 2 de diciembre de 2020 1:52
La concesión expira
miércoles, 2 de diciembre de 2020 9:52
Puerta de enlace predet...
192.168.30.1
Servidor DHCP IPv4
192.168.120.50
Servidor DNS IPv4
192.168.120.50
Servidor WINS IPv4
Habilitado para NetBios ...
Sí
Dirección IPv6
fd55:1b94:c90a:30:58c3:876f:6b86:5a
Concesión obtenida
lunes, 30 de noviembre de 2020 4:31:5
La concesión expira
lunes, 14 de diciembre de 2020 1:52:4
Vínculo: dirección IPv6 l...
fe80::197:b324:bbcb:83b9%7
Puerta de enlace predet...
fe80::926c:acff:febc:8c7a%7
Servidor DNS IPv6
fd55:1b94:c90a:c0::aa
Cerrar

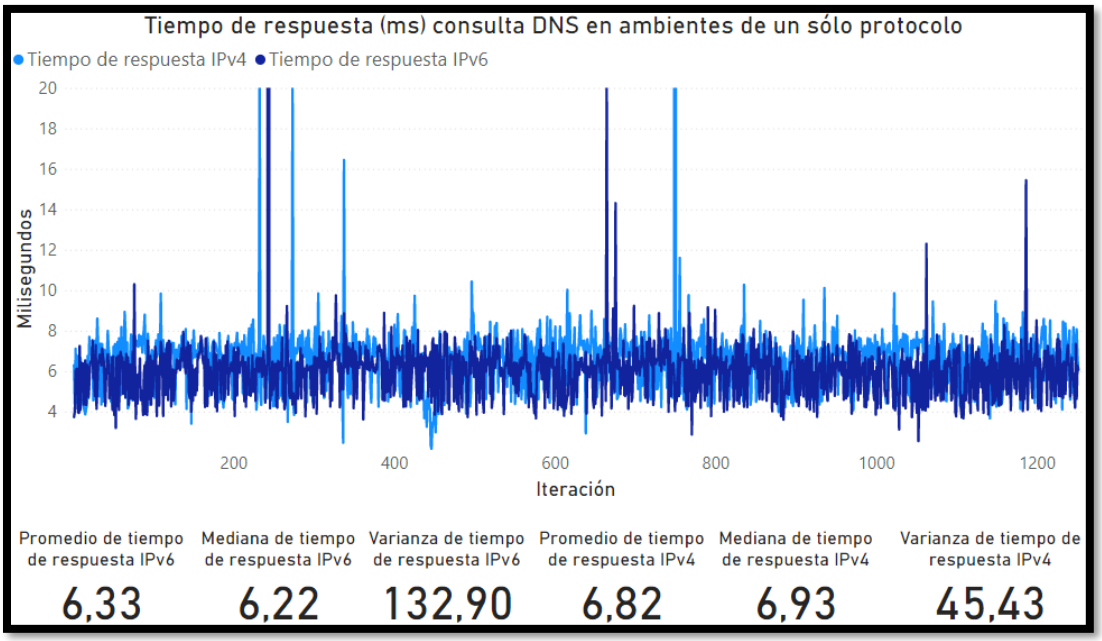

Meraki
Search Dashboard
Announcements
Help
NETWORK
Network-wide
Wireless
Organization
Clients
all
for the last day
20.98 GB (↓ 16.68 GB, ↑ 4.3 GB) | Matches: 52.3 MB (↓ 50.2 MB ↑ 2.1 MB)
Applications
12 Mb/s
9 Mb/s
6 Mb/s
3 Mb/s
0 Mb/s
16:00
18:00
20:00
22:00
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
More »
Policy
connectedTo:"Test IPv6" AND status:online
1 client device in 177
Add client
Download As
Status
Description
OS
IPv4 address
Channel width
Connected To
MAC address
IPv6 address
IPv6 address (link local)
Test-WiFi-IPv6
Windows 10
192.168.30.21
80 MHz
Test IPv6
5c:3a:45:5d:ba:29
fd55:1b94:c90a:30:58c3:876f:6b86:5ab6
fe80:0:0:0:197:b324:bbcb:83b9

ANEXO 2

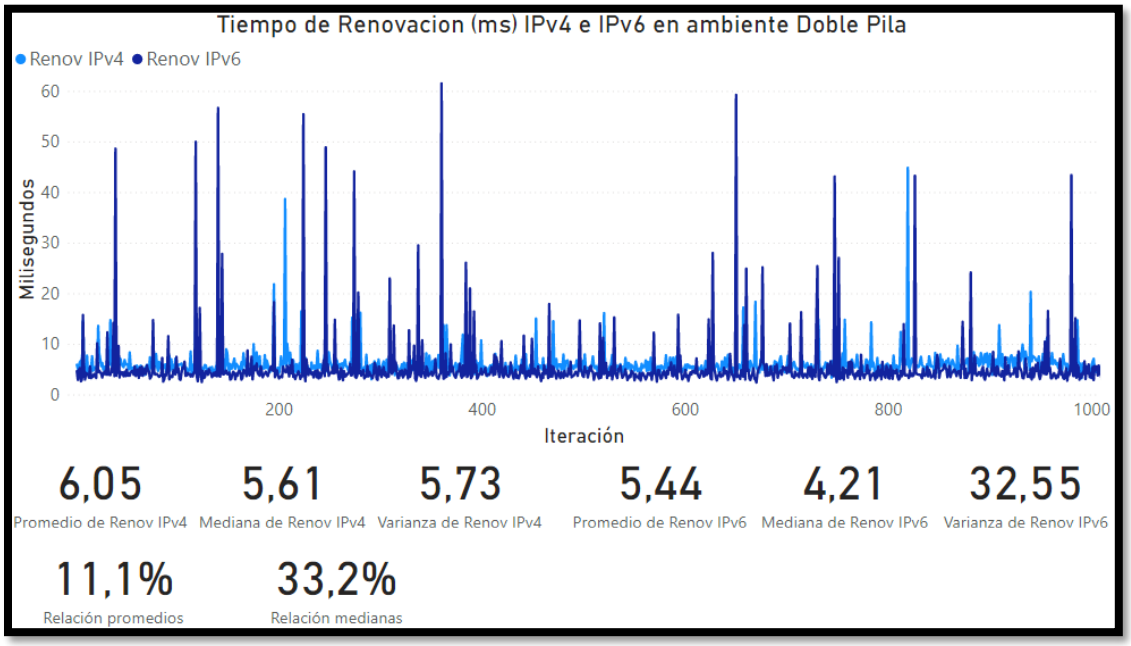
RESULTADOS PRUEBAS DE RENDIMIENTO EN AMBIENTE WIRELESS

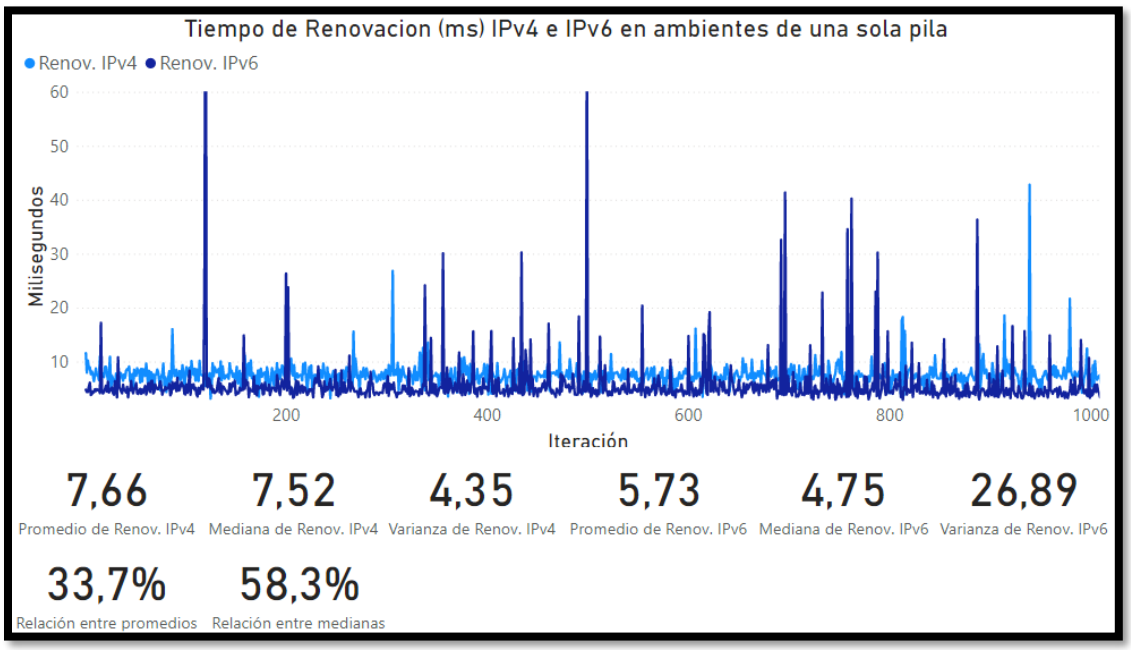
Servicio DNS



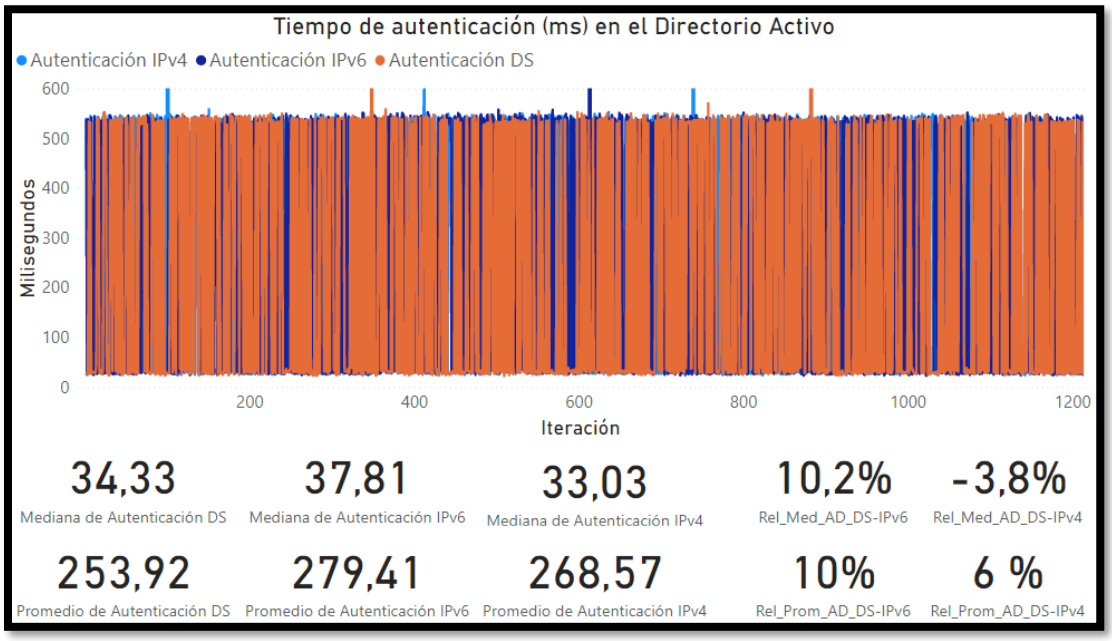


Servicio DHCP

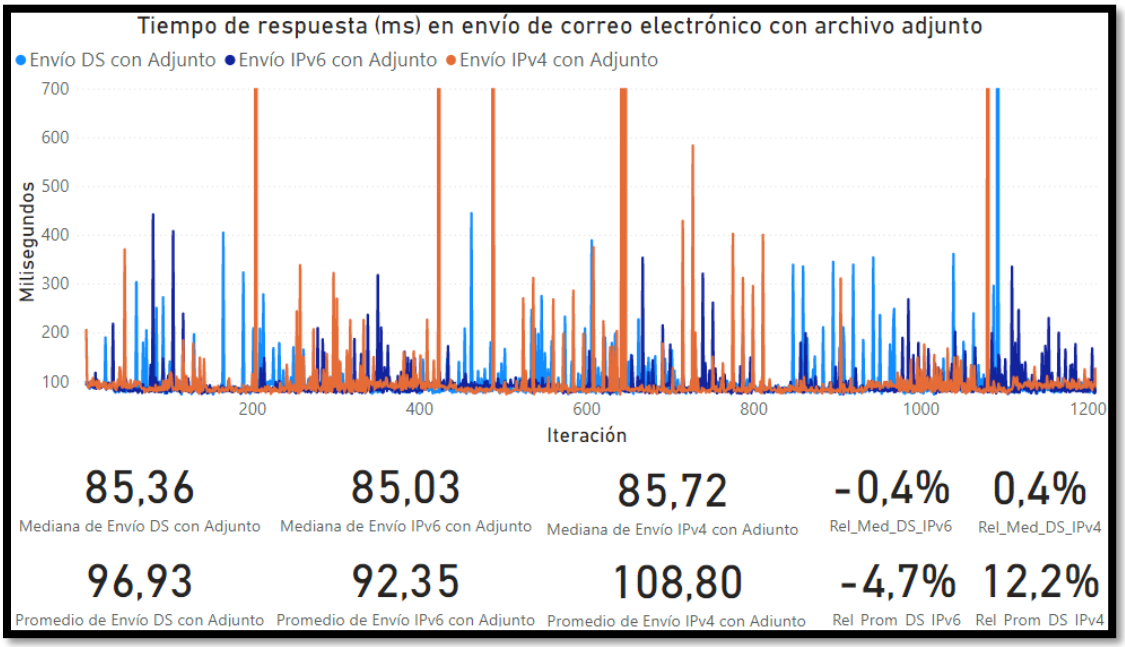


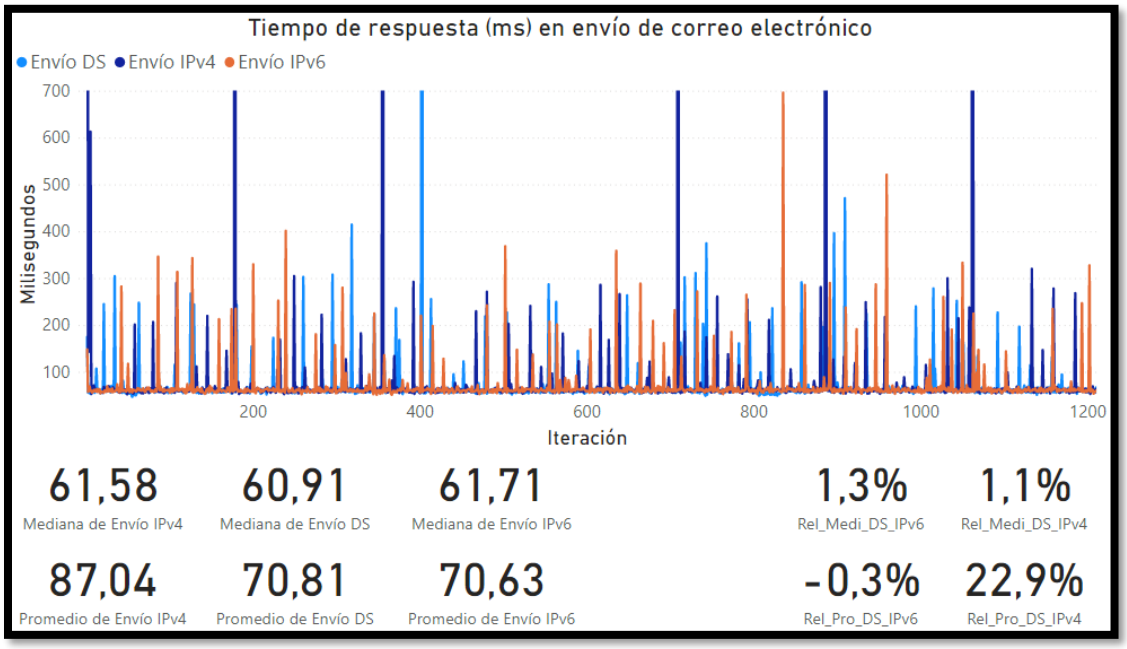


Servicio de Directorio Activo

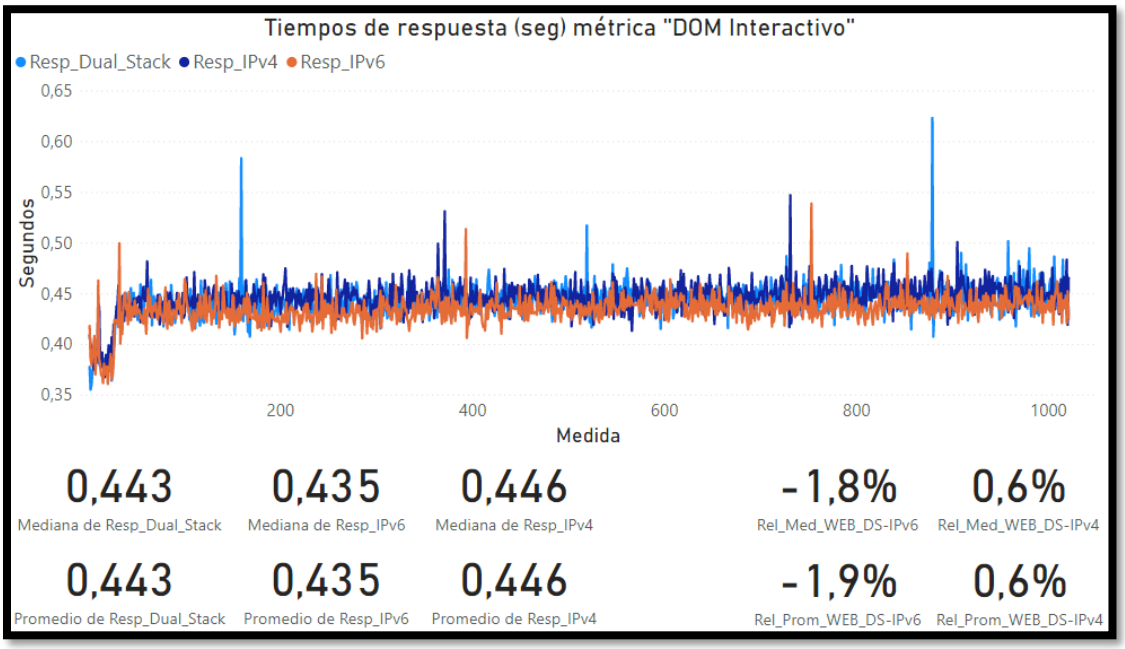


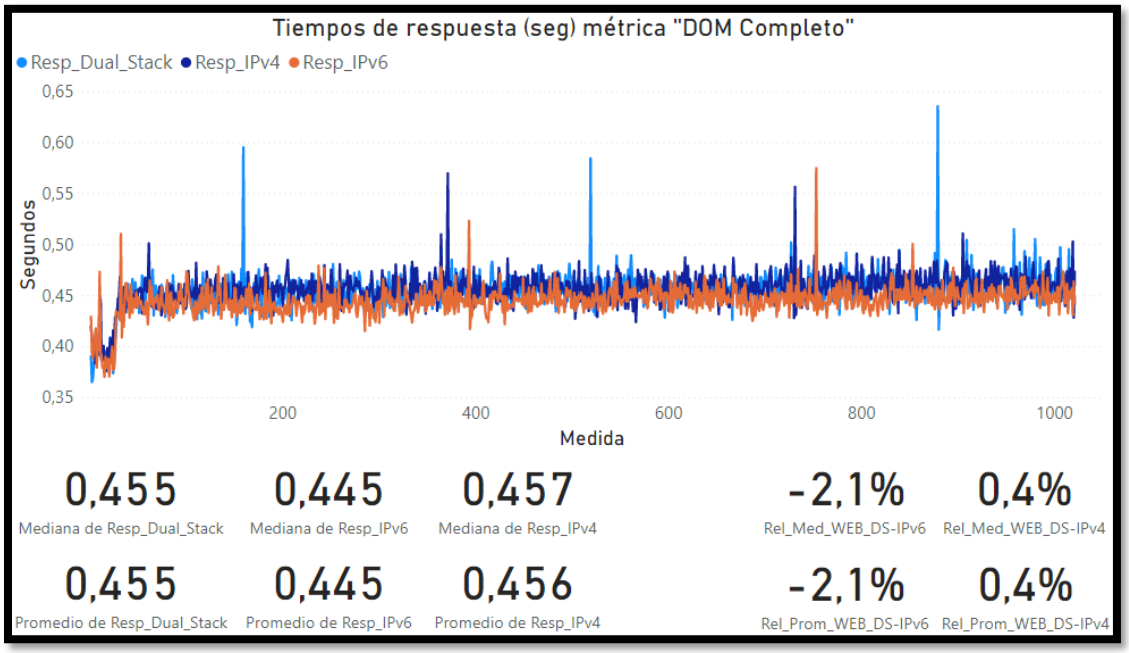
Servicio de Correo Electrónico

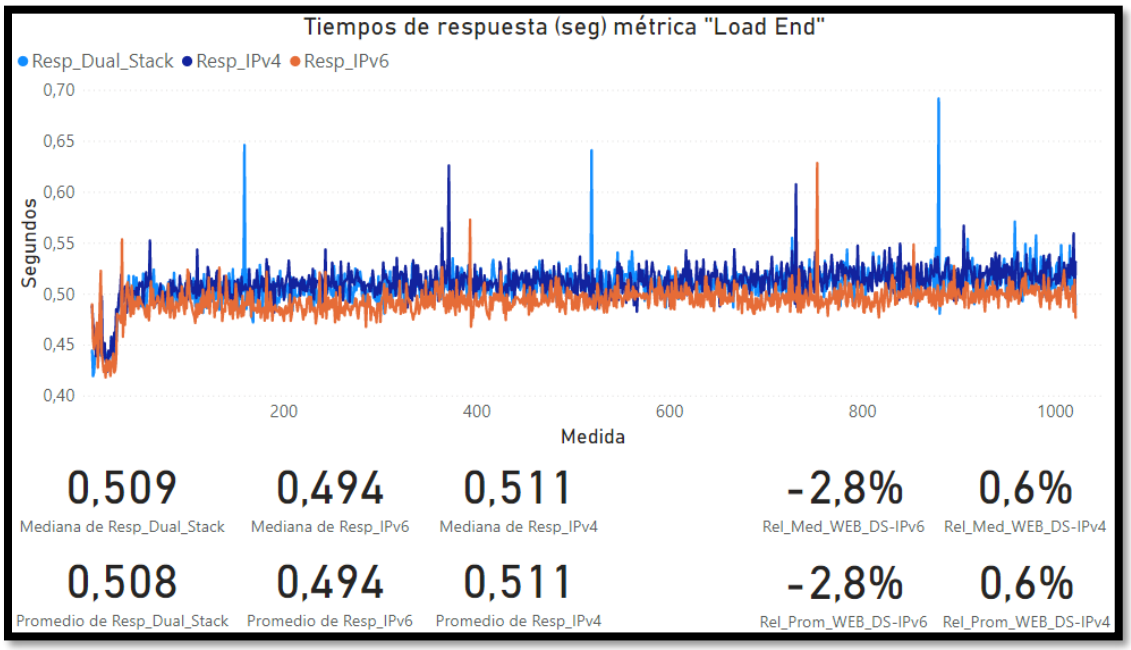




Servicio WEB




Tiempos de respuesta (seg) métrica "DOM Completo"
Resp_Dual_Stack
Resp_IPv4
Resp_IPv6
Segundos
0,65
0,60
0,55
0,50
0,45
0,40
0,35
200
400
600
800
1000
Medida
0,455
Mediana de Resp_Dual_Stack
0,445
Mediana de Resp_IPv6
0,457
Mediana de Resp_IPv4
-2,1%
Rel_Med_WEB_DS-IPv6
0,4%
Rel_Med_WEB_DS-IPv4
0,455
Promedio de Resp_Dual_Stack
0,445
Promedio de Resp_IPv6
0,456
Promedio de Resp_IPv4
-2,1%
Rel_Prom_WEB_DS-IPv6
0,4%
Rel_Prom_WEB_DS-IPv4


Tiempos de respuesta (seg) métrica "Load End"
Resp_Dual_Stack
Resp_IPv4
Resp_IPv6
Segundos
0,70
0,65
0,60
0,55
0,50
0,45
0,40
200
400
600
800
1000
Medida
0,509
Mediana de Resp_Dual_Stack
0,494
Mediana de Resp_IPv6
0,511
Mediana de Resp_IPv4
-2,8%
Rel_Med_WEB_DS-IPv6
0,6%
Rel_Med_WEB_DS-IPv4
0,508
Promedio de Resp_Dual_Stack
0,494
Promedio de Resp_IPv6
0,511
Promedio de Resp_IPv4
-2,8%
Rel_Prom_WEB_DS-IPv6
0,6%
Rel_Prom_WEB_DS-IPv4