# ESTUDIO DE FACTIBILIDAD PARA LA TRANSICIÓN DEL PROTOCOLO IPV4 AL PROTOCOLO IPV6 EN LA COMPAÑIA GAMMA INGENIEROS.

**YEISON ALEXANDER ZAMORA GUTIERREZ**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD**
**ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA**
**PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES**
**BOGOTÁ**
**2020**

# ESTUDIO DE FACTIBILIDAD PARA LA TRANSICIÓN DEL PROTOCOLO IPV4 AL PROTOCOLO IPV6 EN LA COMPAÑIA GAMMA INGENIEROS.

**ESTUDIANTE**
**YEISON ALEXANDER ZAMORA GUTIERREZ**

**PRESENTADO A**
**MANUEL ENRIQUE WAGNER MENDIVELSO**
**MAGISTER EN INGENIERÍA ELECTRÓNICA**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD**
**INGENIERIA DE TELECOMUNICACIONES**
**BOGOTA DC**
**2020**

**PAGINA DE ACEPTACION**

**Nota de aceptación**

_____

_____

_____

_____

_____

**Jurado**

_____

**Jurado**

**Agradecimientos**

Agradezco a la Universidad Nacional Abierta y a Distancia – UNAD, por haber encaminado mis deseos a fortalecer mi habilidades y capacidades no explotadas hasta ahora.

Muchas gracias a los tutores de la universidad, quienes permanecen al frente del estudiante en su proceso de aprendizaje.

También quiero agradecer al tutor e Ingeniero Manuel Wagner, quien siempre estuvo acompañando el proceso de realización del trabajo de grado, siempre con la mejor disposición y los mejores comentarios para mejorar.

Al Ingeniero Juan David Valderrama muchas gracias por dar el aval para realizar mi trabajo de grado dentro de la compañía Gamma Ingenieros, por hacer posible la gestión de los datos y recursos internos de la compañía.

## Tabla De Contenidos

## Lista de tablas



## Lista de Gráficos



## Lista de figuras

## Introducción

El presente trabajo hace referencia al estudio de factibilidad para la migración del protocolo IPv4 al protocolo IPv6 en la compañía Gamma Ingenieros. Se presenta, además, la base teórica acerca de ambos protocolos de internet, y, aunque tienen el mismo objetivo principal, el de interconectar redes, dichos protocolos cuentan con diferencias notables, de lo cual, se explicará en este documento.

Desde la ingeniería de telecomunicaciones, es un reto y una necesidad, estar a la vanguardia de la tecnología, siempre dispuestos al cambio hacia nuevas tendencias, que permitan el avance de la humanidad, encontrando más y mejores soluciones.

Dentro de los temas a tratar en el presente documento se encuentra el protocolo IPv4, en el cual se resumen las características y desventajas que presenta dicho protocolo, así mismo, hace mención al protocolo IPv6, con sus características principales, y los componentes que lo conforman. Luego de la revisión de los conceptos sobre los protocolos IPv4 e IPv6, se presenta un diagnóstico de la red actual de la compañía Gamma Ingenieros, para lo cual, se realiza un inventario de software y hardware, protocolos de pruebas y validación de estos, así como, los esquemas de seguridad de la información y las comunicaciones. Finalmente, se muestra el diseño del plan de implementación del protocolo IPv6, para la compañía GAMMA INGENIEROS y se especifica el

direccionamiento de la nueva red junto con los servicios y las configuraciones sobre los canales de internet.


## Resumen

La compañía GAMMA INGENIEROS es una empresa colombiana fundada en febrero de 1983, dedicada a satisfacer las necesidades de los clientes con soluciones en tecnologías de la información, consultoría e interventoría en obras civiles y telecomunicaciones. Actualmente, la entidad cuenta con una red de telecomunicaciones implementada bajo el protocolo IPv4 en su totalidad, lo que significa, que está dentro de las entidades que deberían migrar al protocolo IPv6. Esta migración, es una solución a mediano y largo plazo, debido a que por el momento los usuarios y/o clientes no van a perder conectividad con los servicios que se prestan y los usuarios seguirán teniendo acceso a internet, sin embargo, esto cambiara con los años, y es un riesgo latente, que en un futuro los usuarios de IPv4, dejen de tener acceso a servicios y/o aplicativos que solo estarán en el protocolo IPv6, lo que puede ocasionar que la compañía entre en una brecha tecnológica, generando desventajas frente a la competencia. Es por ello que el trabajo se enfoca en las condiciones necesarias para que la compañía Gamma Ingenieros logre realizar una transición del protocolo IPv4, al protocolo IPv6 de una manera óptima, cumpliendo con las reglamentaciones aplicadas a Colombia nivelando su esquema tecnológico acorde al avance del país y la inclusión de las novedosas tecnologías de la información.



**Palabras clave**: IPv4, IPv6, protocolo de red, mascara de red, prefijo de red.



## Abstract

The GAMMA INGENIEROS company is a Colombian company founded in February 1983, dedicated to satisfying the needs of customers with solutions in information technology, consulting and supervision in civil works and telecommunications. Currently, the entity has a telecommunications network implemented under the IPV4 protocol in its

entirety, which means that it is among the entities that should migrate to the IPv6 protocol. This migration is a medium and long-term solution, because for the moment users & customers will not lose connectivity with the services provided and users will continue to have internet access, however, this will change with over the years, and it is a latent risk that in the future IPv4 users will no longer have access to services & applications that will only be in the IPv6 protocol, which may cause the company to enter a technological gap, generating disadvantages compared to the competition.

**Keywords:** IPv4, IPv6, network protocol, network mask, network prefix.

## 1. Planteamiento Del Problema

El protocolo IP (Protocolo de Internet) es el mecanismo de direccionamiento de internet que permite la identificación de equipos y conmutación de paquetes, sin embargo, el protocolo IPv4 está llegando a su fin. LACNIC *(Registro de Direcciones de Internet de América Latina y Caribe*) quien es el ente encargado del registro de direcciones de internet para américa latica y el caribe, asignó los últimos bloques de direcciones IPv4 a las regiones, en febrero del 2011, por lo que, la adopción al protocolo IPv6 es una realidad que se debe afrontar para implementarlo de la mejor manera posible.

En Colombia y el mundo, el número de compañías que han venido realizando la transición al protocolo IPv6 ha crecido, debido a que, cada vez más compañías son conscientes que la reducción de direcciones es un problema real, y que, con el crecimiento acelerado de internet es inevitable que se deba hacer un cambio en sus redes pronto.

El problema del agotamiento de direcciones de internet IPv4, surge del crecimiento exponencial que ha tenido internet durante los últimos años. El limitante principal que tiene el direccionamiento IPv4 es la cantidad de direcciones disponibles (4.3 millones de direcciones) las cuales en su momento parecían ser suficientes cuando no se contaba con el crecimiento que iba a tener internet con el paso del tiempo, y que ahora se ha convertido en

un problema mundial. Para cubrir esta demanda de direcciones Steve Deering y Graig Mudge diseñaron el protocolo IPv6 y fue adoptado en 1994 por la *internet engeneering task* como una solución a largo plazo para el agotamiento de direcciones IPV4 como lo afirma (Contreras & MINTIC, 2015, p. 13).

En el 2014, Latinoamérica entró en el proceso de agotamiento de direcciones IPv4 tras otorgar 178 millones de direcciones a la región latinoamericana y Caribe. Actualmente, en el año 2020, según la página oficial de LACNIC, Latinoamérica se encuentra en la fase 3 del agotamiento de direcciones y quedan menos de 690.000 disponibles.(LACNIC, 2015).

En Colombia, la adopción del protocolo de internet versión 6, ha sido un tema de alto valor en los últimos XX años, por parte del ministerio de las telecomunicaciones (MINTIC), el cual es un ente gubernamental que ha venido desarrollando planes de sensibilización sobre la problemática del agotamiento de las direcciones IPv4 y la importancia de la pronta implementación de IPv6. En junio de 2014, se entregaron los últimos bloques /11 disponibles en el *pool* de direcciones para LACNIC, como lo afirma su página oficial (lacnic.net, 2017, p. 7). Por este motivo la necesidad de sensibilizar al sector académico, a los prestadores de servicios (ISP), al sector público y privado de la necesidad de hacer esta transición lo antes posible. La transición al protocolo IPv6 es necesaria para un mejor aprovechamiento de las redes de nueva generación creando las direcciones IP necesarias las cuales no están disponibles en la actualidad con el uso del protocolo IPv4, permitiendo, por ejemplo, el internet de las cosas como lo menciona la resolución 2710 (Resolución 0002710 - Lineamientos Para La Adopción Del Protocolo IPv6, 2017)

El problema del agotamiento de direcciones IPv4, existe desde hace poco más de 10 años, y gracias a la implantación de métodos como el NAT (*network address translation*) se ha alargado la vida de IPv4, pero trae consigo problemas adicionales, aparte del agotamiento de direcciones, según lo afirma (SABOGAL ORTIZ, 2017, p. 73), como, por ejemplo, rompe el modelo cliente-cliente ya que se pierde la transparencia original de la internet, también el hecho de utilizar NAT hace que la red quede oculta debido a que todos

los equipos utilizan la misma dirección pública para salir a internet, lo que puede ocasionar bloqueos en una red completa si algún host presenta comportamiento anormal y se pasa la ip publica a listas negras globales, además, de crear retardos en el procesamiento de los paquetes de información. También, el uso de multidifusión por *broadcast* en muchas ocasiones provoca la colisión de las redes, lo que se soluciona con la retransmisión de los datos, pero, esto añade más pérdidas de tiempo, y múltiples retardos por los saltos y algoritmos de selección de rutas que deben dar los Router al reenviar los datos.

Por otra parte, se presentan múltiples problemas relacionados con la seguridad en las redes IPv4, ya que, en el momento de su creación, su enfoque fue la conectividad, y en temas como la seguridad se quedó corto y no se estableció ningún tipo de control de en el protocolo, lo que con el paso de los años ha ocasionado que *hackers* y aficionados exploten las fallas de seguridad que se han descubierto ocasionando innumerables perdidas de datos y de dinero, además de daños en los equipos.

## 2. Justificación

El gobierno es consciente de este problema por lo que se creó la resolución 2710 para establecer los lineamientos en la adopción al nuevo protocolo y establece fechas en las que las entidades de carácter nacional deben culminar el proceso de transición antes del 31 de diciembre del 2019 y las entidades territoriales antes del 31 de diciembre del 2020. Además, que la transición a IPv6 deberá funcionar en coexistencia con IPv4.

Al pasar al protocolo IPv6 la longitud de las direcciones aumentará y permitirá contar con suficientes direcciones para soportar la gran demanda esperada para la ampliación de servicios y aplicaciones, así mismo, logrará suplir las nuevas tendencias en las necesidades de los clientes ya que IPv6 abre el espacio para seguir creciendo en internet.

En referencia al desarrollo tecnológico es importante saber que la innovación es la clave para competir y mantenerse a la vanguardia tecnológica; ya que, de retrasar mucho más la

transición se dificulta el surgimiento de nuevas aplicaciones y ralentiza el proceso de inclusión digital.

En la compañía gamma ingenieros no se han realizado estudios con respecto a la transición al protocolo IPv6 lo que abre la posibilidad de plantear una propuesta para la transición a un protocolo de internet más sofisticado como el IPv6.

El ministerio de las telecomunicaciones en su plan de adopción de IPv6 para la transformación digital del país, en el modelo de adopción para entidades indica que el primer paso para la adopción del protocolo es generar un proyecto de adopción IPv6, además de exponer que para los nuevos procesos de contratación se exija IPv6 nativo en compras y procesos licitatorios.
La elaboración de este estudio de factibilidad facilitará en gran medida las labores de planeación cuando la compañía desee iniciar con la implementación de la transición.

## 3. Alcance del proyecto

El alcance del proyecto aplicado incluye el diseño y planeación de la implementación del protocolo IPv6, mas no incluye la instalación ni configuración de ningún servicio sobre

el protocolo IPv6 que haga parte de la fase de implementación, sin embargo, se enuncia cual es el alcance recomendado para cuando la compañía defina realizar la transición.

# 4. Objetivos

## 4.1 Objetivo General

Realizar el estudio de factibilidad para la transición del protocolo de internet IPv4 al protocolo IPv6 en la compañía Gamma Ingenieros.

## 4.2 Objetivos Específicos

- Realizar una revisión bibliográfica acerca de los conceptos, funcionamiento y configuración del protocolo IPv6.
- Diagnosticar el estado actual de la red interna de la compañía Gamma Ingenieros.
- Desarrollar un estudio de factibilidad para la transición del protocolo IPv4 al protocolo IPv6 en la compañía Gamma Ingenieros.

# 5. Marco Teórico

El protocolo ip procede de la palabra internet protocolo lo que traduce protocolo de internet el cual como lo menciona (Montanez Prieto, 2018, p. 27) es un conjunto de protocolos de red los cuales son capaces de transportar distintos tipos de comunicaciones

entre equipos conectados a múltiples tipos de redes con el fin de solucionar los problemas de comunicación.

Gracias al avance y adopción que ha tenido el protocolo ip, este ha sido el principal protagonista del desarrollo y crecimiento de internet en las últimas décadas como se menciona en el artículo (Remmy & Gomez, 2016, p. 1).

Las direcciones ip son identificadores del protocolo ip, y hacen referencia a cada host dentro de una red de datos como lo menciona (Arias pulgarín, 2011, p. 24,27) y se caracterizan de dos partes principalmente, donde una parte identifica la red y otra el equipo dentro de ella. Actualmente están vigentes dos protocolos de internet, el protocolo IPv4 y el protocolo IPv6, así mismo donde el primero es el más amplio usado mundialmente, pero con un problema crítico, y es el del agotamiento de direcciones, que, debido al crecimiento exponencial de internet, así como el crecimiento de usuarios y dispositivos las direcciones lógicas posibles no son suficientes.

Con el fin de reparar deficiencias de red, a partir de 1992 se inició con la búsqueda de nuevos mecanismos que mejoraran los problemas del protocolo IPv4 como lo menciona (SABOGAL ORTIZ, 2017, p. 11), así nace IPv6 capaz de ser el sucesor del protocolo IPv4, originalmente fue lanzado en 1999 donde se conoció como el protocolo del futuro de las comunicaciones.

En Latinoamérica la organización encargada de la asignación de los recursos de numeración en internet se denomina LACNIC, la cual tiene presencia en 33 países de américa latina y el Caribe en donde su función principal es la de contribuir al desarrollo de internet mediante políticas de cooperación en el fin de lograr que internet sea un instrumento de inclusión social y desarrollo económico, además de asignar y administrar

los recursos de numeración de internet en los dos protocolos tanto el IPv4, como el IPv6, como se indican en su página oficial (Lacnic, 2015)

### 5.1 El protocolo IPV4

El protocolo de internet, o protocolo IP permite la interacción de las redes por medio de la conmutación de paquetes en todo tipo de dispositivos como computadoras, servidores, celulares, etc. Para que esto sea posible, cada dispositivo conectado a la red debe tener un valor, que representa el valor frente a la red mundial de internet, como lo afirma la resolución 2710 del ministerio de las comunicaciones (Resolución 0002710 - Lineamientos Para La Adopción Del Protocolo IPv6, 2017).

El protocolo IPv4 ha sido el mayor protagonista en el desarrollo del internet hasta la actualidad, este protocolo se basa en el modelo cliente servidor, donde múltiples clientes acceden a un servicio por un mismo equipo, como lo menciona (Remmy & Gomez, 2016).

Las direcciones IPv4 se componen de 32 bits de longitud, lo que equivale a un total de 4.295.967.296 direcciones únicas para enrutar tráfico hacia internet. para la elaboración de la enumeración de las direcciones ip, Montañez indica que una dirección IPv4 es un número de 32 bits formado por cuatro octetos (números de 8 bits) en una notación decimal, separados por puntos, donde un bit puede ser 1 o 0, por lo tanto, la notación decimal de un octeto tendría 2 elevado a la 8va potencia lo que resulta en un total de 256 de distintas posibilidades, ya que, se empieza a contar desde el 0, los posibles valores de un octeto en una dirección IP van de 0 a 255". .(2018, p. 20).

De manera similar Losada Burbano, C. y Morales Nova, O. (2018) afirma que "*El protocolo IP versión 4 es un protocolo no orientado conexión, eso implica que los paquetes*

*que se transmitan en la capa de red bajo este protocolo no requieren que el origen y el destino acordaran previamente una comunicación*." (pag37)

En una red IPv4 los equipos finales pueden comunicarse de las siguientes formas:

**UNICAST:** es cuando se envían paquetes de un host a otro únicamente

**BROADCAST**: es cuando un host envía paquetes a todos los host MULTICAST: este proceso consiste en enviar in paquete de un host a un grupo específico de host en una o en varias redes.
Y las podemos diferenciar según su clase de la siguiente manera:

- 10.0.0.0 a la 10.255.255.255 se denominan redes de clase A (10.0.0.0/8)
- 172.16.0.0 a la 172.31.255.255 se denominan redes de clase B (172.16.0.0/12)
- 192.168.0.0 a la 192.168.255.255 se denominan redes de clase C (192.168.0.0/16).

**5. 2 Características Generales Protocolo IPv4**

Las direcciones IPv4 pueden comunicarse con las demás redes de distintas maneras y dependiendo del uso que se le vaya a dar, estas direcciones se pueden denominar direcciones públicas, direcciones privadas y direcciones reservadas.

**Direcciones públicas**. Según (LACNIC,2014) las direcciones IPv4 deben ser globalmente únicas ya que forman el espacio de direcciones en internet IPv4, el propósito fundamental de las direcciones IPv4 públicas es permitir la comunicación sobre internet. Este tipo de direccionamientos es manipulado por los proveedores de servicios principalmente.

**Direcciones privadas**. Este tipo de direcciones son utilizadas en la administración de las redes internas o redes privadas, como lo menciona (Arias Pulgarin, 2011, p. 25), este tipo de direcciones se caracterizan por su falta de acceso directamente a internet, de igual modo (LACNIC, p. 2) afirma que el uso de estas direcciones es libre y cualquier persona o

empresa puede usarlas pero no pueden estar repetidas al menos dentro de la misma red. Una de las ventajas del espacio de direcciones privadas es la de conservar el espacio de direcciones globales al no asignar direcciones únicas a equipos que no lo requieren como se afirma en el rfc-1918. (Rekhter, 1996, p. 4).

Como lo indica (Coto Cortés, 2017, p. 22) los bloques de direcciones IPv4 privadas se dividen en tres grupos que se pueden configurar en los dispositivos que no requieran acceso a internet:

- 10.0.0.0 a 10.255.255.255 (10.0.0.0/8)
- 172.16.0.0 a 172.31.255.255 (172.16.0.0/12)
- 192.168.0.0 a 192.168.255.255 (192.168.0.0/16).

**Direcciones reservadas o de uso especial:** Las direcciones reservadas son aquellos espacios que se utilizan con fines específicos. Coto Cortés (Coto Cortés, 2017, p. 23), menciona algunas de las más importantes:

- **Direcciones de multidifusión y red**: no se asigna a los equipos finales ni la primera ni la última dirección del segmento.
- **Direcciones de *loopback***: estas direcciones se identifican con el segmento 127.0.0.1 y se utilizan para enviar tráfico al mismo host.
- **Direcciones *Link***. - Local: este tipo de direcciones están dentro del rango 169.254.0.0 hasta el 169.254.255.255 y se pueden asignar de forma automática a los hosts.

### 5.3 Algunas de las características del protocolo IPv4:

- **Dirección**: 32 bits de longitud (4 bytes)
- **Tiempo de vida máximo de la dirección**: Gestionadas por DHCP (*Dynamic host Configuration Protocol*).

- **Mascara de dirección**: se usa indicar a los dispositivos que parte de la dirección IP corresponde a la red, que parte a la subred y al host respectivamente.
- **Tamaño de los paquetes**: 576 bytes requeridos.
- **Fragmentación de los paquetes:** a través de Router y host de envió.
- **Cabecera IP**: longitud variable de 20-60 bytes.
- **Conexión LAN**: utiliza la conexión LAN para acceder a la capa física.

- **Filtrado de paquetes**: es un conjunto de funciones básicas de cortafuegos integradas en TCP/IP.
- **Administración de subredes locales:** internet group management protocolo (IGMP),(solvetic.com, 2020).

### 5.4 Problemas de rendimiento en IPv4

El protocolo IPv4 a pesar de tener un estimado de 4300 millones de direcciones, son muy pocas en comparación al gigante crecimiento de la industria tecnológica y con ello el aumento de dispositivos que deben conectarse a internet. Esto presenta un déficit en el rendimiento del protocolo al no ser capaz de soportar las cargas en el aumento del espacio disponible. Dentro de la red también encontramos múltiples problemas de rendimiento,

Según (Nova Morales & Burbano, 2018) una de las funciones más usadas del protocolo IPv4 es el uso de broadcast en la red; esto hace que en algunos casos se saturen las redes porque los paquetes que son enviados intencionalmente a todas los host, creen tormentas de tráfico y ralentizando la comunicación.

Además, los tiempos de respuesta son mayores debido a las demoras que ocasiona el determinar a qué destino pertenece un paquete, si es de su misma subred o debe enviarse al

router nuevamente para redireccionar el paquete, lo que requiere de procesamiento adicional de los datagramas (Nova Morales & Burbano, pag40).

### 5.5 Problemas de seguridad en IPv4

El protocolo IPv4 no implementa controles de seguridad lo que lo hace blanco de ataques por parte de hackers y aficionados. Con el tiempo se implementaron los parches que son la estructura de la seguridad del protocolo(Nova Morales & Burbano, 2018, p. 41).

El protocolo IPv4 cuenta con un número de 4.300 millones de direcciones enrutables hacia internet. Como lo menciona (MONTAÑEZ PRIETO, 2018, p. 29); esta cantidad de direcciones parecen muchas, pero en realidad no lo son, debido a la gran cantidad de dispositivos conectados a internet en la actualidad. Este número va en aumento con la gran cantidad de dispositivos conectados a internet, además, cada vez se crean nuevas industrias que requieren publicar servicios en internet como sus portales web, por lo que ese espacio de direcciones ip públicas ha ido disminuyendo drásticamente, ya para junio de 2014, LACNIC alcanzo la cuota de 4.194.302 direcciones asignadas, a partir de esta fecha comienzan las políticas de agotamiento del espacio IPv4 disponible como lo indica LACNIC en su página oficial. (lacnic.net, 2014).

La razón principal para realizar la transición del protocolo IPv4 al protocolo IPv6 lo antes posible, es el agotamiento de las direcciones IPv4, sin embargo, hay muchas más razones por las que se debe considerar, como, por ejemplo:

- El ministerio de las telecomunicaciones en la (Resolución 0002710 - Lineamientos Para La Adopción Del Protocolo IPv6, 2017, p. 3) indica que las entidades estatales de carácter nacional deberán culminar el proceso de transición el 31de diciembre de 2019, mientras que las de carácter territorial a más tardar el 31 de diciembre del

2020. Dichas afirmaciones alientan a una temprana transición por parte de las entidades privadas y más aún si se trabaja directamente con las tecnologías de la información, lo que nivela la tecnología de la empresa acorde al avance de las industrias gubernamentales.

- Trae consigo la conectividad de extremo a extremo, lo que resulta en una novedad debido a que en la actualidad el uso de NAT ha creado que internet sea una red difícil de gestionar, en donde solo las aplicaciones entre cliente y servidor funcionan óptimamente según (Montanez Prieto, 2018, p. 46)

- IPv6 está diseñada para ser más fácil de administrar y, las redes y dispositivos tienen la capacidad de autoconfigurarse sin la necesidad de la configuración manual como lo indica (Remmy & Gomez, 2016, p. 45).

- Facilidad de configurar servicios en las redes gracias a que sus direcciones no son dinámicas, además, que la compañía estará a la vanguardia de la innovación digital y se incorpora aún más en la inclusión digital del País.

- Desde el punto de vista de la competitividad hay que ser conscientes que cada día son las industrias y compañías de todo tipo que han adoptado el protocolo IPv6 por las características mencionadas anteriormente, además de siempre mantenerse en actualización en cuanto a tecnología, además de tener direcciones ip suficientes para asignar a sus dispositivos.

La no implementación del nuevo protocolo traerá problemas a futuro ya que IPv4 tiene los días contados y no hay nada que se pueda hacer debido a que LACNIC se encuentra en la fase 3 del agotamiento de direcciones como se detalla en la web de (Lacnic, 2020), para septiembre del 2020 ya no abran direcciones IPv4 disponibles para asignar, así que, antes

que ocurra se debe tener un plan de transición preparado el cambio al nuevo protocolo IPv6 de una forma organizada.

### 5.6 El Protocolo IPV6

(Montanez Prieto, 2018) afirma que el Protocolo de Internet IPv6, se constituye como la alternativa al agotamiento de direcciones disponibles. Debido al crecimiento de Internet las direcciones disponibles actuales no serán suficientes para cubrir la necesidad de estas en los próximos años. Como consecuencia de este escenario, el Grupo Especial sobre Ingeniería de Internet IETF el cual es una comunidad internacional cuya preocupación principal es el desarrollo de los estándares de internet (ICANN, 2016), se elaboró una serie de especificaciones para definir un protocolo IP de Siguiente Generación que se encargue de cubrir esta necesidad a largo plazo.

El protocolo IPv4 cuenta con un valor máximo de 4.294.967.296 direcciones posibles debido a que la cabecera que es la determina el número de bits que codificara las direcciones ip es de 32 bits, mientras que en el protocolo IPv6 cuenta con un valor de 128 bits en su cabezal para un total de $2^{128}$ que es lo mismo que 340.282.366.920.938 x $10^{8}$ direcciones enrutables hacia internet. (Montanez Prieto, 2018, p. 35).

### 5.7 Características del protocolo IPv6

Algunas de las características principales del protocolo IPv6 las explica (solvetic.com, 2020, Chapter 2) y se relacionan a continuación:

- **Dirección:** 128 bits de longitud (16 bytes).

- **Tiempo de vida máximo de la dirección:** se tienen dos tiempos de vida; el preferido y el valido, el tiempo de vida preferido siempre es <= valido.

- **Mascara de dirección:** no aplica mascara, se utiliza el prefijo de red

- **Tamaño de los paquetes:** 280 bytes requeridos.

- **Fragmentación de los paquetes**: a través del host de envió.

- **Conexión LAN**: IPv6 puede ser usado con cualquier adaptador Ethernet, y también soporta conexión a través de Ethernet virtual entre particiones lógicas.

- **Filtrado de paquetes:** el filtrado de paquetes no da soporte a IPv6.

- **Administración de subredes locales**: Multicast Listener Discovery (MLD).

La entidad encargada de asignar los nombres y sistemas de números únicos mundialmente en internet se conoce como la IANA (*Internet Assigned Numbers Authority*), ésta se encarga de coordinar la gestión de nombres de dominio de la raíz de los DNS *(Domain Name System*) como se detalla en la web de (Iana.org, 20), también coordina los recursos numéricos de internet publica globales y luego los distribuye a los llamados RIR que son los (Registros Regionales De Internet), entidades sin ánimo de lucro que se basan en un sistema de membresía. Existen 5 RIR para cubrir el direccionamiento de todo el planeta, estos están distribuidos de la siguiente manera:

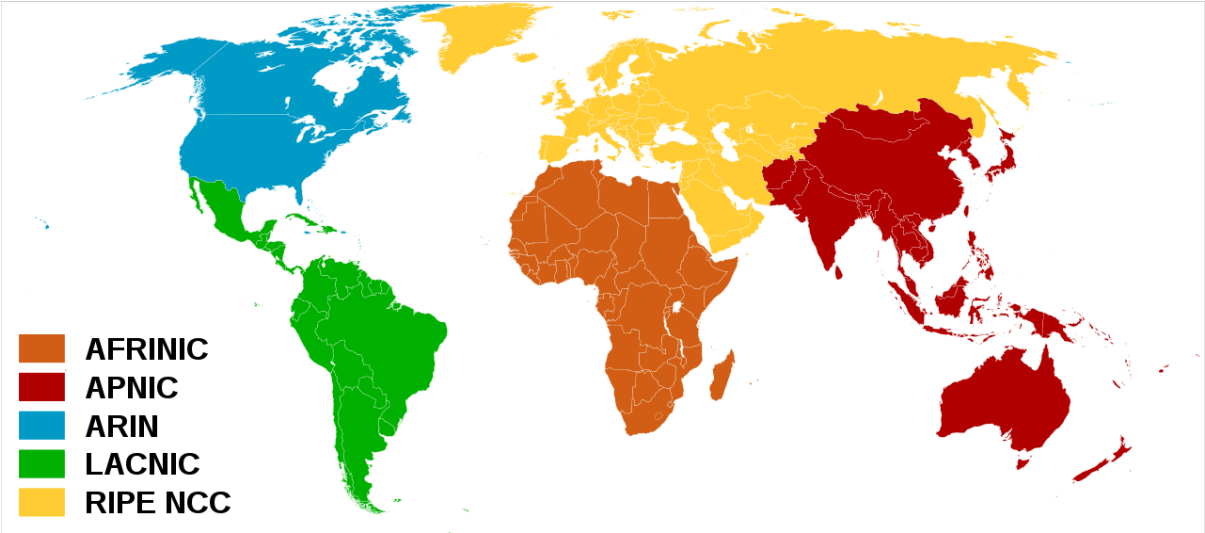



Figura 1. : IANA, Internet Assigned Numbers Authority. (1988). IANA

El agotamiento de direcciones empieza a ser un proceso realmente preocupante cuando el 3 de febrero de 2011 la IANA asignó a cada RIR los últimos 5 bloques de direcciones /8 IPv4 disponibles y de ahí hacia adelante el agotamiento por parte de los RIR es cada vez más rápido y, actualmente, casi todos están en las últimas etapas del agotamiento de direcciones, las cuales se fueron agotando por regiones de la siguiente manera:

- **APNIC (***Asia Pacific Network Information Centre*) agoto su último bloque de direcciones /8 IPv4 el 15 de abril de 2011 (Apnic.net, 2020)
-
- **RIPE NCC** (*Réseaux IP Européens Network Coordinación Centre*) El centro de coordinación de redes IP europeas asigno el ultimo prefijo /8 de direcciones IPv4 el 14 de septiembre de 2012, por lo que las redes en Europa, medio oriente y parte de Asia ya no pueden recibir nuevas (Ncc, 2019).

- **ARIN** (*American Registry For Internet Numbers*) el 23 de abril de 2014 asigno de igual forma su último bloque /8 de direcciones IPv4, siendo esta una de las más avanzadas en el agotamiento debido a que ya agotó completamente las direcciones asignables, finalizando la fase 4 el 1 de junio del 2016 como lo indica la página

(Arin, 2019). Ahora solo se asignan direcciones bajo ciertos parámetros especiales como facilitar la transición a IPv6 o proveedores críticos de infraestructura de internet.

- **LACNIC** *(Registro de Direcciones de Internet de América Latina y Caribe*) El 10 de junio de 2014 asigno el último bloque /10 de direcciones IPv4, actualmente LACNIC está en la fase 3 del agotamiento la cual inicio el 15 de febrero de 2017, y como lo indica la página oficial (Lacnic, 2020, sec. 2) cada nueva asignación debe cumplir con los requisitos establecidos por LACNIC, y la asignación máxima de direcciones será un /24 respectivamente.

- Actualmente LACNIC que es el RIR encargado de gestionar el espacio de direcciones en américa latina y el caribe, se encuentra en la fase 3 de agotamiento la cual inicio el 15 de febrero de 2017 y este será el último bloque de direcciones IPv4 disponible. A continuación, se observa el reporte a la fecha 2020-06-21 sobre el estado del agotamiento y la necesidad de adoptar nuevos mecanismos de direccionamiento en pro del bienestar del internet (Lacnic, 2020).

- AFRINIC (African Network Information Centre) Aun cuenta con direcciones IPv4 disponibles, una de las razones que aun tenga espacio disponible fue la integración como RIR ya que como lo afirma (Afrinic, 2020), ICANN acredito a AFRINIC como el quinto registro regional de internet (RIR) en abril de 2005. Para enero de 2020 entra en fase de terminación de la fase 2, siendo el RIR con el mayor espacio disponible IPv4 en la actualidad.

El gráfico 1, muestra cómo LACNIC ha asignado direcciones IPv4 durante la fase 3 del agotamiento. Donde se observa sobre el eje X la asignación desde el 2017 hasta el 2020 y sobre el eje Y la cantidad de direcciones IPv4 asignadas para cada trimestre:

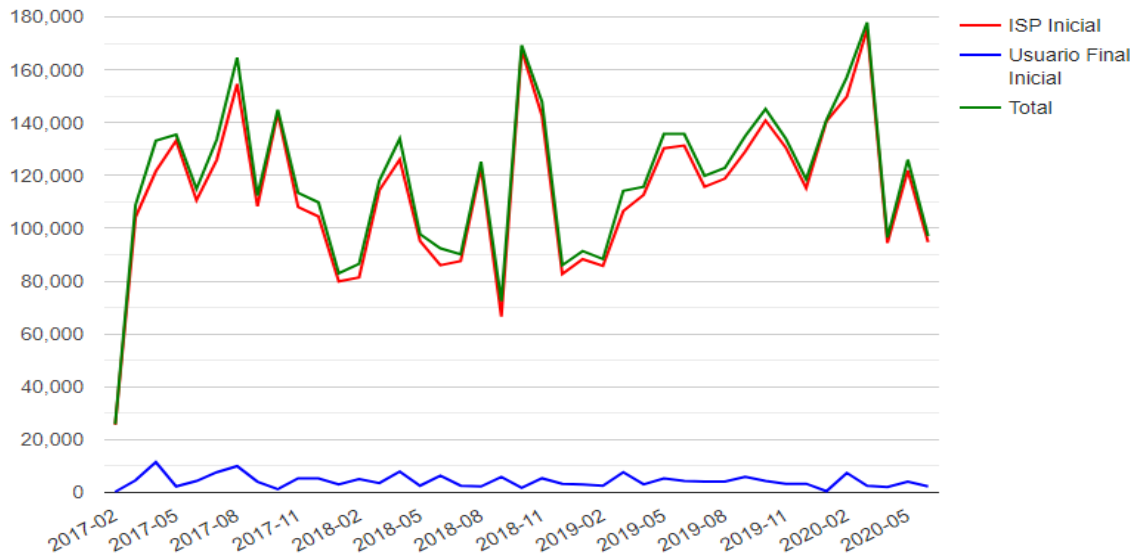



Gráfico 1. Cantidad de asignaciones de ip por mes por LACNIC. Recuperado de (LACNIC, 2020)

En el mes de febrero del 2017, la asignación de direcciones IPv4 fue de 130.000, las asignaciones presentan variaciones considerables durante cada trimestre, sin embargo, a partir del trimestre de febrero del año 2020 la disminución en la asignación es mayor, donde el trimestre de mayo del año 2020 se realizó una asignación de 95.000 direcciones IPv4, el número de asignaciones debe continuar disminuyendo hasta agotar completamente las direcciones disponibles para LACNIC.

El gráfico 2, se basa en el comportamiento de las asignaciones desde que inicio la fase 3 en febrero de 2017 hasta la actualidad, indicando la posible proyección para el agotamiento de direcciones IPv4 para el mes de septiembre del año 2020. Donde se observa sobre el eje X la cantidad de direcciones disponibles para enero del año 2020, y sobre el eje Y la proyección del agotamiento de direcciones IPv4 para América latina y el caribe, con una fecha de agotamiento estimada para enero del año 2021.

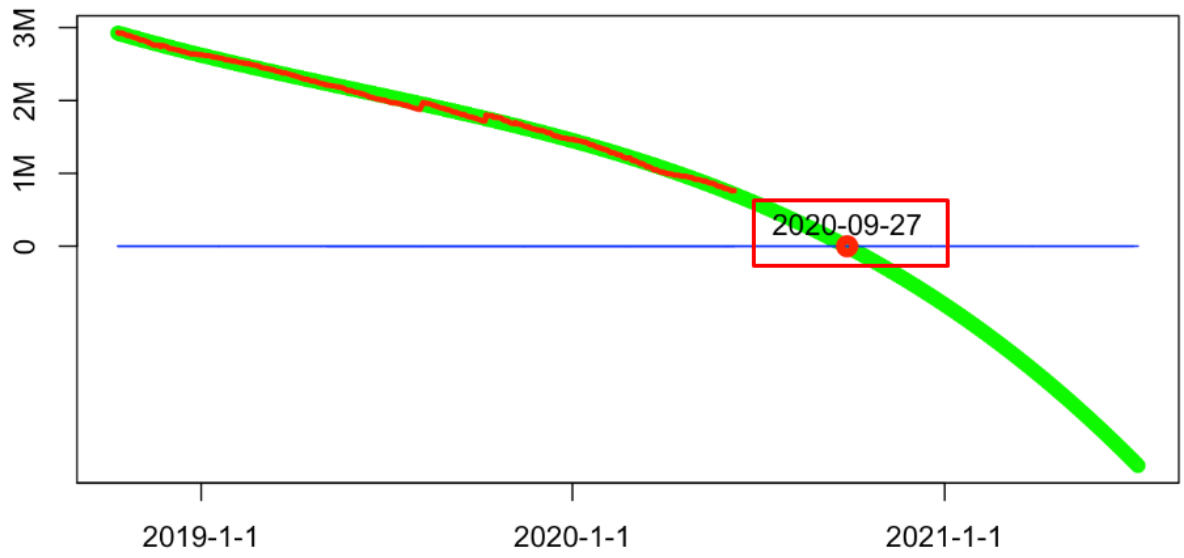



Gráfico 2.Proyección agotamiento IPv4. Recuperado de (LACNIC, 2020, fig. 3)

### 5.8 Métodos de traducción en el protocolo IPv6

Actualmente existen algunos mecanismos que permiten la coexistencia y la migración progresiva tanto de las redes como de los equipos de usuario. En las redes IPv6 existen métodos de traducción que hacen posible la convivencia simultanea de los dos protocolos, (Arias Pulgarin, 2011, p. 88), afirma que los métodos de traducción son procesos mediante los cuales se traducen las cabeceras de datagramas IPv6 a IPv4 y viceversa. La tecnología de traducción es utilizada cuando un único host IPv6 necesita comunicarse con otro. Este método de migración es la única solución en IPv6 que permite eliminar definitivamente el direccionamiento IPv4 de los nodos de red.

Cada uno de los métodos existentes tiene sus propias características especiales y cada uno resuelve un programa en particular, dentro de los que se puede destacar:

- Túneles de IPv6 sobre IPv4
- Túneles manuales
- Túneles GRE IPv6 sobre IPv4
- Túneles Bróker

- Túneles ISATAP
- Túneles IPv6 sobre MPLS
- Doble Pila (Dual Stack)
- Solo IPv6 con el uso de traductores SITT o NAT64

Sin embargo, en una red en producción se debe tener en cuenta que la mayoría de estos métodos, a excepción del Dual Stack tienen los siguientes inconvenientes:

- No son soluciones estandarizadas por lo que no hay soporte técnico formal para la solución de problemas.
- No son fácilmente escalables
- Su administración es compleja a medida que crece el número de dispositivos.
- Agregan carga extra en la red, lo cual no es bueno.
- Las configuraciones pueden llegar a ser muy complejas para lograr que funcionen correctamente.
- Permite la coexistencia indefinida de los dos protocolos ya que trabajan de manera independiente, lo que favorece a una transición gradual hasta usar únicamente IPv6 en todos los procesos, (Chuga Pantoja, 2016, p. 65)

En la figura 2 se observa la coexistencia de los dos protocolos en red mediante el mecanismo de Dual Stack:

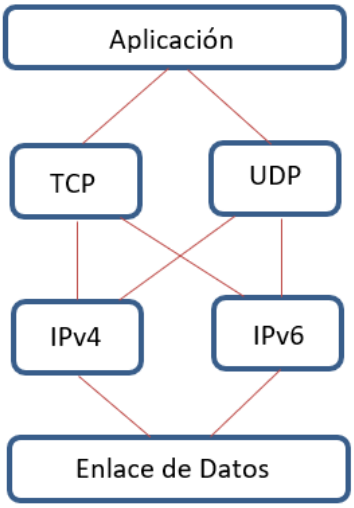



Figura 2. Mecanismo Dual Stack. (2020). Autor

IPv6 en modo Dual Stack proporciona la transición más consistente al presentar mínimas interrupciones del servicio en comparación con los otros métodos, como se observa en la figura 2 los cambios en red se realizan únicamente en la capa red, las demás etapas de la comunicación siguen intactas lo que es una de las principales ventajas Dual Stack que se ha convertido en el método preferido y más versátil, ya que como lo menciona (De la Rosa Falguera, 2016, p. 113) no se requiere la creación de túneles ni mecanismos de traducción de direcciones ip, por lo que los dos protocolos quedan operativos en todos los componentes que hacen parte de la red. Esto se logra habilitando IPv6 en los ambientes junto con IPv4 en las configuraciones de la tarjeta de red. Dual Stack también presenta algunos inconvenientes que suelen ser mucho menores en comparación con la implementación de otros métodos como lo menciona (Chuga Pantoja, 2016, p. 55).

- El uso de Dual Stack requiere soporte de los protocolos IPv4 e IPv6 en cada equipo de red

- Requiere de políticas independientes a nivel de firewall

- Soporte en las aplicaciones y servidores.

Existen varias formas de implementar este protocolo IPv6 utilizando el mecanismo de Dual-Stack, de manera general podemos mencionar las siguientes tres, las cuales se describen en el RFC2893,(Nordmark & Gilligan, 2000):

- Con la pila IPv4 habilitada y la pila IPv6 deshabilitada

- Con la pila IPv4 deshabilitada y la pila IPv6 habilitada

- Con las dos pilas habilitadas.

En este caso los nodos que tengan la pila IPv6 deshabilitada se comportaran como solo nodos IPv4, los nodos que tengan IPv4 desactivado se comportaran únicamente como nodos IPv6 y los nodos que tengan ambos protocolos habilitados preferirán conectarse con IPv6, y en caso de no recibir respuesta se intenta conectar por IPv4, (Nordmark & Gilligan, 2000, p. 5). La Forma más ordenada de implementar Dual-Stack es iniciar con los equipos activos de la red, continuando con los servidores y finalizando con los equipos de las estaciones de los clientes.

# 6. Desarrollo del proyecto

## 6.1 Etapa 1: Estado actual de la red

### 6.1.1 Inventario de TI (hardware y software)

La red actual de la compañía cubre un edificio de cuatro plantas en una única sede en Bogotá. El servicio de internet es suministrado por dos canales dedicados, un principal de 50 megas y otro de respaldo, de 20 megas los cuales llegan al equipo fortigate 100E, el cual actúa como balanceador de los canales respectivamente, además de funcionar como firewall

de la red y enrutador. Del firewall llega al switch principal el cual redirecciona el tráfico a los switch en VLAN distribuidas y nombradas por pisos.

En el protocolo IPv6 se identifican tres grandes áreas de implementación en donde es aplicable el protocolo:

- Equipos activos en red
- Servidores – servicios
- Estaciones de usuario.

Estas tareas podrán realizarse de manera asíncrona ya que es normal que las actividades propias de la operación deban realizarse en ventanas de mantenimiento controladas. Por lo que, el orden de la implementación recomendado que se propone en este proceso de adecuación es el siguiente:


Figura 3. Fases de la implementación Dual Stack. (2020). Autor

Para cada una de estas grandes ubicaciones de red, se definen alcances, los cuales se describen en los siguientes numerales.

### 6.1.2 Proveedor ISP IPv6

- Garantizar segmento de conectividad IPv6 con un proveedor de servicios local

### 6.1.3 Capa de enrutamiento

- Configuración de enrutamiento entre los segmentos de las VLAN.
- Realización de pruebas de enrutamiento IPv6 entre las VLAN configuradas.
- Configuración de IPv6 en la red inalámbrica.
- Configuración de rutas por defecto desde los equipos de enrutamiento hacia la red de internet del ISP.
- Configuración de las reglas de acceso a servicios de red desde internet y de los servicios de la red hacia el firewall, se deben tomar las reglas de IPv4 existentes como guía.
- Realización de pruebas de conectividad en IPv6 con el fin de garantizar una configuración segura y adecuada

### 6.1.3 Servidores y servicios

- Identificación de los servicios que no soporten IPv6 y por este motivo deban tratarse como excepciones en el proceso de implementación
- Configuración de los servidores identificados como compatibles con IPv6.
- Configuración de los servicios compatibles con IPv6
- Realización de pruebas de conectividad IPv6 sobre los servidores configurados.

### 6.1.4 Estaciones de usuario

- Establecer las políticas de conectividad IPv6 que se aplicara los usuarios.
- Configuración de políticas asegurando tráfico hacia y desde internet a la red local
- Realización de pruebas de enrutamiento IPv6 entre las VLAN configuradas.
- Configuración de las interfaces IPv6 en las tarjetas de red de los usuarios
- Verificación de la conectividad IPv6 para los segmentos de la red inalámbrica.

Los equipos de red de la compañía se distribuyen de la siguiente manera:

Para el inventario de los equipos en red, se recopilo información de 14 ítems, entre servidores físicos, firewall, switch y puntos de acceso, como se detalla en la tabla 7, la cual se encuentra en los anexos del documento.

**Servidores**: En el inventario se encontró que los servidores Proliant Dl360 generación 3, disponibles en la estructura de la red, no tienen soporte IPv6, por lo que es necesario adquirir los nuevos equipos para que realice las funciones de controlador de dominio, del sistema de monitoreo y el servidor de archivos. Se detecto también que estos servidores ejecutan el sistema operativo Windows Server 2003, cabe resaltar de igual modo que este sistema operativo no cuenta con soporte IPv6, se requiere que sistemas operativos más recientes, por ejemplo, Windows server 2016.

**Firewall:** Los dispositivos tipo firewall están en la completa capacidad de realizar operaciones de enrutamiento y seguridad en IPv6, se valida la ficha técnica del dispositivo donde se observan buenas características de IPv6, por lo que estos dispositivos no requieren mayor inversión.

**Switch:** Los dispositivos tipo *switch* están en la capacidad de transportar los datos tanto en protocolo IPv4 como en el protocolo IPv6.

**Aplicaciones:** Las aplicaciones de red inventariadas soportan la conectividad IPv6 en su mayoría como se indica en la Tabla 8, a excepción del controlador de dominio y su sistema operativo Windows server 2003, por lo que se deberá reemplazar el servidor y el controlador de dominio como Windows *active directory* por ejemplo en un servidor

Windows server 2019 o 2016 en su defecto; las demás aplicaciones cumplen con el proceso de adopción.

Dentro de las especificaciones técnicas de los equipos en red, se cuenta con las siguientes características:

**Servidor Proliant Dl360 Gen3.** Este tipo de servidores ofrecen características de disponibilidad esenciales en un servidor además de una potencia de cómputo concentrada para entornos de datos controlados donde en general su rendimiento es óptimo y no suelen presentar problemas; sin embargo, es una tecnología anticuada para los avances en servidores, ya que, en la actualidad en esta misma marca y modelo se encuentra en generación 10 y los equipos en la red son generación 3, además, estos servidores no pueden funcionar con sistemas operativos modernos ni es compatible con el protocolo IPv6, las especificaciones técnicas según el fabricante se detallan en la tabla 9.

**Servidor DELL Poweredge 2950**. Este tipo de servidores ofrecen flexibilidad en sus configuraciones lo cual hace que pueda ser adaptado a múltiples entornos, este tipo de servidores son muy estables y requieren actualizaciones mínimas del sistema por ende mejores reinicios y mayor eficacia además de permitir las actualizaciones de la BIOS y el firmware por medio de una pantalla integrada simplificando los mantenimientos, funcionan con múltiples tarjetas de red y son óptimos en la utilización de redes IPv6, las especificaciones técnicas según el fabricante se detallan en la tabla 10.

**Cortafuegos Fortigate 100E.** Este tipo de cortafuegos es un equipo perimetral para pequeñas y medianas empresas, este tipo de equipos provee soluciones avanzadas de seguridad como cortafuegos y Routing, permitiendo la comunicación remota y ofreciendo múltiples estándares de seguridad. Estos firewalls funcionan con un sistema operativo propio del fabricante (FortiOS) y es uno de los más poderosos del mercado en cuanto a seguridad informática se refiere. Las características técnicas las detalla en la tabla 11.

**Punto De Acceso Inalámbrico Fortinet-Fortiap 223e.** Los Access point son parte fundamental en el aseguramiento de la cobertura wifi dentro de un entorno empresarial. Estos puntos de acceso son administrados centralmente por los controladores del FortiGate principal brindando acceso seguro a internet por medio de la red wifi y brindando controles de seguridad. Las características de este modelo se detallan en la tabla 12.

**Switch Cisco Catalyst 2960.** Este tipo de switch son muy buenos para entornos empresariales ya que proveen acceso seguro a la red, estos soportan voz, datos y video además de ser jerárquicamente escalables y adaptables a diferentes tecnologías. Mundialmente la marca cisco es reconocida por brindar soluciones efectivas en la administración de las redes de telecomunicaciones(Cisco, 2013). Las especificaciones técnicas se detallan en la tabla 13.

En el Inventario de equipos de usuarios finales se encuentran los siguientes:

Tabla 1.Inventario equipos finales.

| **Versión Sistema Operativo** | **Estaciones** |
|---|---|
| Microsoft Windows 10 | 20 |
| Microsoft Windows 8.1 | 12 |
| Microsoft Windows 8.0 | 10 |
| Microsoft Windows 7 | 8 |
| Microsoft Windows XP | 6 |
| Total, Estaciones | 56 |

Fuente: autor (2020)

El componente de las estaciones de usuario está en la capacidad de transportar datos en IPv6 en la mayoría de las estaciones. Los sistemas operativos que no soportan IPv6 son los sistemas operativos Windows XP y Windows 7, las cuales deben ser actualizadas o reemplazadas por equipos que puedan soportar las versiones de sistemas operativos vigentes y con soporte IPv6.

Lo anterior nos da como resultado un total de 70 equipos en la red de la compañía Gamma Ingenieros los cuales son aptos para operar tanto en IPv4 como en IPv6. Dentro del análisis para la nueva topología, basados en la infraestructura actual, se propone la siguiente distribución:

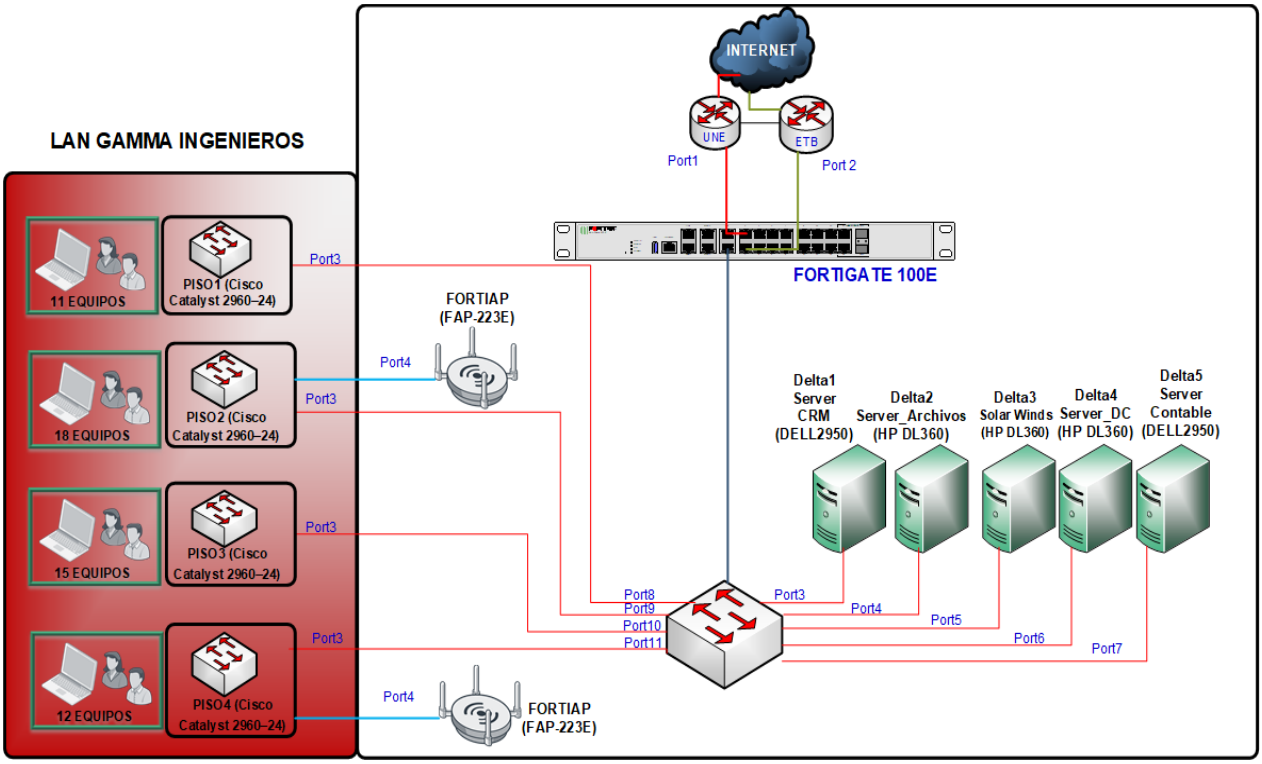



Figura 4. Topología de red Gamma Ingenieros diagrama en Visio. (2020). Autor

.

### 6.1.6 Segmentos de Red Inventariados

Se realiza el inventario de los segmentos de red que operan dentro de la compañía Gamma Ingenieros encontrando tres segmentos de red; un segmento para los servidores, un segmento para la red inalámbrica y un segmento para la red LAN, los cuales se distribuyen de la siguiente manera:

Tabla 2:Segmentos de red inventariados Gamma Ingenieros.

| Tipo | Uso | Identificador | Nombre de Dispositivo | Segmento IPv4 | Puerta de Enlace |
|---|---|---|---|---|---|
| WAN1 | Internet | ISP-ETB 50Mbps | Router Cisco C860 | 190.67.244.200/29 | 190.67.244.200 |
| WAN2 | Internet | ISP-UNE 20Mbps | Router Cisco C890 | 176.52.253.234/30 | 176.52.253.234 |
| LAN | LAN | Segmento LAN | Segmento De Red | 192.168.1.0/24 | 192.168.1.254 |
| LAN | Servidores | Segmento Servidores | Segmento De Red | 192.168.16.0/24 | 192.168.16.254 |
| servidor | Servicios | Servidor CRM | Delta1 | 192.168.16.10/32 | 192.168.16.254 |
| servidor | almacenamiento | Servidor de Archivos | Delta2 | 192.168.16.11/32 | 192.168.16.254 |
| servidor | Monitoreo | Monitoreo Solar Winds | Delta3 | 192.168.16.12/32 | 192.168.16.254 |
| servidor | Servicios | Domain Controler | Delta4 | 192.168.16.13/32 | 192.168.16.254 |
| servidor | Servicios | Contabilidad | Delta5 | 192.168.16.14/32 | 192.168.16.254 |
| Access point | Wireless | AP. Pisos 1-2 | Fortiap 223E | 192.168.100.5/24 | 192.168.100.254 |
| Access point | Wireless | AP. Pisos 1-2 | Fortiap 223E | 192.168.100.6/24 | 192.168.100.254 |
| Cortafuegos | Seguridad y Routing | Gateway-Routing | Fortigate 100E | 192.168.100.254 | 192.168.100.254 |

Fuente: autor. (2020)

En la figura 5, se observa el direccionamiento de la capa de red en el protocolo IPv4, para los equipos de la red de Gamma Ingenieros.

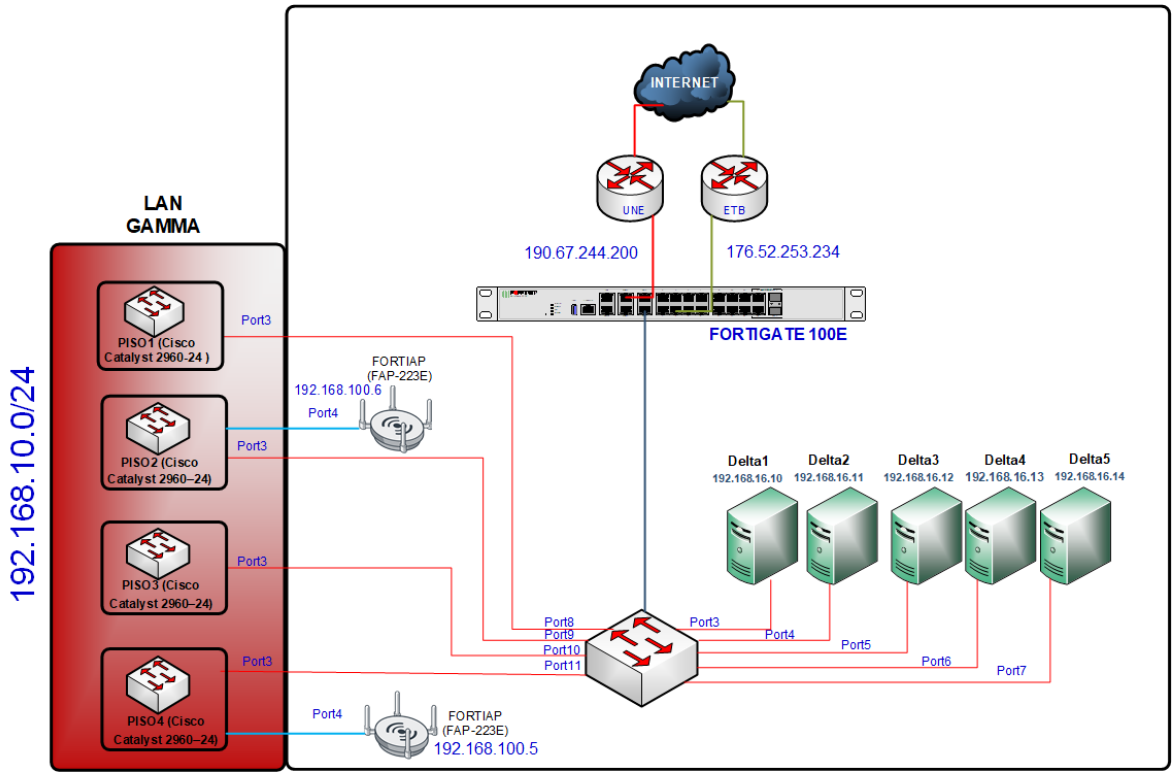



Figura 5. Direccionamiento IPv4 en red Gamma Ingenieros, diagrama en Visio. (2020). Autor

### 6.2 Etapa 2: Plan de implementación del protocolo IPv6

A continuación, se definen los lineamientos de segmentación y asignación del direccionamiento IPv6 para la compañía Gamma Ingenieros. Se define la estrategia de

direccionamiento IPv6 que se debe seguir para la asignación de direcciones en cada uno de los dispositivos en red.

En un plan de direccionamiento IPv6 los rangos de direcciones se deben agrupar efectivamente de forma lógica con el fin de lograr el máximo nivel de eficiencia par la gestión de la seguridad y conectividad de las redes como lo afirma (Alejandro, 2019, p. 11).

Algunos beneficios que presenta un efectivo plan de direccionamiento son:

- Facilidad en la implementación de políticas de seguridad tales como las listas de control de acceso y las reglas del firewall
- Mejor administración de la red con el fin de aumentar la eficiencia de la gestión de la red
- Permite el crecimiento de la red al permitir fácilmente la inclusión de nuevas ubicaciones o redes.

Un plan de direccionamiento puede dimensionar grandes rangos de direcciones IPv6, lo que puede dar la impresión de estar desperdiciando un gran número de direcciones IPv6, sin embargo, esto es algo positivo ya que se mejora la eficiencia, la implementación de políticas, se minimizan las tablas de enrutamiento ya que las direcciones están para ser usadas. Además, luego de la modificación del RFC3177, donde (Group, 2001) se daba a conocer la mejor forma de asignación, se llegó al acuerdo que este debía ser una máscara /48 , lo que en un futuro llevaría a un prematuro agotamiento del espacio ya que se asignaría más de 65000 redes a cada usuario sin importar si fuese doméstico o empresarial.

La modificación de del RFC3177(Group, 2001), lleva a la creación del RFC6177 (Huston et al., 2011), en donde se crean políticas que fomentan la asignación de bloques más pequeños, con bloques de prefijos /56, de esta forma se distribuye de manera más eficiente el espacio disponible con el fin que no ocurra como sucedió en la distribución del

espacio IPv4, en donde inicialmente se entregaron grandes rangos /8, lo que propicio que el agotamiento de direcciones IPv4 fuera aún más rápido.

**Prefijo Global 2001:0db8:2800::/56.** Debido a que actualmente la compañía Gamma Ingenieros no tiene asignado oficialmente un prefijo IPv6, se utilizará el prefijo 2001:0db8:2800: :/56, tomado del prefijo de documentación 2001:0db8::/32 definido en el RFC 3849, donde cada prefijo será asignado a cualquier dispositivo que hospede un recurso a ser accedido desde el exterior o que deba conectarse a cualquier recurso disponible en internet (Huston & P. Smith, 2004).

En el momento que la compañía Gamma Ingenieros desee solicitar prefijo oficial con el proveedor de servicios, se deberá ajustar los valores de las direcciones IPv6 de este documento ajustándolo al nuevo prefijo a asignado.

Prefijo ULA **FD00:0DB8:2800::/56.** Se ha seleccionado el prefijo FD00:0DB8:2800::/56 como prefijo ULA para la infraestructura de la compañía Gamma Ingenieros. Tomando como base el prefijo FC00::/7, definido en el RFC 4193, estas direcciones deben ser asignadas a cualquier dispositivo que no hospede un servicio que deba ser accedido desde internet ni tampoco consultar recursos de internet, se pueden definir como las direcciones privadas de IPv6. Este tipo de direcciones son enrutables dentro de áreas limitadas como un sitio, por ejemplo, como lo menciona el RFC 4193(Haberman et al., 2005), algunas de las características de las direcciones ULA se detallan a continuación:

- Permiten la conexión de redes internas.
- Son las direcciones privadas de IPv6.
- Permite que los equipos combinen direcciones públicas y privadas sin crear conflictos en las interfaces.

### 6.2.1 Propuesta de direccionamiento IPv6

**Segmentación del prefijo:** Se propone una jerarquía basada en NIBBLES, estos son bloques de 4 bits que representan un carácter hexadecimal (0-F), esto hace que las direcciones sean más fáciles de identificar visualmente.

**Prefijo IPv6 asignado por LACNIC:** Prefijo /56. Es el prefijo asignado por LACNIC a la compañía para su distribución IPv6, el prefijo asignado es el 2001:0db8:2800:0000::/56, lo que quiere decir que los primeros 56 bytes se utilizaran para identificar la red y los 72 bytes restantes se utilizan identificador de la interfaz, a partir de este prefijo asignado se inicia la distribución del direccionamiento IPv6.

Tabla 3:Prefijo IPv6 asignado por LACNIC

| ZONA | Tipo de Trafico | Prefijo Global IPv6 /56 | Prefijo ULA /56 |
|---|---|---|---|
| Toda la Zona | INTERNET | 2001:0DB8:2800:0000::/56 | FD00:0DB8:2800:0000::/56 |

Fuente: Autor. 2020

### 6.2.2 Ubicaciones de red.

Prefijo /60 por cada ubicación de red, se asignan los 4 bits siguientes del prefijo IPv6 /56 asignado, lo que permite crear hasta 14 futuras sedes de la organización debido a que $2^4 = 16$, reservando el crecimiento de la sede principal. De este modo cada ubicación geográfica tendría asignado un rango del prefijo 2001:0db8:2800:0000::/60 al 2001:0db8:2800:00F0::/60.

Actualmente la compañía Gamma Ingenieros tiene clasificada su red en una sola ubicación geográfica la cual se conocerá como “toda la zona “. En la Tabla 4 se puede observar la asignación del prefijo /60 a las ubicaciones geográficas, se reservan un segmento de red para crecimiento de la misma sede, queda disponible un pool de asignación de direcciones IPv6 para 14 ubicaciones adicionales para un crecimiento futuro.

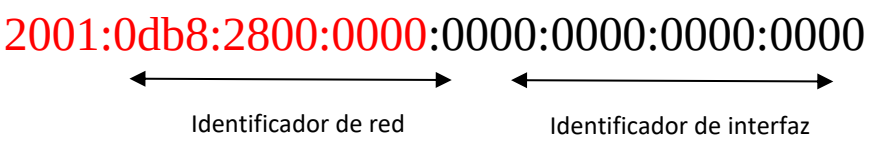
Tabla 4:Prefijos IPv6 asignados por ubicación.

| Sede | Ubicación | Prefijo Global IPv6 /60 | Prefijo ULA /60 |
|---|---|---|---|
| Principal | Toda la Zona | 2001:0DB8:2800:0000::/60 | FD00:0DB8:2800:0000::/60 |
| Crecimiento principal | Toda la Zona | 2001:0DB8:2800:0010::/ 60 | FD00:0DB8:2800:0100::/60 |
| Crecimiento ubicaciones | Ubicaciones adicionales | 2001:0DB8:2800:00F0::/ 60 | 2001:0DB8:2800:00F0::/60 |

Fuente: autor (2020)

### 6.2.3 Tipo de tráfico

Prefijo /64 por cada Vlan al interior de una ubicación, los últimos 4 bits serán asignados a la identificación de cada Vlan por cada tipo de tráfico que se puede identificar como servidores, LAN, servicios inalámbricos etc. El prefijo que se asignara debe ser un /64 lo que permite crear hasta 16 vlan diferentes al interior de una ubicación, debido a que $2^4 = 16$, se identifica con el rango 2001:0db8:2800:0000::/64. Con la asignación del prefijo /64 termina la asignación del identificador de red y queda disponible el rango completo para la distribución a las interfaces de red, la dirección IPv6 sin acortadores queda de la siguiente forma:




Para las VLAN de la compañía se definen las redes nombradas en la Tabla 5

Tabla 5:Prefijos IPv6 asignados por tipo de tráfico

| Tipo de Trafico | Ubicación | Prefijo Global IPv6/64 | Prefijo ULA /64 |
|---|---|---|---|
| Seguridad y Routing | Toda la Zona | 2001:0DB8:2800:0001::/64 | FD00:0DB8: 2800:0001::/64 |

| | | | |
|---|---|---|---|
| LAN | Toda la Zona | 2001:0DB8:2800:0002::/64 | FD00:0DB8:2800:0002::/64 |
| Servidores | Toda la Zona | 2001:0DB8:2800:0003::/64 | FD00:0DB8:2800:0003::/64 |
| Wireless | Toda la Zona | 2001:0DB8:2800:0004::/64 | FD00:0DB8:2800:0004::/64 |
| Crecimiento | Toda zona | 2001:0DB8:2800:000F::/64 | FD00:0DB8: 2800:000F::/64 |

Fuente: autor (2020)

### 6.2.4 Direccionamiento del host

En el protocolo IPv6 se establece que, las estaciones, equipos de red y servidores deben manejar un estándar en donde los primeros 64 bits sean identificadores de red y los últimos 64 como los identificadores de interfaz, tal como se menciona en el RFC3177 (Group, 2001, p. 1), de este modo el prefijo asignado para los host dentro de cada tipo de tráfico corresponde a los cuatro siguientes octetos para un total de $2^{16} = 65536$ host en cada tipo de tráfico.

El plan de direccionamiento IPv6 se asignará de la siguiente manera:

Tabla 6:Direccionamientos equipos finales

| Tipo | Uso | Identificador | Nombre de Dispositivo | Segmento IPv4 | Puerta de Enlace |
|---|---|---|---|---|---|
| servidor | Servicios | Servidor CRM | Delta1 | 2001:0db8:2800:3::3/64 | 2001:0db8:2800:3::1/64 |
| servidor | almacenamiento | Servidor de Archivos | Delta2 | 2001:0db8:2800:3::4/64 | 2001:0db8:2800:3::1/64 |

| | | | | | |
|---|---|---|---|---|---|
| servidor | Monitoreo | Monitoreo Solar Winds | Delta3 | 2001:0db8:2800:3::5/64 | 2001:0db8:2800:3::1/64 |
| servidor | Servicios | Domain Controler | Delta4 | 2001:0db8:2800:3::6/64 | 2001:0db8:2800:3::1/64 |
| servidor | Servicios | Contabilidad | Delta5 | 2001:0db8:2800:3::7/64 | 2001:0db8:2800:3::1/64 |
| Access point | Wireless | AP. Pisos 1-2 | Fortiap 223E | 2001:0db8:2800:4::2/64 | 2001:0db8:2800:1::1/64 |
| Access point | Wireless | AP. Pisos 3-4 | Fortiap 223E | 2001:0db8:2800:4::3/64 | 2001:0db8:2800:1::1/64 |

Fuente: autor (2020)

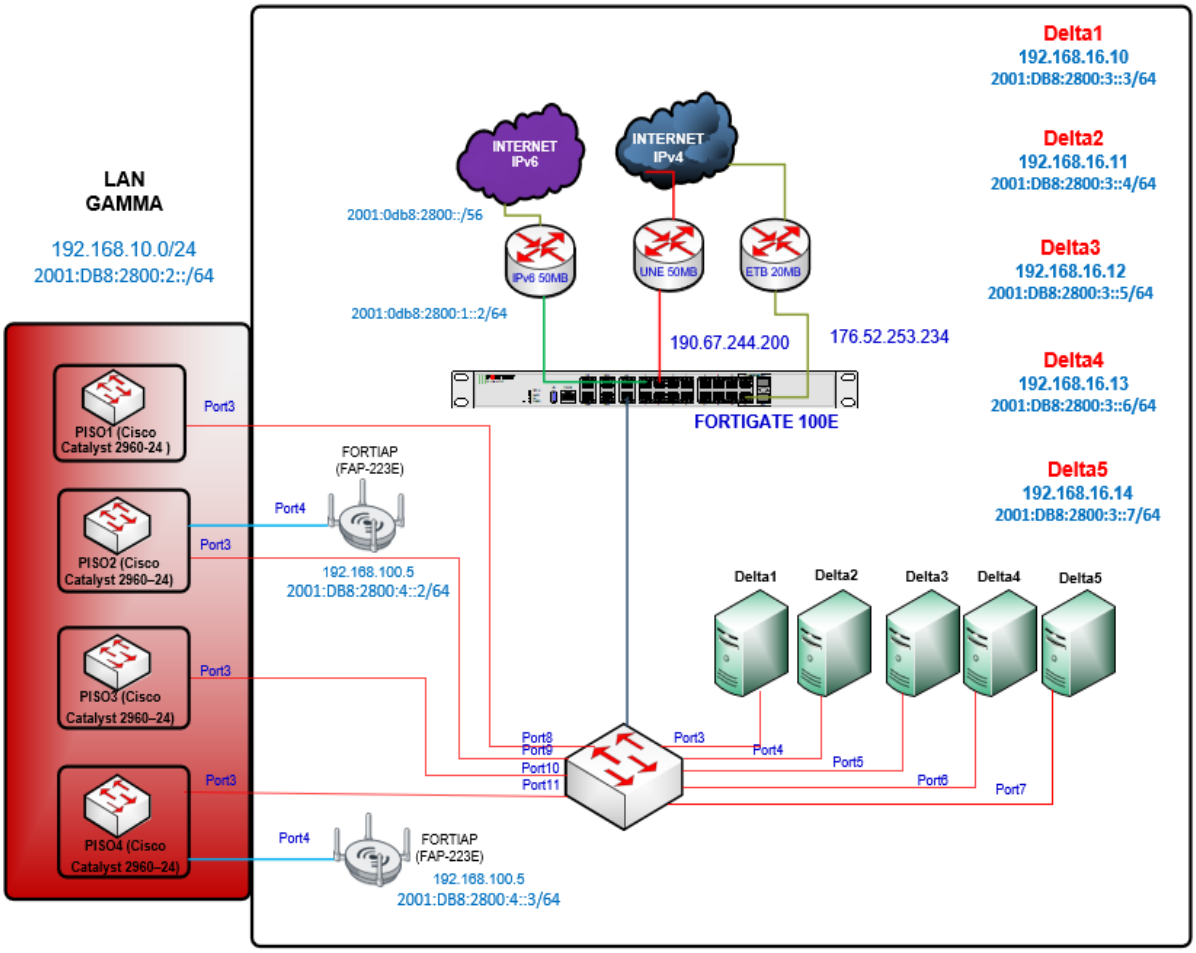



Figura 6. Diagrama de red en doble pila diagrama en Visio. (2020). Autor

Como se observa en la figura 6 y en la tabla 6, se agregan los nuevos prefijos de red IPv6 a las interfaces existentes, esta es una de las características de dual Stack, que, ya que se brinda soporte IPv6 nativo en la mayoría del hardware y software disponible, esto se puede reflejar en un impacto mínimo en la transición hacia el protocolo IPv6. De este modo se tiene en paralelo tanto el direccionamiento IPv4 para que la red pueda funcionar con normalidad, pero permitiendo también el tráfico de paquetes en el protocolo IPv6, a continuación, se observa un ejemplo de configuración en dual Stack para la red de gamma ingenieros:

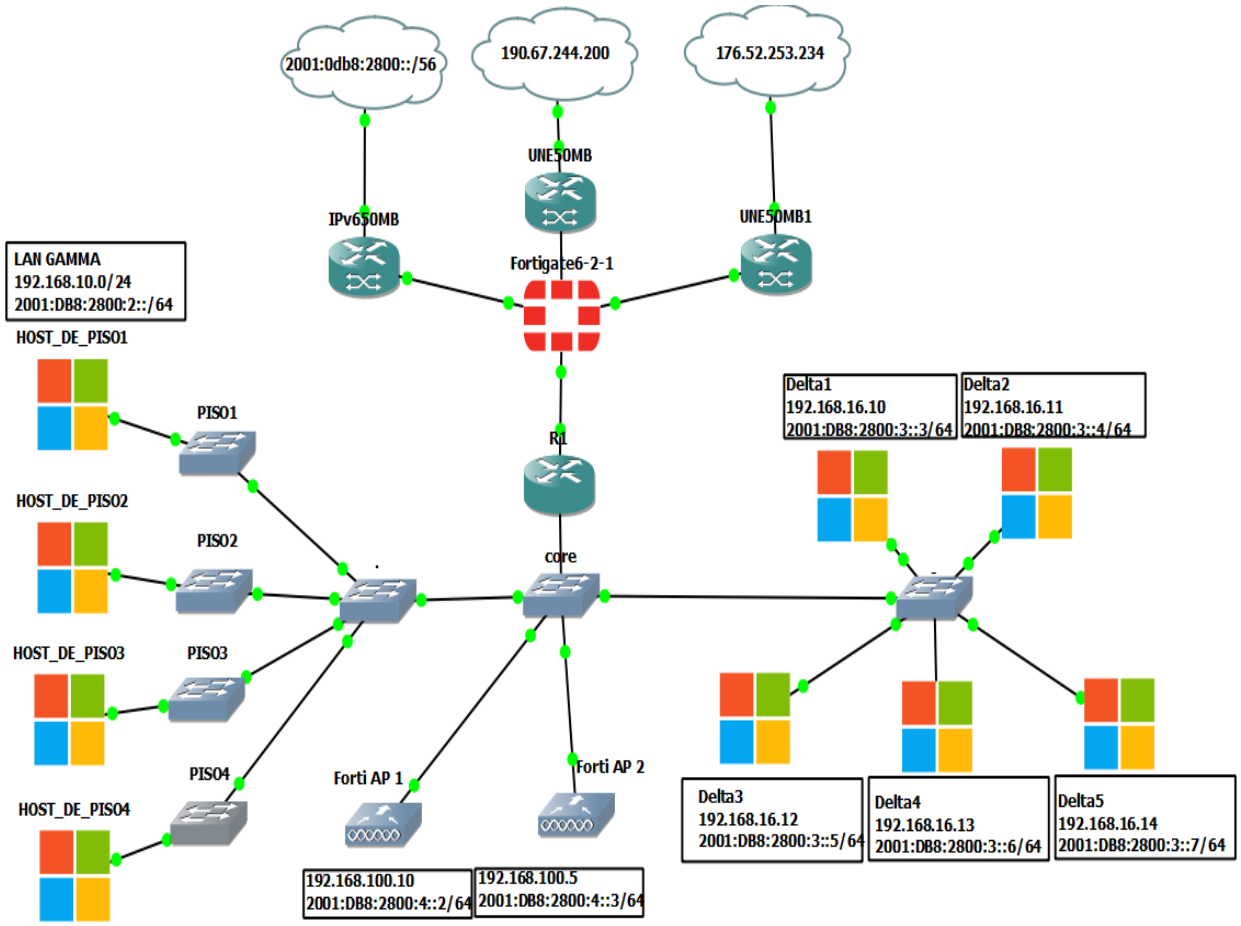



Figura 7. Diagrama de red en el protocolo IPv6 diagrama en Gns3. (2020). Autor

En las interfaces de los switch no se realizan cambios, ya que estos transportan datos en la capa 2 del modelo OSI, y las configuraciones de enrutamiento se hacen a nivel de capa 3, o capa de red, sin embargo, en el Router se debe habilitar y permitir la comunicación de los protocolos IPv4 e IPv6, para ello, adicionamos los prefijos IPv6 en cada interfaz, y habilitamos en el Router el reenvió de paquetes IPv6 de la siguiente manera:

```
Router>en
Router#conf
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int f0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif) #ip add 192.168.10.1 255.255.255.0
Router(config-subif)#ipv6 add 2001:DB8:2800:2::2/64
Router(config-subif) #no sh
Router(config-subif)#int f0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip add 192.168.100.1 255.255.255.0
Router(config-subif)#ipv6 add 2001:DB8:2800:4::2/64
Router(config-subif)#int f0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip add 192.168.16.1 255.255.255.0
Router(config-subif)#ipv6 add 2001:DB8:2800:3::2/64
Router(config-subif)#no sh
Router(config-subif)#int f0/0
Router(config-subif)# exit
Router(config-subif)# ipv6 unicast-routing
```

Figura 8. Configuración de prefijos IPv6 en Router. (2020). Fuente Autor

A nivel de firewall se debe permitir e incluir los segmentos adicionales de IPv6, esto se consigue habilitando IPv6 en el dispositivo ya que por defecto se encuentra deshabilitado. Luego, incluir el prefijo IPv6 en la interfaz según corresponda la pila, doble se habilita de la siguiente manera:

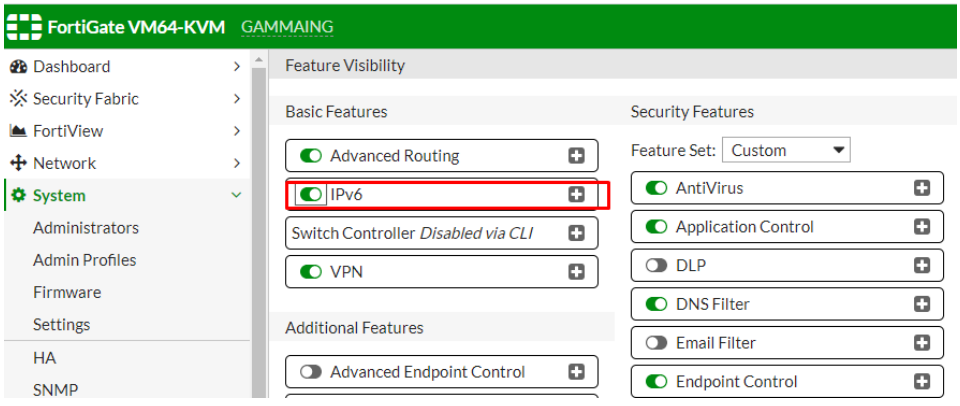



Figura 9. Activación IPv6 en el firewall. (2020). Fuente Autor.

En las interfaces existentes se debe agregar el prefijo IPv6 correspondiente en cada interfaz IPv4. Adicionalmente, en una nueva interfaz se agrega el prefijo global IPv6 asignado por el ISP, en este caso, el prefijo es 2001:db8:2800:0000::/64, el cuál es el encargado de brindar la conexión IPv6 en la red.

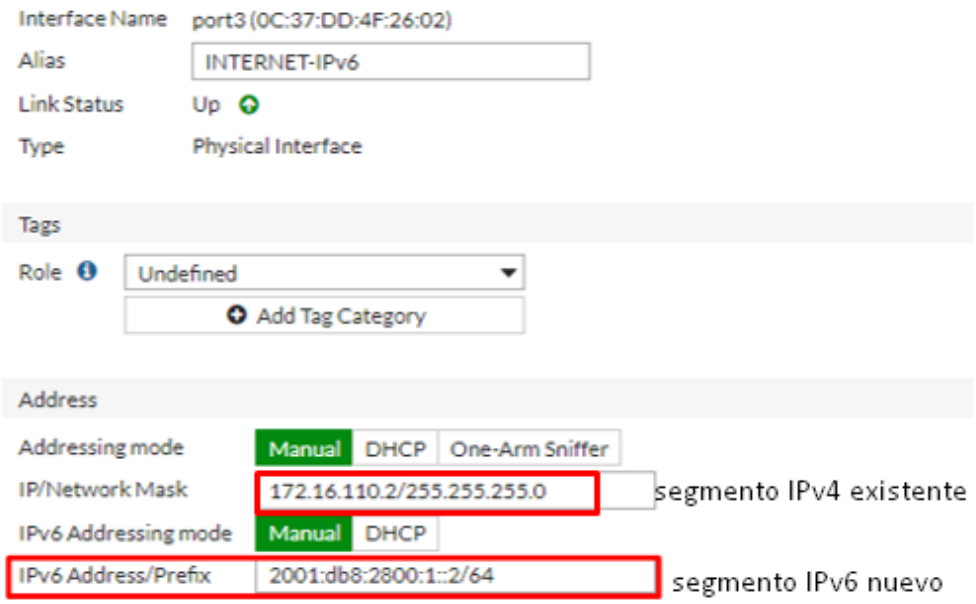



Figura 10. Inclusión nuevo prefijo IPv6 a la red. (2020). Fuente Autor

Para la zona LAN se agrega el prefijo 2001:DB8:2800:2::/64, en la interfaz del firewall, y se asigna la primera dirección como puerta de enlace:

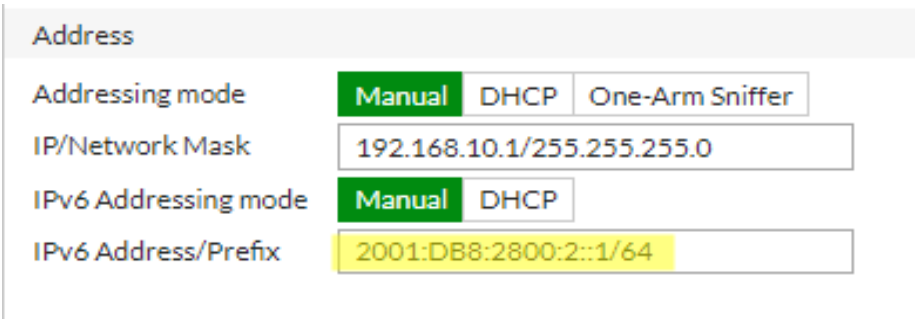



Figura 11. Asignación prefijo IPv6 en interfaz de firewall LAN. (2020). Fuente Autor

A nivel de los equipos finales de la red también se debe activar la doble pila, esto se logra habilitando la interfaz IPv6 que ya trae por defecto, y asignando en ella una dirección IP. A continuación, se observa como en el mismo host se aplica el direccionamiento IPv4 e IPv6 simultáneamente.

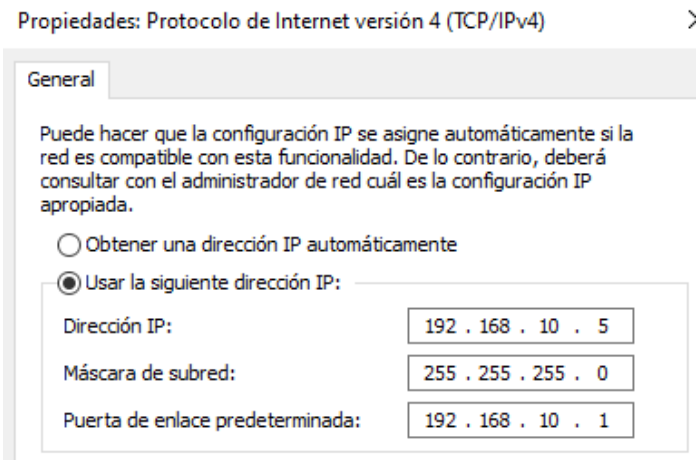



Figura 12. Direccionamiento IPv4 en host A en red LAN. (2020). Fuente Autor

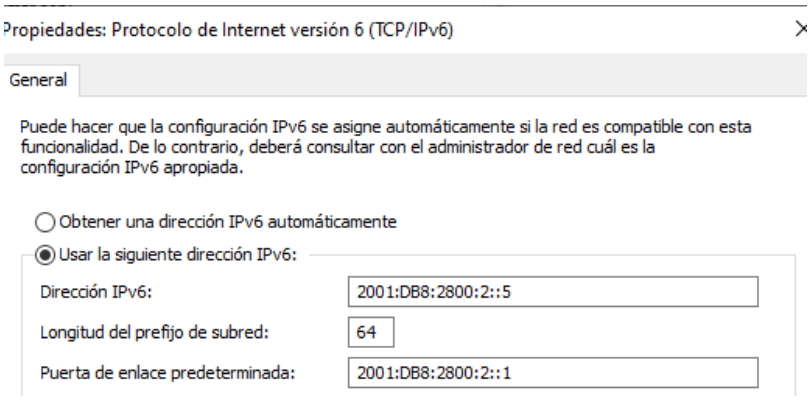



Figura 13. Direccionamiento IPv6 en host A en red LAN. (2020). Fuente Autor.

En la zona de los servidores se agrega el prefijo 2001:DB8:2800:3::/64 en la interfaz existente el firewall:

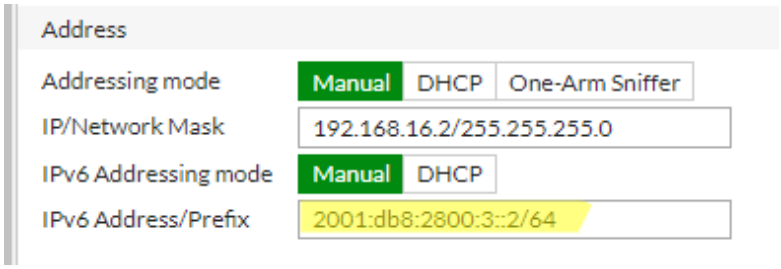



Figura 14. Asignación prefijo IPv6 en interfaz de firewall servidores. (2020). Fuente Autor.

En los equipos servidores se debe configurar el direccionamiento IPv4 e IPv6 en la tarjeta de red:

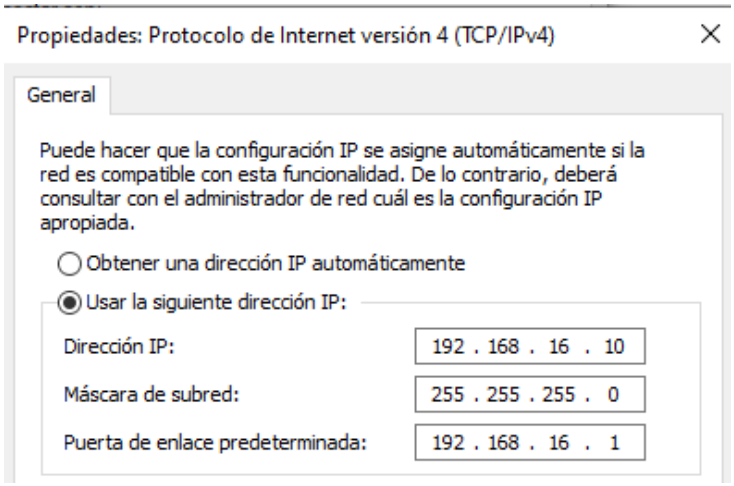



Figura 15. Direccionamiento IPv4 en host de red servidores. (2020). Fuente Autor.

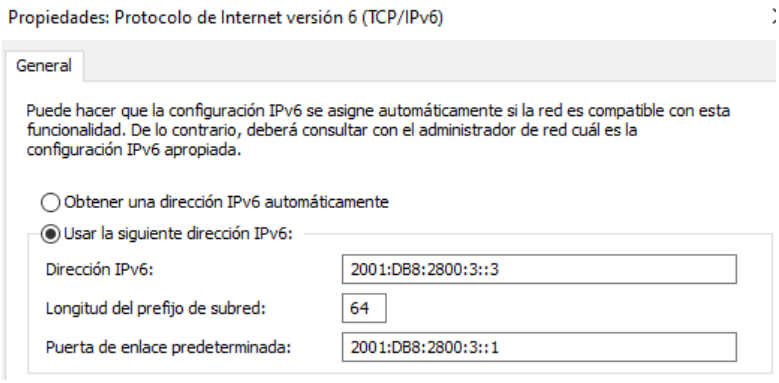



Figura 16. Direccionamiento IPv6 en host de red servidores. (2020). Fuente Autor.

En la zona Wireless, se agrega el prefijo 2001:DB8:2800:4::/64 en la interfaz existente del firewall. De igual modo, se debe activar el direccionamiento IPv6 en las características de configuración IPv6 en cada punto de acceso

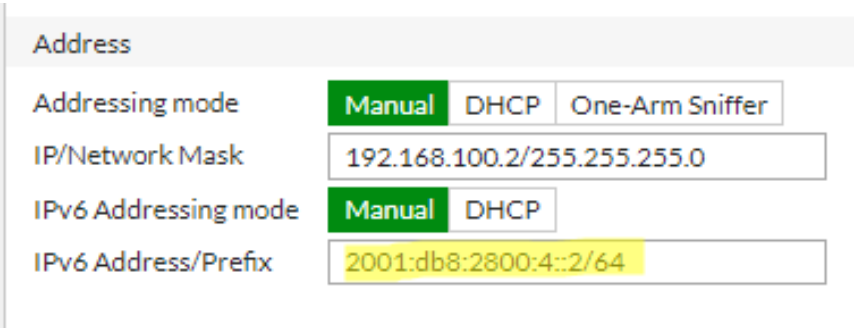
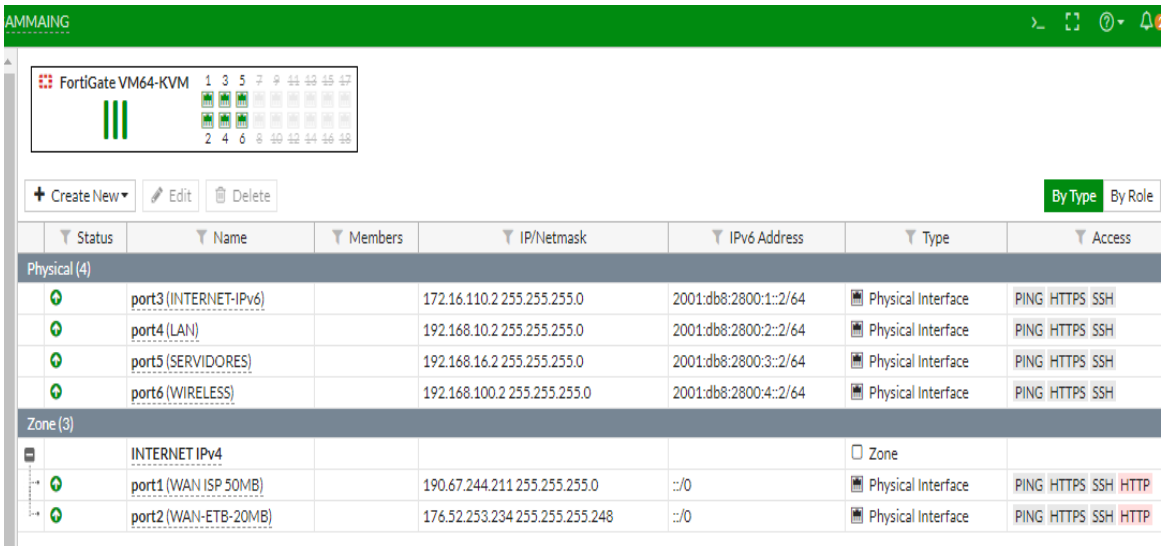



Figura 17. Asignación prefijo IPv6 en interfaz de firewall Wireless. (2020). Fuente Autor.

En la siguiente imagen, se observa las configuraciones del direccionamiento IPv4 como el direccionamiento IPv6 para cada una de las interfaces de red a nivel del firewall de la red garantizando la doble pila en los direccionamientos de la red.




| Status | Name | Members | IP/Netmask | IPv6 Address | Type | Access |
|---|---|---|---|---|---|---|
| Physical (4) | | | | | | |
| | port3 (INTERNET-IPv6) | | 172.16.110.2 255.255.255.0 | 2001:db8:2800:1::2/64 | Physical Interface | PING HTTPS SSH |
| | port4 (LAN) | | 192.168.10.2 255.255.255.0 | 2001:db8:2800:2::2/64 | Physical Interface | PING HTTPS SSH |
| | port5 (SERVIDORES) | | 192.168.16.2 255.255.255.0 | 2001:db8:2800:3::2/64 | Physical Interface | PING HTTPS SSH |
| | port6 (WIRELESS) | | 192.168.100.2 255.255.255.0 | 2001:db8:2800:4::2/64 | Physical Interface | PING HTTPS SSH |
| Zone (3) | | | | | | |
| | INTERNET IPv4 | | | | Zone | |
| | port1 (WAN ISP 50MB) | | 190.67.244.211 255.255.255.0 | ::/0 | Physical Interface | PING HTTPS SSH HTTP |
| | port2 (WAN-ETB-20MB) | | 176.52.253.234 255.255.255.248 | ::/0 | Physical Interface | PING HTTPS SSH HTTP |

Figura 18. Segmentación Dual Stack en interfaces de firewall Fortigate. (2020). Fuente Autor.

Se deben crear politicas que enruten el trafico hacia el internet IPv6, y dentro de las más básicas y esenciales se pueden destacar las que brindan acceso entre equipos de la red y las politicas que enrutan el tráfico hacia internet, una de las caracteristicas a tener en cuenta en la creacion de politicas de firewall en IPv6 es que no requiere el uso de NAT, este es uno de los problemas que solventa el uso de IPv6.

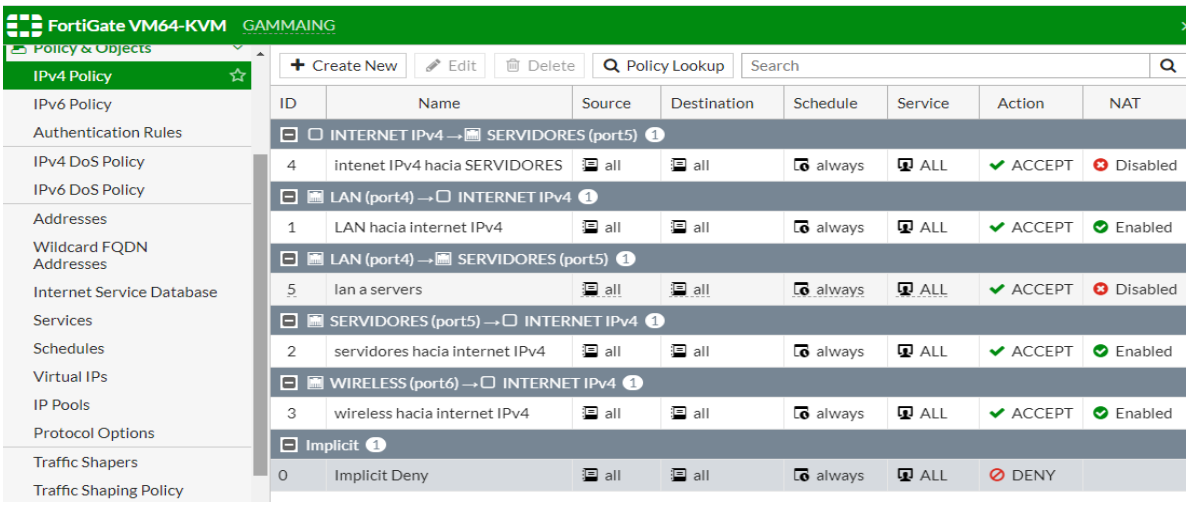



Figura 19. Políticas de firewall en el protocolo IPv4 en firewall Fortigate. (2020). Fuente Autor.

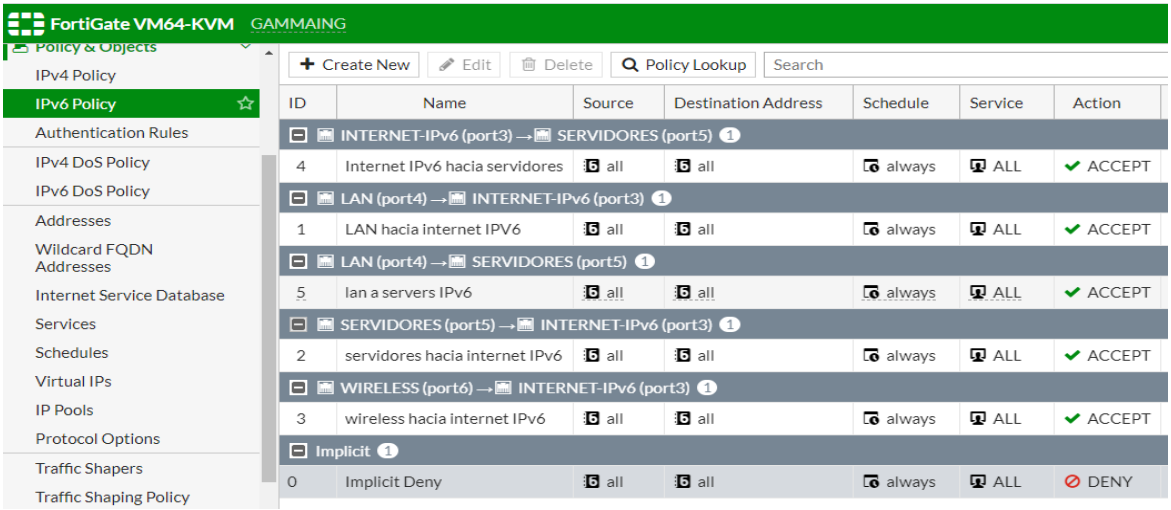



Figura 20. Políticas de firewall en el protocolo IPv6 en firewall Fortigate. (2020). Fuente Autor.

A continuación, se observa el direccionamiento de un equipo aleatorio de la red LAN con la doble pila activa, evidenciando conectividad en red tanto al protocolo IPv4, como IPv6

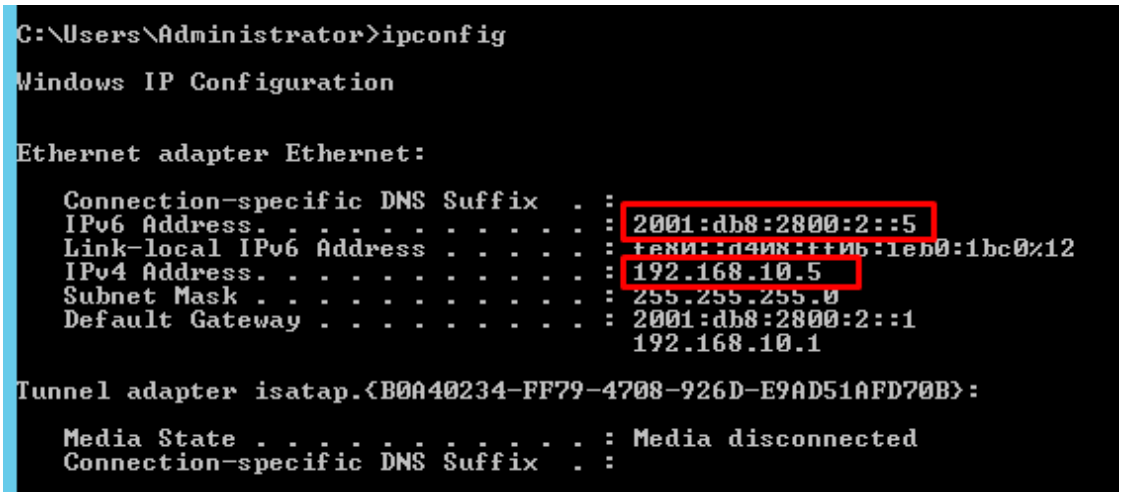



Figura 21. Host con direccionamiento IPv4 e IPv6 simultáneamente. (2020). Fuente Autor.

Ahora se envían paquetes de ping a otro equipo de la red.

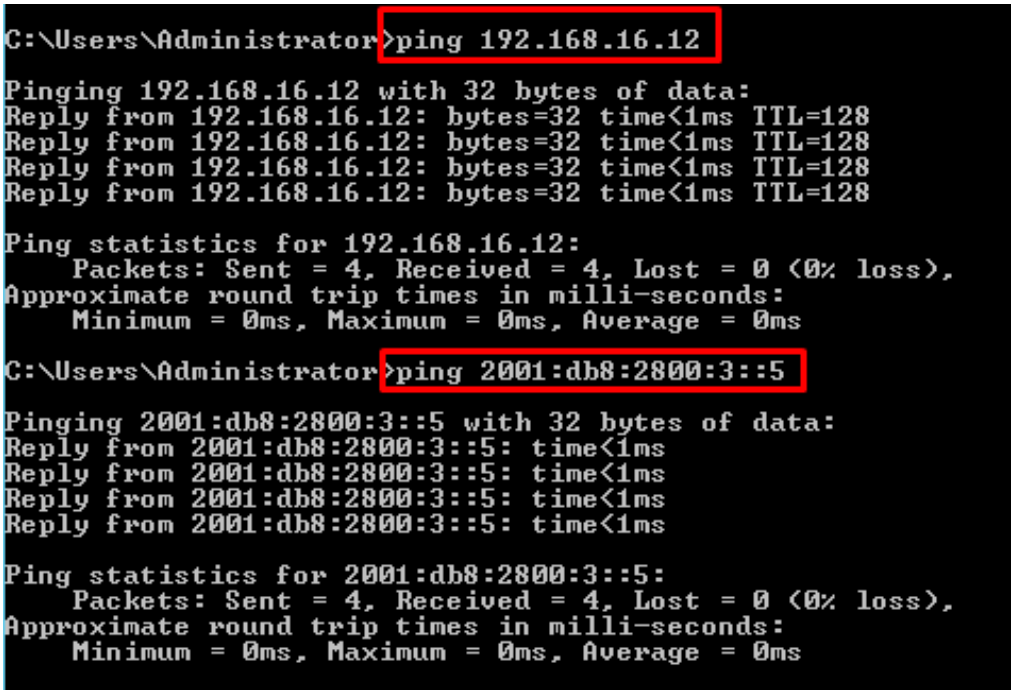



Figura 22. Conectividad hacia otro host en IPv4 e IPv6 (Dual Stack). (2020). Fuente Autor.

## 7. Conclusiones

Los equipos de la red se pueden comunicar desde cualquiera de los dos protocolos, tanto el IPpv4 como el IPv6, lo que indica una correcta aplicación del mecanismo Dual Stack, simplificando la transición, optimizando y estabilizando los recursos en la red.

Una vez finalizada la implementación del nuevo protocolo en la red se valida la conectividad tanto en el protocolo IPv4 como en el protocolo IPv6 sin preocupación a quedar sin acceso a los recursos de la red.

Con una transición progresiva del protocolo IPv4 al protocolo IPv6 utilizando el mecanismo de dual Stack se garantiza una convivencia armoniosa sin perjudicar el funcionamiento de los equipos en la red lo que brinda seguridad y facilidad al ingresar nuevos equipos en la red.

La transición al protocolo IPv6 se implementa bajo la modalidad de Dual Stack o pila doble, por sus siglas en inglés, ya que, como se mencionó, ayuda a mantener activo 100% las capacidades de ambos protocolos, brindando la posibilidad de ampliar la conectividad, con el fin de crear un cambio progresivo en el funcionamiento general de la red y así, utilizar cada vez menos el protocolo IPv4 hasta que se retire completamente de la red.

Este mecanismo acompañará la red durante un largo periodo de tiempo, progresivamente se deberá eliminar todo rastro de IPv4 y trabajar únicamente con direcciones IPv6, además, de los beneficios de usar IPv6.

En la compañía Gamma Ingenieros es factible la implementación del protocolo IPv6 en la red.

## 8. Referencias Bibliográficas


AFRINIC. Afrinic history. 08/05/2020. Disponible en www.afrinic.net/history

APNIC get ip.08/05/2020. Disponible en www.apnic.net/get-ip

Arin. IPv4 Addressing Options. 08/05/2020. Disponible en www.arin.net/resources/guide/ipv4/v

PULGARIN, Hector Fabio. estrategia de migración de ipv4 a ipv6 para las pymes en colombia. 17/04/2020. disponible en https://repositorio.ucp.edu.co/handle/10785/958

CHUGA PANTOJA, Diana Del Pilar. Planificación de procesos para la migración del protocolo ipv4 a ipv6 para la continuidad del servicio en los isp's. 14/04/2020. Disponible en http://repositorio.puce.edu.ec/handle/22000/11312

CONTRERAS SANCHEZ, Fernando Alirio. Guía para el aseguramiento del protocolo ipv6. 14/04/2020. Disponible en www.mintic.gov.co

COTO CORTÉS, Anibal. Direccionamiento IP Introducción a redes Capítulo 8. 02/05/2020. Disponible en www.ie.itcr.ac.cr/acotoc/CISCO/R&S CCNA1/R&S_CCNA1_ITN_Chapter8_Direccionamiento IP.pdf

DE LA ROSA FALGUERA, Ramon. Fundamentos teórico-prácticos del protocolo IPv6. 12/04/2020 Disponible en upcommons.upc.edu/handle/2117/98250?locale-attribute=en

HABERMAN, B., HINDEN, R., & PERKINS, C. RFC4193. 10/04/2020. Disponible en https://tools.ietf.org/html/rfc4193

HUSTON, G. RFC3849. 10/04/2020. Disponible en https://tools.ietf.org/html/rfc3849

HUSTON, G., ROBERTS, L., & NARTEN, T. RFC6177. 10/04/2020. Disponible en https://tools.ietf.org/html/rfc6177

ICANN. IETF. 11/04/2020. Disponible en https://es.icannwiki.org/IETF

LACNIC. No hay más direcciones IPv4 en América Latina y Caribe. 10/04/2020. Disponible en www.lacnic.net/web/anuncios/2014-no-hay-mas-direcciones-ipv4.

LACNIC. Acerca de Lacnic. 10/04/2020. Disponible en https://www.lacnic.net/966/1/lacnic/que-es-lacnic

LACNIC. Fases de Agotamiento de IPv4. 15/04/2020. Disponible en https://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4

MINTIC. Resolución 2710 - Lineamientos para la adopción del protocolo IPv6. 11/03/2020 disponible en www.mintic.gov.co/portal/604/articles-61192_recurso_1.pdf

RIPE NCC. The RIPE NCC has run out of IPv4 Addresses. 16/04/2020 Disponible en https://www.ripe.net/publications/news/about-ripe-ncc-and-ripe/the-ripe-ncc-has-run-out-of-ipv4-addresses

NORDMARK, Gilligan. RFC2893.10/04/2020. Disponible en https://tools.ietf.org/html/rfc2893#section-2

MORALES, Olga & BURBANO, camilo. Consideraciones para las buenas prácticas de seguridad del protocolo ipv6 en redes de área local corporativas. 21/04/2020. Disponible en https://doi.org/10.1542/peds.2006-2099

REKHTER, Groot. RFC1918. 10/04/2020. Disponible en https://www.rfc-es.org/rfc/rfc1918-es.txt

GOMEZ, Remmy. plan de migración de ipv4 a ipv6 para una red de un proveedor de servicios de internet. 05/05/2020 Disponible en http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid=S2075-89362016000100006&lng=pt&nrm=iso

AFRINIC. Afrinic History. 08/05/2020. Disponible en https://www.afrinic.net/history

DELL. Servidor dell poweredge 2950. 21/03/2020 Disponible en https://www.dell.com/downloads/emea/products/pedge/es/PE2950_Spec_Sheet_Quad.pdf

FORITGATE. Fortiap Series. 04/04/2020. Disponible en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_11ac_Series.pdf

Fortinet.com. (2020). Fortigate 100E Series. Fortigate. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_100E_Series.pdf

MONTANEZ PRIETO, Juan Pablo. Propuesta para la migración del protocolo ipv4 a protocolo ipv6 para la secretaria del sisben de la alcaldia de tunja. 12/05/2020. Disponible en https://doi.org/10.1017/CBO9781107415324.004

SABOGAL ORTIZ, Arth Grossy. Elaboración de una guía abierta para la administración de riesgos de seguridad en el protocolo de internet ipv6 sobre estándares de enrutamiento dinámico en equipos con plataforma cisco. 09/05/2020. Disponible en https://repository.unad.edu.co/handle/10596/12015

SOLVETIC. Características IPv4. 29/04/2020. Disponible en https://www.solvetic.com/page/recopilaciones/s/internet/caracteristicas-diferencias-protocolo-internet-ipv4-ipv6.

## ANEXOS

### Anexo 1

Tabla 7:Inventario De Hardware de la red interna

| # | Tipo de Dispositivo | Marca | Tipo de dispositivo | Modelo | Sistema Operativo | IPv 6 |
|---|---|---|---|---|---|---|
| 1 | Router ISP UNE | Cisco | Router internet 50 megas | C860 | Cisco IOS | NO |
| | Router ISP ETB | Cisco | Router internet 20 megas | C890 | Cisco IOS | NO |
| 1 | Switch | Cisco | centro de cableado piso 1 | Catalyst 2960s | Cisco IOS LAN Base | SI |
| 2 | Switch | Cisco | centro de cableado piso 2 | Catalyst 2960s | Cisco IOS LAN Base | SI |
| 3 | Switch | Cisco | centro de cableado piso 3 | Catalyst 2960s | Cisco IOS LAN Base | SI |
| 4 | Switch | Cisco | centro de cableado piso 4 | Catalyst 2960s | Cisco IOS LAN Base | SI |
| 5 | Servidor | Hp | Servidor de archivos (Delta2) | Proliant Dl360 gen3 | Windows server 2003 | NO |
| 6 | Servidor | Hp | Controlador de dominio (Delta4) | Proliant Dl360 gen3 | Windows Server 2003 Estándar Edition | NO |

| | | | | | | |
|---|---|---|---|---|---|---|
| 7 | Servidor | Hp | Sistema de monitoreo (Delta3) | Proliant Dl360 gen3 | Windows Server 2003 Estándar Edition | NO |
| 8 | Servidor | Dell | Servidor de contabilidad (Delta5) | PowerEdge 2950 | Server 2016 Datacenter | SI |
| 9 | Servidor | Dell | Servidor CRM (Delta1) | PowerEdge 2950 | Server 2016 Datacenter | SI |
| 10 | Firewall | Fortinet | Seguridad perimetral | Fortigate 100E | Fortios | SI |
| 11 | Access Point | Fortinet | Punto de acceso Wifi pisos 1-2 | Fortiap 223E | Fortios | SI |
| 12 | Access Point | Fortinet | Punto de acceso Wifi pisos 3-4 | Fortiap 223E | Fortios | SI |
| 13 | TOTAL: 14 Host | | | | | |

Fuente: autor (2020)

**Anexo 2**

Tabla 8: Inventario de Software

| Nombre | Dirección IPv4 | Servicio o Aplicativo | Versión | URL de Acceso |
|---|---|---|---|---|
| Delta1 | 192.168.16.100<br>192.168.16.101 | CRM HISTORICO | Microsoft Dynamics CRM 4.0 | Delta5.gammalocal.com:8787 |
| Delta2 | 192.168.16.102<br>192.168.16.103 | Almacenamiento HP P6300 command view | V10.3.0.130517 | http://<br>Delta5.gammalocal.com/spog |
| Delta3 | 192.168.16.104<br>192.168.16.105 | Solar Winds | Windows Server 2012 R2 | https://soporte.gamma.com/otrs<br>index.pl?Action=/ |
| Delta4 | 192.168.16.106<br>192.168.16.107 | Controlador de Dominio BCK | Windows Server 2003 Estándar | Delta4.gammalocal.com:12446 |
| Delta5 | 192.168.16.108<br>192.168.16.109 | Sistema Administrativo y Financiero | siesa 8.5 | Delta5.gammalocal.com:42222 |

Fuente: autor (2020)

**Anexo 3***:*

Tabla 9 :Servidor Proliant Dl360 Gen3

| ESPECIFICACION | Servidor HP Proliant DL 360 G3 |
|---|---|
| Procesadores | Intel Xeon 3.06 GHz |
| Memoria RAM | Módulo DDR SDRAM 2 x 512MB a 255 MHz |
| Memoria | 8GB máximo slots DIMM 184pin x 4 slots |
| Almacenamiento | Nivel de RAID 0, RAID 1, RAID 10, RAID 5 |
| Almacenamiento interno máximo | Hasta 1,8 TB |
| Almacenamiento interno | 4 o 6 unidades SAS de 3,5" conectables en marcha (a 10.000 y 15.000 rpm) /unidades SATA (7.200) o 8 unidades SAS de 2,5" conectables en marcha (a 10.000 rpm) |
| Protocolo de enlace de datos | Ethernet, Fast Ethernet, Gigabit Ethernet |
| Sistemas operativos | Microsoft Windows 2000 Advanced Server, Red Hat Linux 8.0, Red Hat Linux Advanced Server 2.1, SuSE Linux Enterprise Server 7, UnitedLinux 1.0, Microsoft Windows 2003 Server, Microsoft Windows NT Server 4.0, Microsoft Windows NT Server 4.0 Enterprise Edition, Microsoft Windows NT Server 4.0 Terminal Edition, Novell NetWare 5.1 |

Fuente: Cnet,(2020). HP ProLiant DL360 G3.

**Anexo 4**

Tabla 10: Servidor DELL Poweredge 2950

| ESPECIFICACION | Servidor DELL Poweredge 2950 Intel Xeon E5310 |
|---|---|
| Procesadores | Hasta dos procesadores de secuencia de doble núcleo Intel Xeon 5000 con 3.0 GHz de frecuencia de reloj o hasta dos procesadores de secuencia de doble núcleo Intel Xeon 5100 con 3.0 GHz de frecuencia de reloj o hasta dos procesadores de secuencia de cuatro núcleos Intel Xeon 5300 con 2.66 GHz de frecuencia de reloj |
| Memoria | Módulos DIMM de 256 MB/512 MB/1 GB/2 GB/4 GB con memoria intermedia completa (FBD) en pares coincidentes; 533 MHz o 667 MHz; 8 zócalos para admitir hasta 32 GB |
| Ranuras de E/S | Seis en total: tres ranuras PCI, con aumento PCIe con tres ranuras PCI Express (una de 1 x 4 y dos de 1 x 8) o dos ranuras PCI-X de 64 bits/133 MHz y una ranura PCI Express de 1 x 8; 2 tarjetas NIC Gigabit integradas; puerto de administración con DRAC5 opcional |
| Driver RAID complementario | PERC 4e/DC opcional (driver RAID PCI Express de canal dual); Adaptador PERC 5/E opcional para almacenamiento RAID externo |
| Almacenamiento interno máximo | Hasta 1,8 TB |
| Almacenamiento interno | 4 o 6 unidades SAS de 3,5” conectables en marcha (a 10.000 y 15.000 rpm) /unidades SATA (7.200) o 8 unidades SAS de 2,5” conectables en marcha (a 10.000 rpm) |

| | |
|---|---|
| Tarjeta de interfaz de red | NIC Gigabit Ethernet Broadcom NetXtreme II 5708 dual integrada. NIC Ethernet con compensación de carga y capacidad de recuperación. TOE (motor de carga TCPIP) compatible con Microsoft Windows Server 2003, SP1 o superior con Scalable Networking Pack. Tarjetas NIC complementarias opcionales: Adaptador de puerto dual Intel PRO/1000 PT, Gigabit, Copper, PCI-E x4; adaptador de servidor de un solo puerto Intel PRO/1000 PT, Gigabit, Copper, PCI-E x1; |
| Fuente de alimentación | Fuente de alimentación estándar de 750 vatios conectable en marcha, fuente de alimentación redundante opcional de 750 vatios conectable en marcha; conmutación automática universal de 110/220 voltios |
| Sistemas operativos | Microsoft Windows Server 2003 R2, Standard, Enterprise y Web Edition, x64, Standard y Enterprise Edition; Microsoft Windows Storage Server 2003 R2, Workgroup, Standard, Enterprise Edition; Red Hat Linux Enterprise v4, ES y ES EM64T; SUSE Linux Enterprise Server 9 EM64T, SP3 |

Fuente: Dell,(2020). SERVIDOR DELL POWEREDGE 2950. Dell.com.

**Anexo 5**

Tabla 11: Cortafuegos Fortigate 100E

| ESPECIFICACION | Fortigate 100E |
|---|---|
| *Latencia de Firewall* | 3 µs |
| Cantidad de políticas | 10.000 |
| Nuevas sesiones por segundo | 30.000 |
| Túnel VPN IPsec | 10000 |
| Velocidad VPN IPsec | 250 Mbps |
| Cantidad de switch soportados | 24 |
| Cantidad de AP soportados | 64 |
| Cantidad de token soportados | 5000 |
| Alta disponibilidad | si |
| Energía requerida | 100–240V AC, 60–50 Hz |
| Dominios virtuales | 10 |
| RED | Compatibilidad con IPV4 e IPV6 |
| Almacenamiento inicial | 400Gb |

Fuente: Fortigate, (2020). Fortigate 100E Series

**Anexo 6**

Tabla 12: FORTIAP 223E

| ESPECIFICACION | FORTIAP 223E |
|---|---|
| Tipo de hardware | Indoor AP |
| Numero de radios | 2 + 1 BLE |
| Numero de Antenas | 4 External + 1 Internal BLE |
| Radio 1 Capacidades | 2.4 GHz b/g/n (2x2:2 Stream) 20/40 MHz (256 QAM) |
| Radio 2 Capacidades | 5 GHz a/n/ac (2x2:2 Stream) 20/40/80 MHz (256 QAM) |
| Velocidad máxima de datos | Radio 1: up to 400 Mbps Radio 2: up to 867 Mbps |
| Interfaces | 1x 10/100/1000 Base-T RJ45 |
| SSID simultáneos | 16 |
| Autenticación de usuario / dispositivo | Wpa, wpa2, wpa3, web, web cautive portal |
| Potencia máxima de transmisión | 2.4 GHz: 23 dBm / 200 mW 5 GHz: 24 dBm / 251 mW |
| Tipos de SSID compatibles | Local-Bridge, Túnel, Mesh |
| Coexistencia celular | si |
| Demodulación (MLD) | si |
| Modo Sniffer de paquetes | Si |
| Analizador de espectro | si |

Fuente: Fortinet, (2020). Fortiap Series.

**Anexo 7**

Tabla 13: Switch Cisco Catalyst 2960s

| ESPECIFICACION | SWITCH CISCO CATALYST 2960S |
|---|---|
| Tipo de interruptor | Gestionado |
| MIB, soporte | si |
| Calidad del servicio QoS | si |
| Multidifusión | si |
| Administración basada en Web | si |
| Cantidad de puertos básicos de conmutación | 24 |
| Puertos tipo básico de conmutación RJ-45 Ethernet | Fast Ethernet (10/100) |
| Estándares de red | IEEE 802.1p, IEEE 802.1x, IEEE 802.3af |
| Rendimiento | 6.5 Mbps |
| Algoritmos de seguridad soportados | 802.1x RADIUS |
| Memoria interna | 128MB |
| Memoria Flash | 64MB |
| Ancho de banda | 16 Gbit/s |
| Software incluido | Cisco IOS LAN Base |

Fuente: Spdigital. (2019). Catalyst 2960.