UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

PROPUESTA TECNOLÓGICA

"DISEÑO DE LA TRANSICIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LA EMPRESA GRUPO JATIVA CON BASE EN CONSIDERACIONES DE SEGURIDAD EN IMPLEMENTACIÓN DE IPV6."

Propuesta Tecnológica presentada previo a la obtención del Título de Ingenieros en Informática y Sistemas Computacionales.

Autores:

Montaleza Paucar Paúl Andrés

Jativa Reyes Angel Polivio

Tutor Académico:

Ing. M.Sc. Manuel William Villa Quishpe

LATACUNGA – ECUADOR

2022

DECLARACIÓN DE AUTORÍA

Nosotros, Jativa Reyes Angel Polivio y Montaleza Paucar Paúl Andrés, declaramos ser los autores del presente proyecto de investigación: "diseño de la transición del protocolo IPv4 hacia IPv6 en la empresa grupo Jativa con base en consideraciones de seguridad en implementación de IPv6.", siendo Ing. M.Sc. Manuel William Villa Quishpe tutor del presente trabajo; y eximo expresamente a la Universidad Técnica de Cotopaxi y a sus representantes legales de posibles reclamos o acciones legales.

Además, certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

Jativa Reyes Angel Polivio
C.I: 080423142-1

Montaleza Paucar Paúl Andrés
C.I:2350192536-6

AVAL DEL TUTOR DEL PROYECTO DE TITULACIÓN

En calidad de Tutor del Trabajo de Investigación sobre el título:
"DISEÑO DE LA TRANSICIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LA EMPRESA GRUPO JATIVA CON BASE EN CONSIDERACIONES DE SEGURIDAD EN IMPLEMENTACIÓN DE IPV6.", de JATIVA REYES ANGEL POLIVIO Y MONTALEZA PAUCAR PAUL ANDRES, de la carrera de SISTEMAS DE INFORMACIÓN, considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Proyecto que el Consejo Directivo de la Facultad de CIENCIAS DE LA INGENIERÍA Y APLICADAS de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, 17 de marzo 2022

El Tutor

.....

Ing. Manuel William Villa Quishpe
Cédula: 180338695-0

APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

En calidad de Tribunal de Lectores, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la FACULTAD de CIENCIAS DE LA INGENIERÍA Y APLICADAS; por cuanto, los postulantes: JATIVA REYES ANGEL POLIVIO Y MONTALEZA PAUCAR PAUL ANDRES con el título de Proyecto de titulación: **"DISEÑO DE LA TRANSICIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LA EMPRESA GRUPO JATIVA CON BASE EN CONSIDERACIONES DE SEGURIDAD EN IMPLEMENTACIÓN DE IPV6."** han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación de Proyecto.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, 17 de marzo 2022

Para constancia firman:

Lector 1 (Presidente)

Nombre: Ing. Rubio Peñaherrera Jorge Bladimir

CC:050222229-2

Lector 2

Nombre: Ing. Cadena Moreano José Augusto

CC:050155279-8

Lector 3

Nombre: Ing. Llano Casa Alex Christian

CC:050258986-4

GJ
GRUPO JATIVA
IMPORTADORES
DIR. CALLE AMBATO Y EJECITO SECTOR CODESA
Tlf: 098615736
ESMERALDAS - ECUADOR

AVAL DE IMPLEMENTACIÓN

Mediante el presente documento pongo a consideración que los señores: Montaleza Paucar Paul Andrés portador de la cedula de ciudadanía 23501925-36 y Jativa Reyes Angel Polivio portador de la cedula de ciudadanía 080423142-1 estudiantes de la Universidad Técnica de Cotopaxi de la Carrera de Ingeniería en Informática y Sistemas Computacionales realizaron la implementación de su propuesta tecnológica bajo el nombre de **"DISEÑO DE LA TRANSICIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LA EMPRESA GRUPO JATIVA CON BASE EN CONSIDERACIONES DE SEGURIDAD EN IMPLEMENTACIÓN DE IPV6.";** trabajo que fue desarrollado de manera satisfactoria logrando obtener resultados positivos, en los meses de Octubre 2021 hasta Marzo 2022.

Es todo cuanto puedo certificar en honor a la verdad y autorizo al interesado hacer uso del presente documento en cuanto estime conveniente mientras se encuentre dentro del marco legal.

Atentamente,

Firmado electrónicamente por:
ANGEL EDMUNDO JATIVA PEÑA

Angel Edmundo Jativa Peña

CI: 171076281-4

GERENTE GrupoJativa S.A.

AGRADECIMIENTO

A nuestra querida Universidad, por la colaboración e iniciativa en esta Propuesta Tecnológica.

Al Ing. Manuel Villa quien nos ha ayudado, guiando y corregido como tutor de nuestro proyecto.

De la misma manera a nuestros lectores de tesis, Ing. Jorge Rubio, Ing. José Cadena e Ing. Alex Llano quienes nos han guiado y corregido.

Gracias a esto sea podido culminar este proyecto de manera exitosa.

DEDICATORIA

Con mucho cariño dedicamos:

A nuestros padres

Este trabajo, que es fruto de su esfuerzo y sacrificio constante, para hacer de nosotros seres humanos dignos, gracias a su apoyo incondicional durante nuestro proceso de formación académica.

ÍNDICE GENERAL

ÍNDICE DE TABLA

ÍNDICE DE FIGURAS

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TÍTULO: "DISEÑO DE LA TRANSICIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LA EMPRESA GRUPO JATIVA CON BASE EN CONSIDERACIONES DE SEGURIDAD EN IMPLEMENTACIÓN DE IPV6."

Autores:

Montaleza Paucar Paul Andrés

Jativa Reyes Angel Polivio

RESUMEN

El presente proyecto de titulación se realizó en la Empresa grupo Jativa ubicada en Codesa primera parada frente al cuartel militar de la ciudad Esmeraldas, en donde mediante la aplicación de la encuesta se identificó que se tiene problemas con el protocolo de IPv4 como el bajo rendimiento en la trasmisión y problemas de seguridad al momento de enviar paquetes de datos, además de la mala estructuración de la red existente, por otra parte no cuenta con una administración propia de la red, estas acciones promovían que empresa sea vulnerable a ataques de terceros y depender de una administración externa para poder manejar su propia red, lo cual provoca una mayor inversión de tiempo y dinero, por tal motivo se genera la necesidad de migrar de IPv4 a Ipv6 en la empresa Grupo Jativa. Para su realización se utilizó metodologías de investigación, con el fin de dar a conocer el problema e identificar las necesidades primordiales. Para el desarrollo del proyecto se empleó los protocolos de: direccionamiento de IPv6 el cual nos permite conocer cómo funciona el mismo, 568 es el estándar del cableado para telecomunicaciones en edificios comerciales, 569 permite el diseño para la adecuación de rutas y espacios de canalización, 606 provee la administración de la infraestructura de la red y 607 establece la protección de los equipos de telecomunicación. Como resultado se obtuvo la migración de IPv4 a IPv6 en la empresa grupo Jativa, destacando el aumento de trasmisión de paquetes en un 87% y una mejor codificación de los datos gracias a los protocolos de seguridad implementados en IPv6, optimizando favorablemente los recursos como el tiempo de trasmisión de datos y el dinero que se invertía en una administración externa.

Palabras claves: Migración, Protocolos, IPv6, Seguridad, Trasmisión

TECHNICAL UNIVERSITY OF COTOPAXI

FACULTY OF ENGINEERING SCIENCES AND APPLIED

THEME: "DESIGN OF THE TRANSITION FROM IPV4 TO IPV6 PROTOCOL IN GRUPO JATIVA COMPANY BASED ON SECURITY CONSIDERATIONS IN IPV6 IMPLEMENTATION."

Authors:

Montaleza Paucar Paul Andrés

Jativa Reyes Angel Polivio

ABSTRACT

This degree project was conducted in the company Jativa group located in Codesa first stop in front of the military barracks in the city of Esmeraldas, where through the application of the survey it was identified that there are problems with the IPv4 protocol such as low performance in the transmission and security problems when sending data packets, In addition to the poor structuring of the existing network, on the other hand does not have its own network administration, these actions promoted that the company is vulnerable to attacks from third parties and depend on an external administration to manage its own network, which causes a greater investment of time and money, for this reason it generates the need to migrate from IPv4 to IPv6 in the company Grupo Jativa. Research methodologies were used for its realization, in order to make the problem known and identify the main needs. For the development of the project the following protocols were used: IPv6 addressing which allows us to know how it works, 568 is the standard for telecommunications cabling in commercial buildings, 569 allows the design for the adequacy of routes and channeling spaces, 606 provides the administration of the network infrastructure and 607 establishes the protection of telecommunication equipment. As a result, the migration from IPv4 to IPv6 was obtained in the company Grupo Jativa, highlighting the increase of packet transmission in 87% and a better data encryption thanks to the security protocols implemented in IPv6, optimizing favorably the resources such as data transmission time and the money that was invested in an external administration.

Keywords: Migration, Protocols, IPv6, Security, Transmission

UNIVERSIDAD TÉCNICA DE COTOPAXI

CENTRO DE IDIOMAS

AVAL DE TRADUCCIÓN

En calidad de Docente del Idioma Inglés del Centro de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal **CERTIFICO** que:

La traducción del resumen al idioma Inglés del artículo cuyo título versa: **"DISEÑO DE LA TRANSICIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LA EMPRESA GRUPO JATIVA CON BASE EN CONSIDERACIONES DE SEGURIDAD EN IMPLEMENTACIÓN DE IPV6"** presentado por: **Montaleza Paucar Paul Andrés y Jativa Reyes Angel Polivio,** estudiantes de la Carrera de: **Ingeniería en Informática y Sistemas Computacionales** perteneciente a la **Facultad de Ciencias de la Ingeniería y Aplicadas,** lo realizaron bajo mi supervisión y cumple con una correcta estructura gramatical del Idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo a los peticionarios hacer uso del presente aval para los fines académicos legales.

Latacunga, 24 marzo del 2022

Atentamente,

UNIVERSIDAD TÉCNICA DE COTOPAXI LATACUNGA - ECUADOR

CENTRO DE IDIOMAS

Mg. Marco Paúl Beltrán Semblantes

DOCENTE CENTRO DE IDIOMAS-UTC
CI: 0502666514

1 INFORMACIÓN GENERAL

Título:

Diseño de la transición del protocolo ipv4 hacia ipv6 en la empresa GrupoJativa con base en consideraciones de seguridad en implementación de ipv6.

Fecha de inicio:

25 de octubre del 2021.

Fecha de finalización:

Marzo 2022.

Lugar de ejecución:

Esmeraldas/Esmeraldas/Esmeraldas/Codesa primera parada frente al cuartel militar.

Facultad que auspicia:

Ciencias de la Ingeniería y Aplicadas.

Carrera que auspicia:

Ingeniería en Informática y Sistemas Computacionales.

Proyecto de investigación vinculado:

Redes.

Equipo de Trabajo:

Tutor: Ing. Manuel William Villa Quishpe.

Postulantes: Jativa Reyes Ángel Polivio, Montaleza Paucar Paul Andres.

Área de Conocimiento:

06 Información y Comunicación (TIC)/ 061 Información y Comunicación (TIC)/Base de datos, diseño y administración de redes.

Línea de investigación:

Tecnología de la información y comunicación

Sub líneas de investigación de la Carrera:

Diseño, implementación y configuración de redes y Seguridad Computacional, aplicando normas y estándares internacionales.

2 DISEÑO INVESTIGATIVO DE LA PROPUESTA TECNOLÓGICA

2.1 INTRODUCCIÓN

Para abordar esta temática se empezará por comentar que desde hace más de tres décadas, las redes de telecomunicaciones han venido creciendo exponencialmente generando una mayor demanda de servicios y oportunidades en la red mundial de internet; con el aumento de las tecnologías computacionales y de comunicaciones, ha aumentado el proceso de innovación tecnológica en los diversos dispositivos tanto alámbricos como inalámbricos, como por ejemplo, celulares, puntos de acceso, tabletas, servidores, equipos de almacenamiento entre otros, que comenzaron a incrementar la conectividad en muchas redes en el mundo y para ello han tenido que hacerlo con direcciones de internet que permiten establecer conexiones para cada elementos conectado a la red, estas direcciones se conocen como direcciones IP (Internet Protocol Versión 4), que en estos momentos entraron a una fase de agotamiento final, a partir de diversos grupos de trabajo definió el RFC 2460 (Especificaciones del Protocolo Internet Versión 6 (IPv6) que dio origen al nuevo protocolo de conectividad denominado IPv6 o IPng (Next Generation Internet Protocol).

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

2.2 TÍTULO DE LA PROPUESTA TECNOLÓGICA

2.3 TIPO DE ALCANCE

Este proyecto busca orientar las entidades que estén interesadas en el proceso de transición desde IPV4 a IPV6, teniendo en cuenta las normativas emitidas por MINTIC (Ministerio de Tecnologías de la Información y la Comunicación). Este proyecto describe las diferentes fases para el proceso de transición, las directrices concretas y fundamentales al momento de realizar la planeación de la transición [1].

2.4 ÁREA DE CONOCIMIENTO

Área: 06 Información y Comunicación (TIC)/ 061 Información y Comunicación (TIC)/Base de datos, diseño y administración de redes.

Sub-Área: Diseño, implementación y configuración de redes y Seguridad Computacional, aplicando normas y estándares internacionales.

2.5 SINÓPSIS DE LA PROPUESTA TECNOLÓGICA

GrupoJativa demuestra algunos inconvenientes con su protocolo en IPv4, como modelo para analizar las falencias que presenta como es el desperdicio de banda ancha, bajo rendimiento al momento de la transmisión, la poca seguridad al momento de enviar paquetes de datos, etc. Para lo cual, se busca una migración de protocolos IPv4 a IPv6 con la finalidad de solventar las falencias que presentan los protocolos actuales tanto en seguridad como en transmisión de información.

2.6 OBJETO DE ESTUDIO Y CAMPO DE ACCIÓN

2.6.1 Objeto de Estudio

Para definir el objeto, el cual es de suma importancia para el desarrollo de la propuesta de redes, se debe realizar un análisis del tema en el cual se realizará la investigación y desarrollo, en este caso es: Diseño de la transición del protocolo IPv4 a IPv6 en la empresa GrupoJativa con base en consideraciones de seguridad en implementación de ipv6.

- Se puede distinguir Investigar sobre la configuración de Ipv6 con referencias en trabajos pasados para poder realizar la migración de Ipv4 a Ipv6.
- Obtener información de campo mediante el uso de técnicas e instrumentos de investigativos para satisfacer las necesidades de los involucrados.
- Realizar la migración de ipv4 a ipv6 aplicando los protocolos para mejorar la seguridad y la velocidad del envío de datos.

2 aspectos de suma trascendencia que se tienen que detectar, el primero es el problema de investigación, por el que se lograra obtener el objeto de la indagación. En el asunto tenemos la posibilidad de distinguir el problema de indagación como: “La migración de protocolos IPv4 a IPv6”, dando como consecuencia el siguiente objeto de investigación: “La empresa GrupoJativa de la ciudad de Codesa”.

2.6.2 Campo de Acción

Y para el campo de acción, el cual está definido por Nomenclatura Internacional de la UNESCO para los campos de Ciencia y Tecnología, tomaremos la siguiente nomenclatura: 1203.09 Diseño Con Ayuda del Ordenador / 1203.18 Sistemas de Información, Diseño Componentes

2.7 SITUACIÓN PROBLEMÁTICA Y PROBLEMA

2.7.1 Situación Problemática

La globalización junto con el desarrollo tecnológico pone en una nueva perspectiva al comercio mundial, puesto que ha permitido desarrollar espacios comerciales rompiendo las barreras de tiempo y espacio, las transacciones económicas se formalizan en tiempo real acelerando el crecimiento económico [2]. El comercio electrónico es una herramienta que ha permitido cruzar fronteras y realizar transacciones de compra y venta de servicios de forma rápida y eficaz [2].

Es importante que en el Ecuador, al ser un país en vías de desarrollo, se tome en consideración todos los cambios relacionados con la globalización y el desarrollo tecnológico, debido a que existen repercusiones que afectan a quienes no se preparen de forma adecuada para enfrentar esos vertiginosos cambios, especialmente en lo que concierne a la competencia, implementación de plataformas digitales que permitan poner al país en estos nuevos entornos de negocios y sean potenciadores del crecimiento económico, articulando la industria del país con los desarrollos tecnológicos, para que sirva como vitrina al mundo de los productos y servicios hechos en el Ecuador [2].

2.7.2 Problema

Desde la creación de las redes TCP/IP, el direccionamiento lógico ha sido el eje fundamental que soporta la identificación de los hosts en una red [3]. Este direccionamiento fue concebido con una longitud de 32 bits (IPv4), que se creía sería suficiente para las proyecciones de crecimiento de las redes que se tenía en ese entonces (esto nos daba un margen de más de 400 millones de direcciones distintas). Pero el auge de Internet y su crecimiento exponencial, ha llevado a que este esquema sea insuficiente, de allí que la IETF (Internet Engineering Task Force) replantea un nuevo esquema de direccionamiento lógico e hiciese la propuesta que está en marcha hace algunos años, las direcciones IPv6 [3].

A raíz de los estudios que prevén el agotamiento de las direcciones públicas IPv4, la IETF inició el estudio de un nuevo esquema de direccionamiento lógico jerárquico que solucionara dicha problemática y que adicionalmente permitiese adicionar esquemas más dinámicos y seguros

[3]. Fue así como a principios de los años 90, se dio a conocer este nuevo esquema que consiste de 128 bits que se representan en 8 grupos de 4 dígitos hexadecimales separados por dos puntos (:). IPv6 adiciona un sinnúmero de características que permiten asegurar su uso por muchos años [3]. Dichas características están representadas en seguridad, autoconfiguración y movilidad [3].

IPv4 demuestra algunos inconvenientes en las instituciones como por ejemplo se ha tomado a GrupoJativa como modelo para analizar los inconvenientes que presenta como es el desperdicio de banda ancha, bajo rendimiento al momento de la transmisión, la poca seguridad al momento de enviar paquetes de datos, etc. Esta investigación también servirá para que los usuarios comiencen a tener conocimiento de este protocolo IPv6, como nuevo protocolo de la nueva generación, todo esto con el fin de ganar seguridad, crecimiento de usuarios y por supuesto mucha más velocidad de la información y calidad de servicio, etc. [4]

2.8 HIPÓTESIS

¿Cuál es la mejoría en tiempos de velocidad y seguridad de envíos de datos en la empresa GrupoJativa?

2.9 OBJETIVOS

2.9.1 Objetivo General

Migrar de IPv4 a IPv6 en la empresa GrupoJátiva ubicada en el cantón Esmeraldas, mediante el uso de técnicas y herramientas investigadas para mejorar la seguridad y la velocidad del envío de datos.

2.9.2 Objetivos Específicos

- Definir las bases teóricas acerca de Ipv6 con referencias en trabajos pasados para poder realizar la migración de Ipv4 a Ipv6.
- Obtener la información necesaria mediante la aplicación de una encuesta para satisfacer las necesidades de los involucrados.
- Realizar la migración de IPv4 a IPv6 aplicando los protocolos para mejorar la seguridad y la velocidad del envío de datos.

2.10 DESCRIPCIÓN DE LAS ACTIVIDADES Y TAREAS PROPUESTAS CON LOS OBJETIVOS ESTABLECIDOS

Tabla 2.1 Descripción de las actividades y tareas propuestas

OBJETIVO ESPECÍFICO	ACTIVIDAD	RESULTADO	TÉCNICAS E INSTRUMENTOS
Definir las bases teóricas acerca de Ipv6 con referencias en trabajos pasados para poder realizar la migración de Ipv4 a Ipv6.	Identificar antecedentes investigativos. Comparar los conceptos de varios Autores.	Fundamentación Teórica.	Investigación Bibliográfica. Fichas Bibliográficas.
Aplicar técnica de campo mediante una encuesta para recopilar la información necesaria por parte de los involucrados.	Diseñar cuestionarios para levantar información.	Cuestionario de encuesta o entrevista.	Encuesta. Entrevista Observación.
Realizar la migración de IPv4 a IPv6 aplicando los protocolos para mejorar la seguridad y la velocidad del envío de datos.	Investigar sobre los diversos protocolos en ipv6. Identificar los protocolos necesarios para su aplicación en la red.	Mejora en el nivel de seguridad y transmisión de datos en ipv6.	Investigación Bibliográfica.

3 JUSTIFICACIÓN

IPV4 es el primer protocolo que se creó para el uso de Internet. Sin embargo, las direcciones IP que emplea se han agotado, lo que limita el crecimiento de diversas conexiones [5]. Por tanto, es difícil su adecuación a las nuevas aplicaciones, más aún cuando a nivel mundial se presenta el crecimiento continuo de las mismas, las cuales requieren una IP pública única, ejemplo de ello son: los teléfonos con tecnología VoIP, televisión y radio, seguridad, televigilancia, mercados virtuales, juegos, videoconferencia, redes inalámbricas, etc. [5]. Sumado a ello las estadísticas evidencian que este tipo de protocolo no permite la asignación 15 de nuevas direcciones IP a los usuarios de diferentes empresas u organizaciones del sector educativo, bancario, industria, entre otros [5].

En la actualidad, se necesitan protocolos que garanticen unas características adecuadas a los tipos de tráfico de datos, pues cada día crece de forma constante el número de usuarios que acceden a la red desde diversos dispositivos, esta creciente demanda de conectividad ha hecho que cada vez sean más escasas las IP públicas y se necesitan mejores prácticas para salvaguardar el flujo de información [5].

Ante el panorama descrito, surge el protocolo IPV6, el cual tiene como objeto subsanar las falencias observadas en el protocolo IPv4, como lo son: el agotamiento de direcciones IP y la seguridad de la información a través del envió cifrado y autenticado de paquetes, lo que permite mantener una transmisión más confiable y segura de la Información [5]. También, posee un sencillo mecanismo de autoconfiguración y velocidad en la transmisión; además entre sus características más importantes se resaltan la cantidad ilimitada de espacio de direcciones IP y la calidad del servicio [5].

Ahora bien, teniendo en cuenta las bondades de este nuevo protocolo el Ministerio de las TIC emitió la circular 002/2011, mediante la cual busca que todas las entidades que hagan parte del programa de Gobierno en línea, empiecen a llevar a cabo los estudios para la migración al protocolo IPV6 [5].

Por último, se resalta que el camino hacia IPV6 es un paso de evolución e integración necesaria, por lo cual se debe asegurar el futuro frente al inevitable auge tecnológico que aumenta cada día y por una red global más efectiva, que fortalezca y apoye la creciente movilidad de usuarios de Internet, redes domésticas y la aparición de nuevas aplicaciones que requieren mejores tiempos de respuesta, disponibilidad de ancho de banda y sobretodo seguridad [5].

Actualmente, la necesidad de un protocolo que brinde las garantías necesarias para que una institución o compañía cuente con características adecuada en el tráfico de datos es notoria ante la creciente demanda de conexión que es realizada a través de múltiples dispositivos, y a esto se le suma que las IP's públicas se vuelvan más escasas y obliga a los expertos a mejorar las prácticas para salvaguardar la corriente de información [1]. El protocolo IPV6 es una solución necesaria para corregir la gran cantidad de errores y falencias que se han manifestado en la implantación del IPV4, lo que en pocas palabras significa que sus beneficios quedan reflejados en diversas áreas de la infraestructura donde se realice la migración, llevando al protocolo IPV6 a tomar la vanguardia en el campo de la tecnología, logrando aplicar mejores tiempos de respuesta a esas nuevas aplicaciones que surgen en el mercado, sin dejar de mencionar que realizar esta transición permite que una compañía tenga una red más segura en la cual podrá confiar [1].

4 BENEFICIARIOS DEL PROYECTO

4.1 DIRECTOS

Propietarios, accionistas y empleados de la empresa "GrupoJativa", ubicada en la ciudad de Codesa, provincia de Esmeraldas.

Cantidad de beneficiarios: 15

4.2 INDIRECTOS

Clientes de la empresa "GrupoJativa" y el sector tecnológico.

Cantidad de beneficiarios: Clientes.

5 MARCO TEÓRICO

5.1 Direccionamiento IP

Es la identificación de forma lógica y jerárquica de la interfaz de un dispositivo o host que se conecta a la red y maneja el protocolo de internet, dicha identificación denominada también dirección consta de una consecución de unos y ceros en el caso de direcciones IPv4, y en el caso de direcciones IPv6, éstas están basadas en secuencias del sistema hexadecimal [6].

5.1.1 Función.

El direccionamiento IP es un punto fundamental dentro del protocolo de internet, básicamente permite el encaminamiento de paquetes desde una fuente de información hacia un destino a través de redes interconectadas entre sí [6].

5.1.2 Tipos de Direccionamiento.

Según [6], existen diferentes tipos de direccionamiento que permiten conectar redes de computadoras para poder encaminar paquetes de información desde un emisor hacia un receptor ubicados en cualquier parte de la red, los principales y más utilizados son:

- Direccionamiento IPv4
- Direccionamiento IPv6

5.2 Direccionamiento IPv4.

Está expresado por un conjunto de números binarios compuestos por cuatro octetos separados por puntos, conformando un total de 32 bits, también se pueden expresar en notación decimal, correspondiendo cada octeto a un número decimal entre 0 y 255 [6]. Por ejemplo, una dirección IP está representada de la siguiente manera [6]:

Tabla 5.1 Direccionamiento IPv4 [6]

Direccionamiento IP		
	Forma Binaria	**Equivalencia Decimal**
Direccionamiento Mínimo	00000000. 00000000. 00000000. 00000000	0.0.0.0
Direccionamiento Máximo	11111111. 11111111. 11111111. 11111111	255.255.255.255
Ejemplo 1	11000000.10101000.00000001.000000001	192.168.1.1
Ejemplo 2	11100000.00000010.00000010.00000010	224.2.2.2

Como podemos observar en la tabla superior, encontramos la dirección máxima y mínima que puede ser asignada a una interfaz, permitiendo dentro del direccionamiento IPv4 hasta un máximo de 4.294.967.296 direcciones posibles, sin embargo, para poder asignar direcciones IPv4 a la interfaz de un ordenador también se considera la clase de dirección y el dominio al que el dispositivo debe permanecer dentro de la red [6]. Una dirección IP se divide en un número de red y un número de host, donde el número de red es el contenido del octeto principal y el número de host es lo que queda de la dirección IP [7].

Tabla 5.2 Direccionamiento IPv4 con número de red y un número de host [6]

ESTRUCTURA DE UNA DIRECCION IPV4		DESCRIPCION
Representación Dirección IP	192.168.1.50/24	Es la representación más común para definir una dirección IP y el dominio al que pertenece.
Dirección de Red	192.168.1.0	Es una dirección que identifica a un grupo de host dentro de una misma red.
Dirección de Host	192.168.1.50	Es una dirección que pertenece a un rango válido de una red y es asignada a un host.
Dirección de Broadcast	192.168.1.255	Es la dirección que permite la comunicación a todos los host en una misma red.
Prefijo de Red	/24	Permite saber cuántos bits pertenecen a la dirección de red y cuantos a la dirección de host.

5.2.1 Clases de Direccionamiento IPV4 según [6]

Dentro de este tipo de direccionamiento se puede representar cinco clases:

- **Clase A.-** Establece el primer octeto para identificar a una red, mientras tanto los tres octetos restantes son asignados para hosts. Siendo que el número máximo de computadoras que se pueden conectar a una red de este tipo es 16777214, y el número máximo de redes que se pueden asignar es 126 [6].
- **Clase B.-** Establece los dos primeros octetos para identificar una red, y los dos últimos octetos se asignará a los hosts, siendo 65534 el número máximo de computadoras que pueden conectarse a una red de este tipo y el intervalo de red permitirá crear 16384 redes [6].
- **Clase C.-** Es una de las más utilizadas debido a que el número de redes que se puede crear con los tres primeros octetos es de 2097152, cada red tendrá un límite de 254 hosts; esto es muy útil para poder tener una buena distribución de la red [6].
- **Clase D (Multicast). -** Este tipo de direccionamiento tiene una función en específico, permite enviar tráfico multicast en una red. Entonces, es de suma utilidad cuando se desea transmitir servicios multicast como por ejemplo IPTV [6].

- **Clase E (Experimental). -** Se puede definir a este tipo de direccionamiento como experimental, debido a que se reservó para ponerlas en uso a futuro. Cabe recalcar que el número calculado de hosts para cada clase fue determinado con la fórmula 2 n-2, donde n es el número de bits que determina las direcciones de red. El -2 de la fórmula representa la dirección de red y la dirección de broadcast, ninguna de estas dos direcciones se puede asignar a un host. A continuación, realizamos una tabla con los rangos respectivos de cada clase [6]:

Tabla 5.3 Rango de direccionamiento IPv4 [6]

CLASE	RANGO DE DIRECCIONAMIENTO	MÁSCARA DE RED	RANGO DE DIRECCIONES PRIVADAS
A	1.0.0.0 – 126.0.0.0	255.0.0.0	10.0.0.0 – 10.255.255.255
B	128.0.0.0 – 191.255.0.0	255.255.0.0	172.16.0.0 – 172.31.255.255
C	192.0.0.0 – 223.255.255.0	255.255.255.0	192.168.0.0 – 192.168.255.255
D	224.0.0.0 – 239.255.255.255	-	-
E	240.0.0.0 – 255.255.255.255	-	-

5.3 Direccionamiento IPv6

Actualmente la operación del protocolo de internet a nivel mundial se basa cada vez con mayor fuerza sobre la nueva versión del protocolo IP, dando lugar sin duda a uno de las evoluciones más importantes llevadas a cabo en la historia del internet, brindando la posibilidad de que la red de redes pueda mantener su desarrollo y crecimiento de manera segura y constante [6]. El direccionamiento IPv6 tiene sus inicios en la década de los 90 bajo la responsabilidad del Internet Engineering Task Force y a la fecha aún se encuentran sumándole funcionalidades [7].

5.3.1 Definición

La dirección de Internet Protocol Version 6 (IPv6) es la identificación de forma lógica y jerárquica de una interfaz de red de un ordenador o de un nodo que se encuentre en una red de tipo IPv6, esta identificación es única para cada host localizado en la red y permite encaminar los paquetes IP entre host [6].

5.3.1.1 Características

El protocolo de direccionamiento IPv6 tiene características que lo diferencian de su predecesor IPv4 [8], las que tienen mayor relevancia son:

- Mayor cantidad de espacio para poder asignar direcciones en el host, debido a que cuenta con 128 bits en las direcciones IP, las posibilidades de identificación para un host no están limitadas por el rango de direccionamiento.
- Autoconfiguración de direcciones IP. Un nodo crea de forma automática una dirección de enlace local, esta dirección es usada comúnmente para la comunicación dentro de un nodo o router [6]. Esta dirección no interfiere con el proceso de envió hacia el exterior debido a que un host necesita configurar direcciones globales para comunicarse con otros nodos en la red [6].
- Posee un protocolo de Seguridad Integrada, también conocido como IPsec. Este protocolo está basado en estándares que brindan una mayor seguridad.
- Tiene un nuevo formato de encabezado, debido a que está conformado por menos campos y se elimina la verificación de encabezado.
- Capacidades de autenticación y privacidad.
- No más NAT, este proceso era comúnmente en direccionamiento IPv4, ya que sus direcciones públicas estaban limitadas, pero con direccionamiento IPv6 no será necesario una traducción de direcciones por la cantidad de direccionamiento que posee.
- Mejora la calidad de servicio (QoS) y la clase de servicio (CoS), también llamado Flow Labeling [6].
- Mejora el enrutamiento del tráfico multicast.

5.3.1.2 Representación

Al igual que la representación de direcciones IP en IPv4 se puede dar dos casos para representar direcciones IPv6, el primero es cuando la dirección se la representa en formato binario: Por ejemplo: 0000011101010100 0000110101010101 01010101010000… 0101010100010101, se divide en 8 bloques de 16 bits y la suma total de los bloques es de 128 bits [6]. Como se muestra en la tabla 1-5 [10].

Tabla 5.4 Representación de direcciones PI en IPv6 [6]

REPRESENTACION DE UNA DIRECCION IP EN BITS			
0101000000011111	0101000011000000	0101010000001111	0100001110100000
0100110011001100	1111000011000111	1110001100101011	0100001111100010

La segunda forma de representación es en formato hexadecimal, esto se realiza de la siguiente manera: Una vez que se haya dividido en 8 bloques de 16 bits cada uno, se procede a convertir

cada bloque a formato hexadecimal. Considerando que cada número hexadecimal está representado por 4 bits [6].

Tabla 5.5 Representación de direccionamiento hexadecimal en IPv6 [6]

REPRESENTACION DE UNA DIRECCÓN IP EN HEXADECIMAL			
501F	50C0	540F	43A0
4CCC	F0C7	E32B	43E2

Una vez finalizada la conversión de los grupos de bits en formato hexadecimal procedemos a colocar de forma continua los grupos de 4 números hexadecimales separados por dos puntos entre sí [6]:

Formato de Dirección IPv6: 501F:50C0:540F:43A0:4CCC:F0C7:E32B:43E2 [6]

Esta es la representación de una dirección IPv6 en formato Hexadecimal [6]. A su vez, podemos mencionar que debido a que la dirección es extensa hay reglas que permiten simplificar ciertos grupos en caso de ser necesario, por ejemplo: compresión de ceros [10].

5.3.2 Estructura de direccionamiento IPv6

En resumen, una dirección v6 tiene dos partes, una es el Prefijo, y el resto es la identificación de la interfaz en particular, es decir el Interface ID. A veces, vamos a disponer de unos bits extra conocidos como Subnet ID. Interface ID tienen que estar en un formato especial conocido como EUI-64 [9].

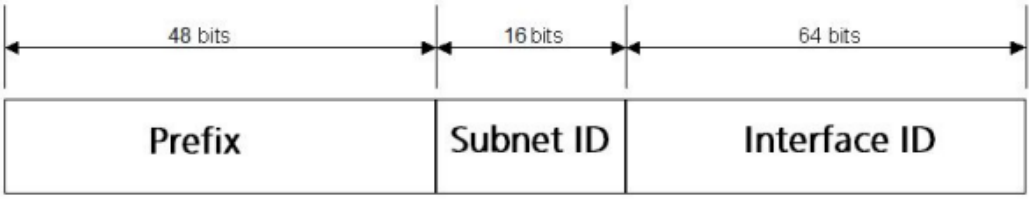


Figura 5.1 Esquema IPv6 [9]

El 77% del espacio total de direcciones IPv6 está aún reservado para futuros usos. Resumen de los prefijos más importantes:

0000::/8 - Sin especificar, Lookback (similar a 0.0.0.0/0 o 127.0.0.0/8)

2000::/3 - Global Unicast Addresses (similar a las públicas IPv4)

FC00::/7 - Unique Local Addresses (similar a las privadas IPv4)

FE80::/10 - Link-Local Unicast Addresses (similar al rango 169.254.0.0/16)

FF00::/8 - Multicast Adresses (similar al rango 224.0.0.0/4)

5.3.3 Representación de direccionamiento IPv6

Las direcciones IPv6 pueden comprimirse para una fácil lectura y escritura mediante tres métodos.

- **Grupos con todos "ceros", puede reemplazarse con un sólo cero.**

Ejemplo:

Antes: 2001:1291:0200:8738:0000:0000:0000:0001

Después: 2001:1291:0200:8738:0:0:0:0001

- **Quitar los ceros de la izquierda en los grupos que corresponda.**

Ejemplo:

Antes: 2001:1291:0200:8738:0:0:0:0001

Después: 2001:1291:200:8738:0:0:0:1

- **Múltiples grupos de ceros, pueden ser comprimidos utilizando los dos puntos (":"). Este método puede ser utilizado una vez, preferentemente donde cause más efecto.**

Ejemplo:

Antes: 2001:1291:200:8738:0:0:0:1

Después: 2001:1291:200:8738::1

5.3.4 Tipos de Direcciones IPv6

Las direcciones IPv6 se pueden clasificar según el propósito de encaminamiento de paquetes dentro de una red [10], estos son:

- **Unicast. -** Es el concepto más común de la comunicación entre host. Se refiere a que en una transmisión de paquetes de información se tendrá a un emisor y un receptor para enviar o recibir información. También se suele decir que este tipo de direcciones están asociadas a una única interfaz de host [6].
- **Multicast. -** Se refiere a que en la transmisión de paquetes de información van a existir varios receptores interesados pero una sola fuente de información. Este tipo de direcciones es una función específica del router, debido a que esta recepta del host

fuente un paquete, el router revisa su tabla de enrutamiento y replica los paquetes a todos los receptores que hayan informado del interés por recibir la información desde esa host fuente. Mediante este tipo de direccionamiento también se puede llegar a todos los dispositivos conectados en una red, este proceso se le conoce como el envío Broadcast de información. Es la principal diferencia respecto a su predecesor IPv4 [6].

- **Anycast. -** Se utiliza para identificar a un conjunto de receptores, el proceso se basa en que el host fuente de información envía los paquetes hacia el router, después el router se encarga de enviar únicamente al que considere cercano en su red [6].

5.3.5 Monitoreo de IPv6

Las pruebas de funcionalidad (monitoreo) en IPv6 no solo debe ser tenido en cuenta en la fase de pruebas del modelo de transición de IPv4 a IPv6, sino que también debe permitir establecer el nivel de funcionamiento y criticidad de las redes IPv6 ya en operación, por lo que es necesario tener en cuenta la detección y prevención de problemas, diagnóstico de fallas, determinación de acciones para la solución de problemas de seguridad y tener un plan de contingencias a la mano [11].

Las siguientes son las variables a tener en cuenta a la hora de realizar monitoreo de los servicios de red en IPv6 [12]:

- Medición de tráfico sobre interfaces y dispositivos de red [12].
- Estado de servicios [12].
- Estado de aplicaciones.
- Actividad de los hosts.
- Canales de comunicación hacia Internet.

Para ello es importante contar con herramientas de monitoreo, como por ejemplo analizadores de tráfico que provean análisis de interfaces de red, monitoreo de librerías de IPv6 y soporte sobre SNMP [11].

Cada entidad debe estar en capacidad de utilizar libremente las herramientas de test y/o de monitoreo una vez implementado IPv6, teniendo en cuenta que la complejidad de cada una de estas no es lo importante sino los resultados exitosos que arroje el mismo [13].

5.3.6 Seguridad de IPv6 en los Centros de Datos

Al momento de implementar IPv6 en las organizaciones, los centros de datos son los elementos importantes a revisar por ser los ejes centrales de todas las operaciones tecnológicas de la

empresa, por lo tanto, tal y como se menciona en muchas organizaciones [14], “Existen varias formas de introducir y operar IPv6 en Centros de Datos. Una forma es continuar con una operación IPv4 dentro del centro de datos y hacer algún tipo de translación en el borde (no recomendable de acuerdo a los lineamientos del gobierno), una segunda forma es usar la doble pila y una tercera es usar únicamente IPv6 [15].

En resumen, tenemos:

- Translación de IPv4 en el borde: En este escenario el centro de datos mantiene su infraestructura interna en IPv4 y hace algún tipo de translación a IPv6 en el borde [12].
- Pila Doble: Aquí encontramos pila doble a través todos los servicios del centro de datos o al menos en los que prestan servicios a usuarios [12]. También puede encontrarse pila doble solo en el borde mientras que las conexiones internas son IPv4 o IPv6 únicamente [12].
- Solo IPv6: Esta es generalmente la etapa final de la transición de un centro de datos a IPv6. Aquí encontramos IPv6 en todos los elementos del centro de datos [12]. Para ofrecer servicios a los usuarios legados de IPv4 se utiliza algún tipo de translación en el borde [12].

El uso de estos escenarios no es necesariamente en la forma secuencial descrita y tampoco ninguna es el mejor, el más correcto o el recomendado [12]. Cada uno ofrece diferentes beneficios y desventajas que deben ser analizados para seleccionar la mejor opción [12].

La mayoría de los aspectos de seguridad de IPv6 se aplican a los centros de datos los cuales pueden encontrarse en [15]. Sin embargo, un aspecto importante son los ataques a Neighbor Discovery Protocol (NDP). Este ataque es similar a los ataques de ARP de IPv4 y el atacante puede llenar el caché de vecinos y acabarse la memoria del enrutador resultando en la inhabilidad de éste para reenviar paquetes [12].

5.3.7 Pilares de la seguridad de la información en IPv6

Dado que IPv6 contiene el protocolo, Internet Protocol Security- IPSec, la seguridad se establece de acuerdo a las características esenciales de este mismo, lo que permite que el paquete de IPv6 (de 128 bits) pueda salir a la red de internet completamente cifrado sin que tengan que intervenir procesos como la traslación de direcciones (NAT) o esquemas de encapsulamiento (Túneles) que reducen considerablemente el desempeño de las direcciones IP [12]. Debido al gran número de direcciones IPv6 para atender el despliegue de nuevos servicios en la comunidad de Internet, es necesario aplicar lineamientos de seguridad tal y como se

realizan actualmente con IPv4 para el entorno tanto de las redes de comunicaciones como de las aplicaciones en las entidades, porque a pesar de que las entidades comienzan a generar tráfico en IPv6, los constantes ataques de los hacker no se hacen esperar [12]. Por lo tanto, es importante desarrollar lineamientos de seguridad bajo la premisa de los pilares básicos de la seguridad de la información como son la Confidencialidad, la Integridad y la Disponibilidad [16].

5.3.7.1 Confidencialidad

La Confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización. Desde el punto de vista de la estructura del protocolo mismo, el paquete IPSec, maneja dos protocolos de seguridad; de un lado uno relacionado con la Cabecera de Autenticación (AH), encargado de proporcionar autenticidad de los datos, integridad y no repudio y por el otro lado el Encapsulado de Carga Útil (ESP), consistente en proporcionar confidencialidad mediante el cifrado de los datos. Este último, el encapsulating Security Payload (ESP) de la cabecera de IPv6 puede utilizar un algoritmo de cifrado encargado de proporcionar integridad, autenticidad, y confidencialidad de la información [12]. Es preciso tener en cuenta que el uso de la Cabecera de Autenticación del paquete datagrama IPv6, genera aumento de latencia de las comunicaciones, esto debido principalmente al cálculo de la información de autenticación por parte del nodo origen y el cálculo de comparación de la información de autenticación por el nodo destino de cada datagrama IPv6 [12]. Tanto el AH, como el ESP, son instrumentos para el acceso de datos con base en la distribución de flujo de tráfico de paquetes y claves cifradas [12]. Estos métodos permiten trabajar en dos modalidades, a tratar en los siguientes puntos [17].

5.3.7.2 Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. A groso modo, la integridad consiste en mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados [12]. Desde el punto de vista del paquete IPv6, la integridad apunta a relacionar la Cabecera de Autenticación (AH) y el Encapsulado de Seguridad de Carga Útil (ESP), con la integridad de los datos asegurando los datos al momento de generar tránsito de paquetes a través de la red IPv6 [12]. Complementariamente a lo anterior, dentro de la estructura del paquete IPv6, el AH permite proporcionar integridad y autenticidad de los datos por medio de una función de autenticidad cifrada sobre los datagramas de IPv6 que se hace por medio de una clave de autenticación [12].

El esquema de funcionamiento para proveer seguridad se establece cuando el nodo origen procesa la información de autenticidad antes de enviar el paquete cifrado de IPV6 por la red y el nodo receptor chequea la información autenticada cuando la recibe; el Campo Límite de Saltos (Hop Limit), contenido en la estructura del paquete IPv6, puede ser omitido en el cálculo de la autenticidad en razón a que este evalúa constantemente los número de saltos de ruteo producidos en la red y no el tiempo de vida de los mismos sin afectar la seguridad de los datos [12]. Los algoritmos de autenticación utilizados en el campo de Cabecera de Autenticación podrían producir no repudio (es decir que tanto las claves del nodo origen como del nodo destino se utilizan en el cálculo de la autenticidad), esta característica no es nativa de todos los algoritmos de autenticación que pueden utilizarse en el campo de Cabecera de Autenticación de IPv6 [18].

5.3.7.3 Disponibilidad

La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran. La disponibilidad en soluciones bajo IPv6 se puede visualizar en la garantía de ofrecer a los usuarios de las entidades una alta disponibilidad en servicios bajo IPv6, sin embargo se prevé que los servicios de las redes tanto a corto como a mediano plazo se establezcan con la coexistencia de protocolos IPv4 y IPv6, lo cual implica que las organizaciones tendrán que tener configurados los sistemas de enrutamiento para el soporte simultáneo de ambos protocolos a fin de mantener la continuidad del negocio y proteger las inversiones [19].

5.3.7.4 Privacidad

Con la desaparición de la traslación de direcciones de red, o NAT (Network Address Traslation); muy comunes en IPv4, surge el problema de mantener la privacidad en los accesos de IPv6, para ello es necesario plantear niveles y servicios de privacidad de IPv4 en IPv6 [12]. En IPv6 se pueden combinar dos esquemas de seguridad de IP para transmitir un paquete IPv6, por un lado, la autenticación y por el otro la privacidad [20].

5.3.7.5 Cifrado antes de Autenticación

Este procedimiento sucede cuando el paquete IP es transmitido y autenticado en su totalidad, previo a un esquema de cifrado en los extremos [14]. Primero se aplica la Carga de Seguridad Encapsulada - ESP a los datos que se van a proteger y después se incorpora el texto original al comienzo de la cabecera de autentificación IP [18].

5.3.7.6 Autenticación antes del Cifrado

La Cabecera de Autentificación se encapsula dentro del paquete IP interno. Este paquete interno es identificado y protegido por el esquema de privacidad. Esta técnica sólo es adecuada para el Encapsulado de Carga Útil - ESP en modalidad de túnel [12]. El método puede preferirse en virtud de que la cabecera de autenticación AH se protege por la Carga de seguridad encapsulada ESP y de esta forma es muy complejo que los mensajes del paquete sean interceptados y modifiquen el AH sin ser detectado [19].

5.3.7.7 Servicios Impactados en Seguridad

Según [14], los siguientes son los servicios que impactan en seguridad de las Entidades al momento de iniciar el plan de implementación del nuevo protocolo IPv6:

- Directorio Activo
- DNS (Domain Name System)
- DHCP (Dynamic Host Configuration Protocol)
- Servicios Proxy
- Dominio de red
- Correo electrónico
- Mensajería Instantánea
- Telefonía IP
- Videoconferencia
- Servicio Web y Acceso a Internet
- Aplicaciones y bases de datos
- Equipos de comunicaciones fijos y móviles
- Equipos de seguridad (Firewalls, Servidores AAA (Authentication, Authorization and Accounting), NAC (Network Access Control)
- Canal de Comunicación de internet.

5.4 Cableado Estructurado.

Es una infraestructura de cableado, la cual cumple una serie de estándares y que está destinada a transportar las señales de un emisor hasta el correspondiente receptor. Su principal objetivo es proveer un sistema total de transporte de información a través de un mismo tipo de cable (medio común). La instalación de dicha infraestructura se realiza de una manera ordenada y planeada lo cual ayuda a que la señal no se degrade en la transmisión y asimismo garantiza el eficiente desempeño de la red [21].

En un sistema de cableado estructurado, se utiliza la topología de red tipo estrella, es decir que cada estación de trabajo se conecta a un punto central con un cable independiente al de otra estación. Esta concentración hará que se disponga de un conmutador o switch que sirva como bus activo y repetidor [21]. El cableado estructurado se utiliza principalmente para trasmitir voz, datos, video, imágenes, entre otros [22].

Es de fundamental importancia entender que para que un edificio quede exitosamente diseñado, construido y equipado para soportar los requerimientos actuales y futuros de los sistemas de telecomunicaciones, es necesario que el diseño de las telecomunicaciones se incorpore durante la fase preliminar de diseño arquitectónico [21].

5.4.1 Normas para el cableado estructurado

El Instituto Americano Nacional de Estándares, la Asociación de Industrias de Telecomunicaciones y la Asociación de Industrias Electrónicas (ANSI/TIA/EIA) publican conjuntamente estándares para la manufactura, instalación y rendimiento de equipo y sistemas de telecomunicaciones y electrónico. Cinco de estos estándares de ANSI/TIA/EIA definen cableado de telecomunicaciones en edificios. Cada estándar cubre una parte específica del cableado del edificio. Los estándares establecen el cable, hardware, equipo, diseño y prácticas de instalación requeridas. Cada estándar ANSI/TIA/EIA menciona estándares relacionados y otros materiales de referencia [23].

La mayoría de los estándares incluyen secciones que definen términos importantes, acrónimos y símbolos. 36 Los estándares principales de ANSI/TIA/EIA que gobiernan el cableado de telecomunicaciones en edificios son:

5.4.1.1 Estándar 568

Commercial Building Telecommunications Cabling Standard (Estándar de Cableado para Telecomunicaciones en Edificios Comerciales).

El estándar regula los requerimientos que debe cumplir para la implementación del sistema de cableado garantice seguridad y flexibilidad en el sistema.

[23] indica que se estima que la “vida productiva” de un sistema de cableado para edificios comerciales debe ser de 15 a 25 años. En este período, las tecnologías de telecomunicaciones seguramente cambien varias veces. Es por esto que el diseño del cableado debe prever grandes anchos de banda, y ser adecuado tanto a las tecnologías actuales como a las futuras [23].

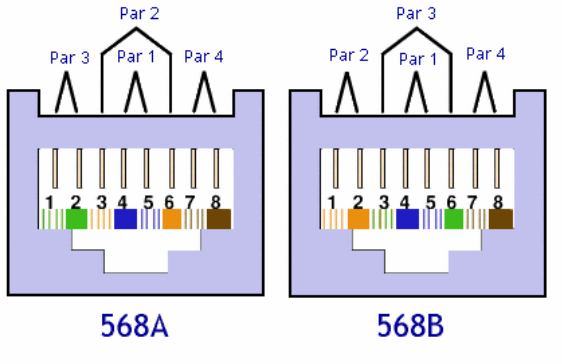


Figura 5.2 Orden de color Estándar 568 [23]

5.4.1.2 Estándar 569

Commercial Building Standard for Telecommunications Pathways and Spaces (Estándar de Rutas y Espacios de Telecomunicaciones para Edificios Comerciales).

El estándar trata el tema de diseño de la instalación y la infraestructura para la adecuación de rutas y espacio de canalización.

[24] indica que es de fundamental importancia entender que para que un edificio quede exitosamente diseñado, construido y equipado para soportar los requerimientos actuales y futuros de los sistemas de telecomunicaciones, es necesario que el diseño de las telecomunicaciones se incorpore durante la fase preliminar de diseño arquitectónico.

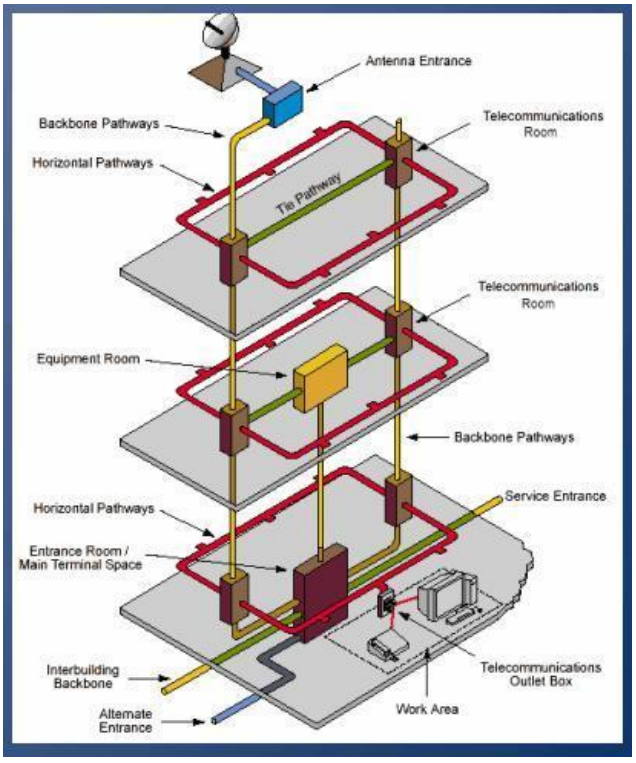


Figura 5.3 Diseño de Estándar 569 [23]

5.4.1.3 Estándar 606

Administration Standard for Commercial Telecommunications Infrastructure (Estándar de Administración para la Infraestructura de Telecomunicaciones Comerciales).

El estándar provee información acerca del esquema para la administración, etiquetación y documentación uniforme de los sistemas de cableado, independiente de las aplicaciones que estas manejen.

[23] indica que la norma EIA/TIA-606 especifica que cada terminación de hardware debe ser etiquetada de modo que lo identifique de forma exclusiva, esto incluye los dos extremos de cualquier cable. En redes pequeñas podríamos poner los nombres de las personas que usan esos equipos, pero si cambian, deberíamos cambiar el etiquetado. Por ello se recomienda los códigos nemotécnicos neutros o invariables [25]. Estos códigos deben identificar la sala o habitación donde se encuentran la roseta y un identificador de conector [25].

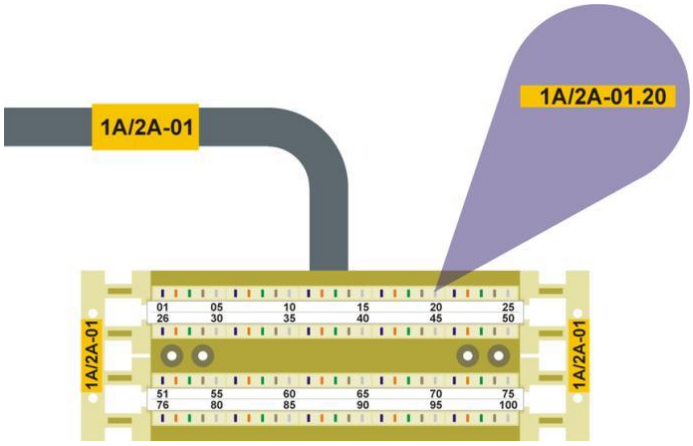


Figura 5.4 Esquema de Estándar 606 [23]

5.4.1.4 Estándar 607

Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications (Requerimientos para Telecomunicaciones de Puesta a Tierra y Puenteado de Edificios Comerciales).

El estándar establece requerimiento que se debe tener en consideración al momento de implementar un sistema que permita brindar protección de los equipos de telecomunicación en el edificio.

[24] indica que el propósito de este documento es brindar criterios de diseño e instalación de las tierras y el sistema de aterramiento para edificios comerciales, con o sin conocimiento previo acerca de los sistemas de telecomunicaciones que serán instalados.

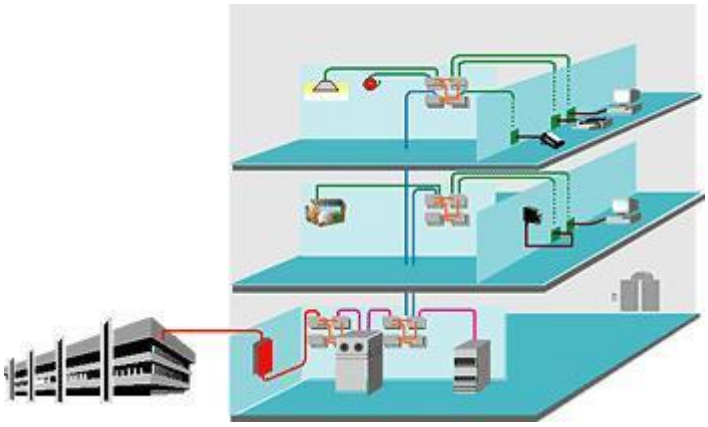


Figura 5.5 Requerimientos de Estándar 607 [23]

5.5 IPv6 vs IPv4

A continuación, se mostrará una tabla donde se presentará algunas de las diferencias entre IPv6 e IPv4.

Tabla 5.6 Diferencias entre IPv4 e IPv6

	IPv4	IPv6
Formato de paquetes		
Longitud de cabecera	20 bytes (variable)	40 bytes (fijo)
Campos para QoS	DSCP	TC+FL
Direccionamiento		
Longitud de dirección	32 bits	128bits
Espacio de direcciones	4,294,967,296	$3.4x20^{38}$!
Representación	Decimal	Hexadecimal
Mecanismos		
Comunicaciones	Unicast	Unicast
	Multicast	Multicast
	Anycast	Anycast
	Broadcast	
Resolución dir. L2	ARP	ND
Fragmentación	Host y routers	Sólo host

5.6 IPv6 vs IPv4 (Espacio de IPs)

- En IPv4 (2^{32}) hay 4.294.967.296 direcciones disponible
- En IPv6 (2^{128}) hay 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones disponibles (serían 340 sextillones).

5.6.1 Formato de un paquete IPv6

Campos de IPv4 que se mantienen en IPv6:

- Version (mismo nombre)
- Traffic Class (llamado ToS / DSCP)
- Payload lenght (llamado Total Lenght)
- Next Header (llamado Protocol)
- Hop Limit (llamado Time to Live)
- Src and Dst Address

Campo nuevo en IPv6:

- Flow Label (20 bits)

5.7 Topología en estrella.

La red se une en un único punto; un concentrador de cableado o HUB que a través de él los bloques de información son dirigidos hacia las estaciones. Su ventaja es que el concentrador monitorea el tráfico y evita las colisiones y una conexión interrumpida no afecta al resto de la red. La desventaja es que los mensajes son enviados a todas las estaciones, aunque vayan dirigidas una a una [26].

Figura 5.6 Topología en estrella [27]**.**

5.8 Enrutamiento estático.

Se considera una ruta estática aquella creada manualmente por el administrador de red. Al no tener vínculos con los protocolos, las rutas estáticas no reciben actualizaciones, lo cual indica que el administrador debe reconfigurar estas rutas nuevamente e incluir los cambios en la topología [28].

Ventajas

- Mayor seguridad en las redes informáticas [26].
- Al no utilizar protocolos de enrutamiento, el consumo de recursos es menor. No se consume mucho ancho de banda [26].
- Practicidad en la administración por parte del administrador de la red, siempre y cuando la red sea pequeña [26].

Desventajas

- Al tener cambios en la topología no se presenta una actualización automática [26].
- Los mantenimientos son complejos [26].

5.9 Servidor DHCP

DHCP se define como un protocolo de configuración dinámica de host diseñado para simplificar la administración de la configuración IP de los equipos de una red, por ello el servidor DHCP recibe peticiones de clientes solicitando una configuración de red IP así el servidor responderá proporcionando una autoconfiguración al cliente (Dirección IP y mascará de subred, aunque algunas veces adicionalmente puerta de enlace, servidor DNS, etc.)

Importancia: permite proporcionar una configuración de red segura, evitando conflictos con direcciones repetidas, usando un modelo cliente-servidor, donde el servidor DHCP mantiene una administración centralizada de las direcciones IP de la red, donde el cliente solicita al servidor una IP para formar parte de la red

Funcionamiento: El servidor DHCP solo asigna direcciones dentro de un rango fijado, asimismo se debe tener en cuenta que si se encuentra algún cliente con una IP estática que se encuentra dentro de ese rango podría ser asignada también a otro cliente lo que generaría conflictos con dicha IP, sin embargo, al realizar la solicitud de IP por parte del cliente se continuara comprobando hasta que se obtenga una IP que aún no haya sido asignada en la red [29].

5.10 IPsec

IPsec es un protocolo de seguridad muy importante para proteger toda la información que circula a través de una red, trabaja en la capa de red del modelo de referencia OSI.

Cabe destacar que IPsec es protocolo que brinda seguridad a la capa IP, una de las funcionalidades de IPsec es la encriptación lo cual garantiza una comunicación segura entre

diferentes puntos a través de Internet, IPsec se adapta perfectamente a las necesidades de VPN [24].

IPsec es un protocolo robusto para la seguridad de los datos, cumple con los cuatro pilares básicos de seguridad de la información como autenticación, confidencialidad, integridad y no repudio, IPsec es un estándar de seguridad para las redes de datos, en la actualidad IPsec es un componente básico en seguridad [30].

5.11 Calidad de Servicio o QoS (Quality of Service)

El concepto de calidad de servicio (QoS) en telecomunicaciones puede tener, al menos, dos interpretaciones habituales. En primer lugar, se refiere a la capacidad de determinadas redes y servicios para admitir que se fije de antemano las condiciones en que se desarrollarán las comunicaciones (dedicación de recursos, capacidades de transmisión, etc.).

En segundo lugar, se habla calidad de servicio como una serie de cualidades medibles de las redes y servicios de telecomunicaciones, como el tiempo que se tarda en realizar una llamada telefónica (desde que el usuario marca hasta que suena el teléfono en el otro extremo) [31].

5.11.1 Aplicaciones

La motivación para aplicar Calidad de Servicio en redes IP se resume en las siguientes necesidades [32]:

- Priorizar ciertas aplicaciones en la red que requieren de un alto nivel de servicio VOIP [32].
- Maximizar el uso de la infraestructura de red, manteniendo un margen de flexibilidad, seguridad y crecimiento para servicios emergentes [32].
- Mejorar las prestaciones para servicios en tiempo real [32].
- Responder a los cambios en el perfil de tráfico establecido [32].
- Proporcionar mecanismos para priorizar tráfico [32].

5.11.2 Factores que la afectan

Son diversas las causas que pueden atentar contra el correcto funcionamiento de la red o que el usuario tenga una percepción negativa del servicio recibido. Estos factores están dados en su mayoría a que la voz debe viajar en un entorno diseñado para paquetes de datos, sufriendo cambios de paquetización, fragmentación, intercalado, codificación o descodificación a través de la red [32]. Algunos de estos parámetros se describen a continuación [31].

6 MATERIALES Y MÉTODOS

Para el diseño de la transición del protocolo ipv4 a ipv6, existen varias técnicas y métodos los cuales otorgan, en su mayor parte, una mejor comprensión del tema y facilitan su desarrollo.

En este caso, este diseño será desarrollado para la mejora en velocidad de datos y estándares de seguridad de la empresa "GrupoJativa", para lo cual, se utilizará las técnicas que den mayor facilidad en la investigación y que agilicen el proceso por el cual se diseñará la transición.

6.1 TIPO DE INVESTIGACIÓN

6.1.1 Investigación Descriptiva

A través de la investigación descriptiva se podrá conocer cuáles son las actividades y procesos que realiza la empresa, de esta manera se logrará determinar cuál es el problema a solventar con el desarrollo de la aplicación, de la misma manera permite construir una hipótesis en base a los datos recolectados.

6.1.2 Investigación de Campo

Con la investigación de campo se podrá recopilar la información del tipo de datos y la rapidez con la que se transmiten estos dentro de la empresa, las necesidades que esta necesita y las preferencias de los clientes según los servicios que ofrece la empresa. Para la recolección de los datos mencionados se utilizarán dos herramientas en específico: la entrevista al propietario de la empresa y las encuestas a los clientes de la misma.

6.2 MÉTODOS DE RECOLECCIÓN DE INFORMACIÓN

6.2.1 Encuesta

Mediante la encuesta se podrá analizar cuáles son las preferencias de los usuarios al momento de hacer uso de la red de la empresa, y las opiniones de los empleados estratégicos sobre el uso de la misma. De los datos obtenidos de dicha encuesta se logrará tener un desarrollo del proyecto más acorde a las necesidades del propietario y de los usuarios que utilizaran la red establecida.

Esta encuesta será aplicada a una muestra obtenida del total de la población que interactúa con la empresa, de esta manera, se podrá analizar el nivel de aceptación que tiene la propuesta tecnología en la población afectada.

6.3 DETERMINACIÓN DE LA POBLACIÓN Y MUESTRA

6.3.1 Población

La población es el total que tiene aproximadamente la empresa, se obtendrá de las charlas realizadas con el propietario de la empresa.

Actualmente la población que se tiene es de 15 persona, se procederá a realizar las respectivas técnicas de recolección de información.

7 RESULTADOS

7.1 RESULTADOS DE LA ENTREVISTA Y ENCUESTAS

7.1.1 Resultados de las Encuestas

El análisis se realizó en base a las encuestas aplicadas al gerente y empleados de la empresa "GrupoJativa". El formato de la encuesta aplicada la podrá encontrar en la sección de anexos (ANEXO B).

7.2 HERRAMIENTAS UTILIZADAS

7.2.1 Herramientas Principales de Uso

7.2.1.1 Cable UTP categoría 6

Es un tipo de cable de par trenzado cuya categoría es una de la clasificación de cableado UTP descritos en el estándar EIA/TIA 568B. Puede transmitir datos a velocidades de hasta 1000 Mbps o 1 Gbps a frecuencias de hasta 200 MHz, marcando un hito en el mundo de telecomunicación al migrar de 100 Mbps (categoría 5e) a 1000 Mbps [33].

7.2.1.2 Swicth 8 puertos (TP Link)

Es un conmutador de escritorio de ethernet rápido de 8 puertos y 100Mbps que proporciona ocho puertos RJ45 de auto-negociación 10/100M que admiten MDI / MDIX automático. Tiene dos modos comunes y enlace ascendente. Dispone de arquitectura de switching sin bloqueos de reenvío y filtrado de paquetes a la máxima velocidad del cable para obtener un rendimiento óptimo. Soporta 2 K de jumbo frame, lo que mejora significativamente el rendimiento de las transferencias de archivos de gran tamaño.

7.2.1.3 Router Mercusys

Ofrece mayor velocidad inalámbrica N y cobertura a 300 Mbps para compartir archivos, jugar en línea y transmitir videos de forma inalámbrica. La encriptación avanzada protege su red inalámbrica, las herramientas de control de acceso ayudan a bloquear sitios Web indeseados y

usuarios desconocidos, así como hacer control de ancho de banda QoS por IP o MAC Address. La tecnología MIMO avanzada (múltiple entrada, múltiple salida) le ofrece amplia cobertura y eliminación de puntos muertos. La especificación WPS (Wi-Fi Protected Setup) le permite integrar otros adaptadores inalámbricos compatibles con WPS con sólo tocar un botón. La tecnología de calidad de servicio (QoS) WMM prioriza los videojuegos, las llamadas por Internet y la transmisión de video.

7.2.1.4 Router mikrotik hex lite 5 puertos

También conocido como hEX lite es un pequeño router ethernet en una agradable caja de plástico. Su precio es casi tan bajo como el de una licencia RouterOS de Mikrotik. No sólo es accesible, pequeño, muy bonito y fácil de usar, sino que es probablemente el Router Ethernet MPLS más accesible del mercado, sin más compromisos entre precios y características.

7.2.1.5 Conectores rj45 categoria 6

El conector RJ45 Cat6 Alter es una interfaz física comúnmente usada para conectar redes de cableado estructurado. Es utilizado normalmente con estándares como TIA/EIA-568-B que define la disposición de los pines. Sirve para armar cables Ethernet y realizar instalaciones o renovaciones de redes de computadoras o conectar cables de red a rosetas, ruteadores, módems, Smart TV y aparatos de teléfono. El conector RJ45 Cat6 Alter es ideal para conectar cable UTP CAT6 ya que este cable tiene alta frecuencia les permite a las redes con cables Cat 6 operar a 1000 Mbps (megabits por segundo) o 1 gigabit de velocidad.

7.2.1.6 Canaletas

Se utilizan para conducir los cables de comunicación y poder sobrepuestas sobre una pared al interior o exterior de cualquier edificación. Son fabricadas con los más altos estándares, ofreciendo excelentes acabados y durabilidad a lo largo del tiempo. El proceso de fabricación de este producto incluye un equipo humano calificado, máquinas de control numérico, y un tratamiento de lámina que utiliza Fosfato de Zinc y Garantiza más de 1000 Horas de Cámara Salina.

7.3 Configuración de la red IPv6

A continuación, se mostrará de manera gráfica la configuración realizada para la red de protocolo IPv6.

7.3.1 Verificación de dispositivos.

En primer lugar, se verificó los dispositivos que tenía la red ya que para poder realizar la migración tienen que ser dispositivos avanzados para que no tengamos problema, por lo cual se pudo apreciar que si poseían equipos con los requisitos que se necesitaban, pero no tenían un mantenimiento preventivo adecuado, por lo cual se decidió realizar su respectivo manteamiento como se puede apreciar en la Figura 7.1.

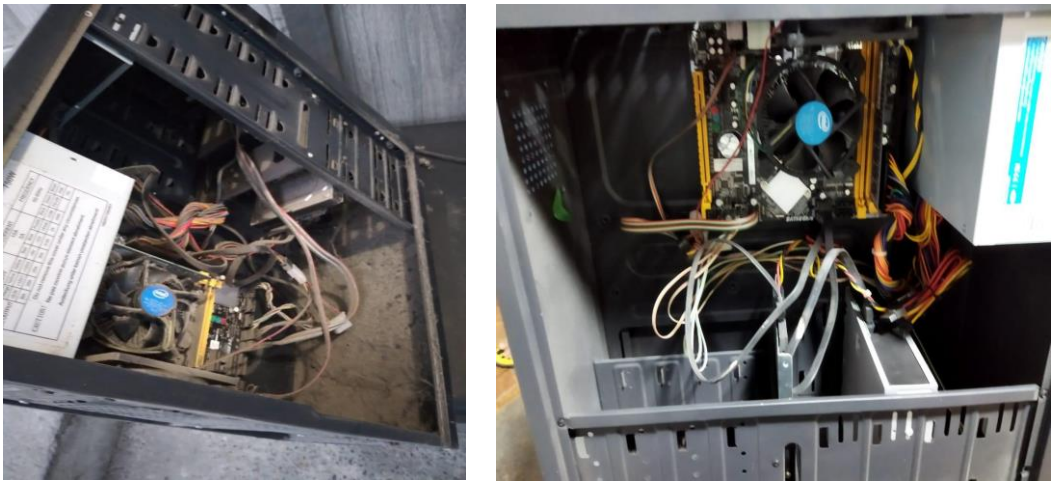


Figura 7.1 Antes y después del mantenimiento del equipo.

En la estructura de red de la empresa se pudo apreciar que solo estaban equipos conectados entre sí sin llevar alguna norma o protocolo del cableado estructurado, por lo cual se procedió a verificar el tipo de cable que tenía la red, el cual era un cable categoría 5e, dicho cable estaba sin canaletas ni amarras plásticas con el switch colgando de los cables y en el mal estado como se puede apreciar en la Figura 7.2.

Figura 7.2 Estado defectuoso de los cables y estado del switch.

Para suplir estas falencias se procedió a colocar el cable categoría 6 de cobre certificado conjuntamente con canaletas sin división y amarras plásticas, también se colocó una caja para el switch para que esté protegido de los roedores y daños exteriores, permitiendo que el tiempo de vida del cableado perdure más tiempo y no tenga interferencia o pérdida de conexión en el envió de datos como se puede apreciar en la Figura 7.3.

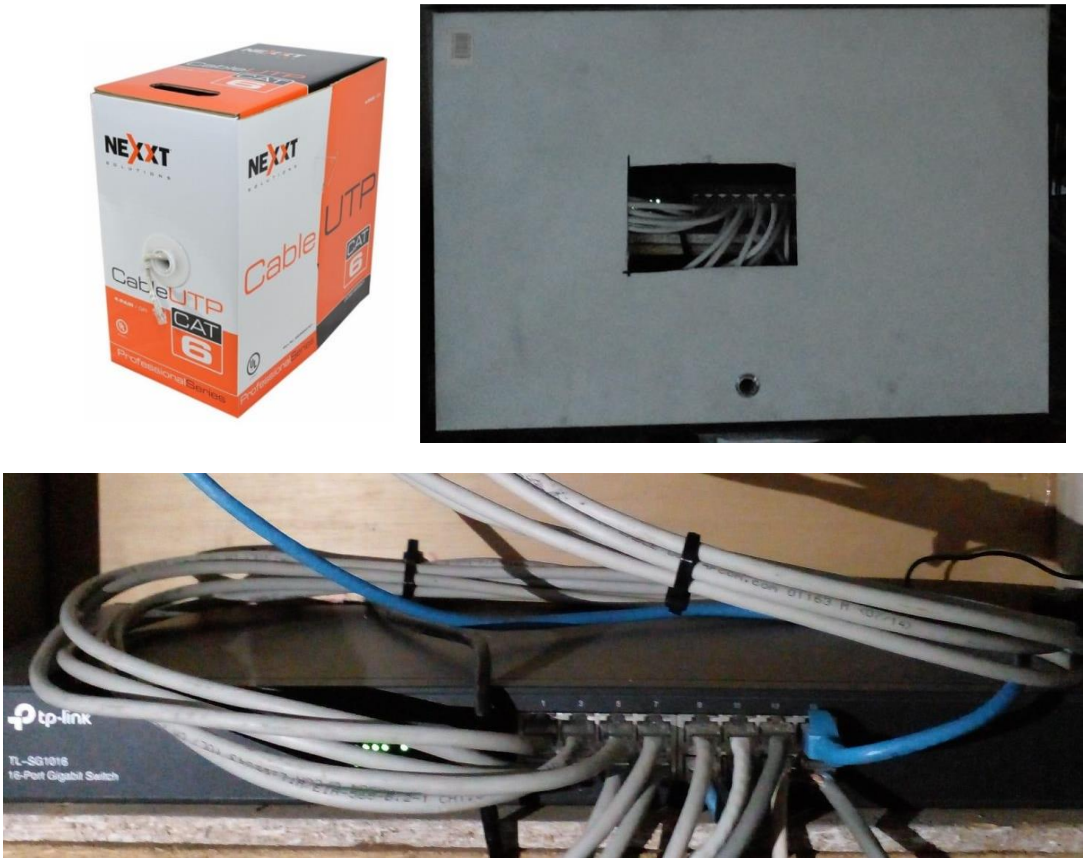


Figura 7.3 Cable categoría 6, amarras de plástico y caja para la protección del switch.

Se implementó el estándar 568 para poder garantizar la seguridad y flexibilidad en el sistema del cableado para edificios comerciales para que estos perduren durante mucho tiempo y no se dañen, como mínimo puede perdurar entre 15 a 25 años.

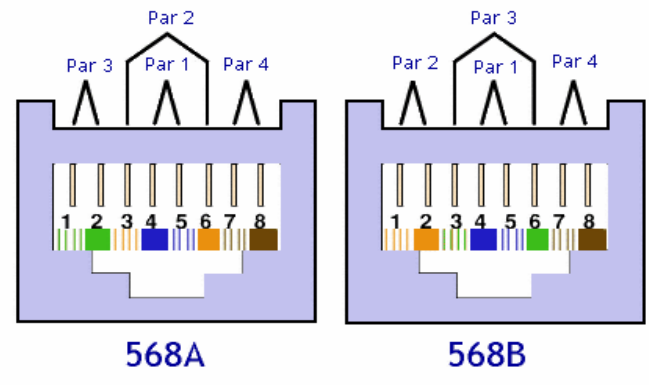


Figura 7.4 Estándar 568.

Otros de los estándares que se implemento es el 569 que nos permite identificar cualquier parte de la infraestructura para que la empresa soporte el diseñado, construido y equipado de los requerimientos actuales y futuros de red en un maquetado de packet tracer.

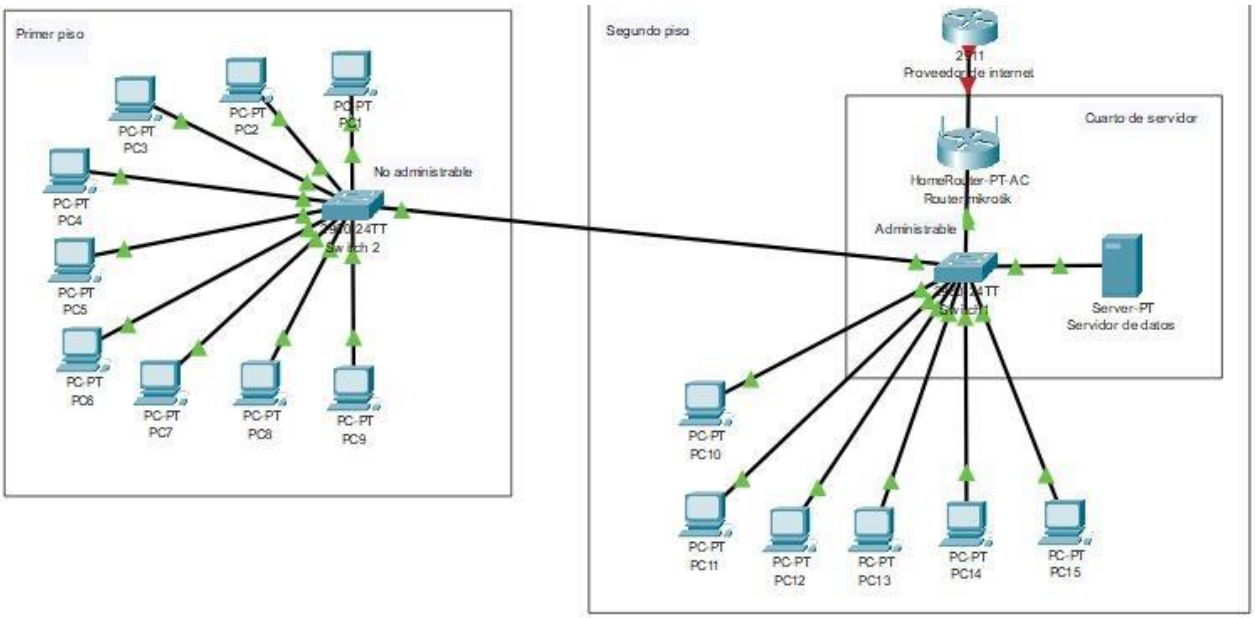


Figura 7.5 Estándar 569.

Uno de los tantos estándares que se utilizó es el 606 que permite identificar cada dispositivo de la infraestructura de red por medio de un etiquetado por lo cual se colocó el nombre del equipo ya que es una empresa pequeña en crecimiento.

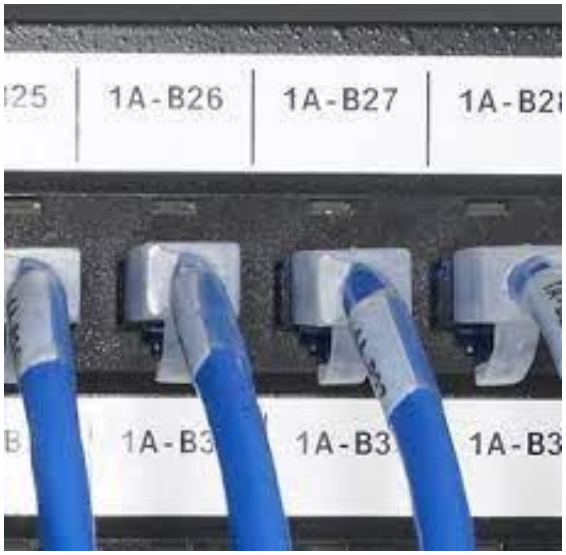


Figura 7.6 Estándar 606

Se utilizó el estándar 607 para colocar tierra en el local para cuidar los dispositivos de una tormenta eléctrica ya que estos pueden conducir alta energía por medio de los cables UTP y puede dañar los dispositivos con algún corto como se puede apreciar en la Figura 7.7.

Figura 7.7 Estándar 607.

Se procedió a colocar el servidor con su malla para que no entren los roedores en el servidor, en la oficina del gerente del segundo piso con su rack y switch administrable para que este a una temperatura óptima que está entre los 18°C y los 23°C, ya que el aire siempre pasa encendido a la temperatura óptima y hay pocas personas en la oficina para que este no varíe su temperatura por la acumulación de persona en la sala u oficina.

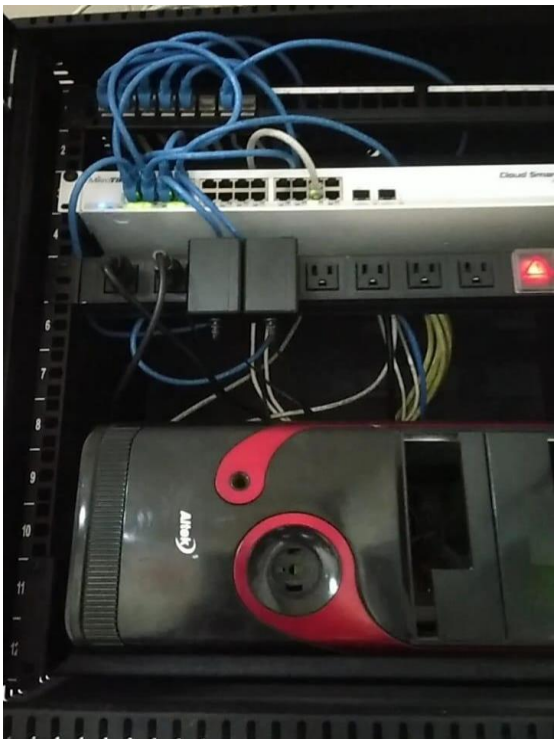


Figura 7.8 Rack y switch administrable.

Después que se procedió a realizar todo el cableado estructurado, se comenzó a realizar la migración de ipv4 a ipv6 por medio de un router Mikrotik que nos permite administrar toda la red de la empresa GrupoJativa con el dispositivo que se puede observar en la Figura 7.9.

Figura 7.9 Router Mikrotik.

7.3.2 Procedimiento de configuración.

7.3.2.1 Dar acceso a internet.

Para dar acceso a internet cuando se tiene una red IPv6 y una salida de internet en Ipv4 se debe crear un túnel que en mikrotik se llama 6to4 esta es la única manera por la cual los dispositivos que tengan asignada una IP en ipv6 puedan navegar.

- Contratar conexión a un ISP IPv6.
- Configurar un túnel IPv6(con un “Tunnel broker”).
- Hacer tu propia red privada IPv6(con IPs “Unique Local” o “Link Local”).

Para poder realizar la migración se procedió a utilizar un tunnel por medio de la página web tunnelbroker que nos permite a nosotros obtener nuestra dirección ipv4 publica en ipv6 para obtener internet ya que el proveedor de internet Netlife no trabaja con ipv6 por el momento como se puede apreciar en la Figura 7.10.

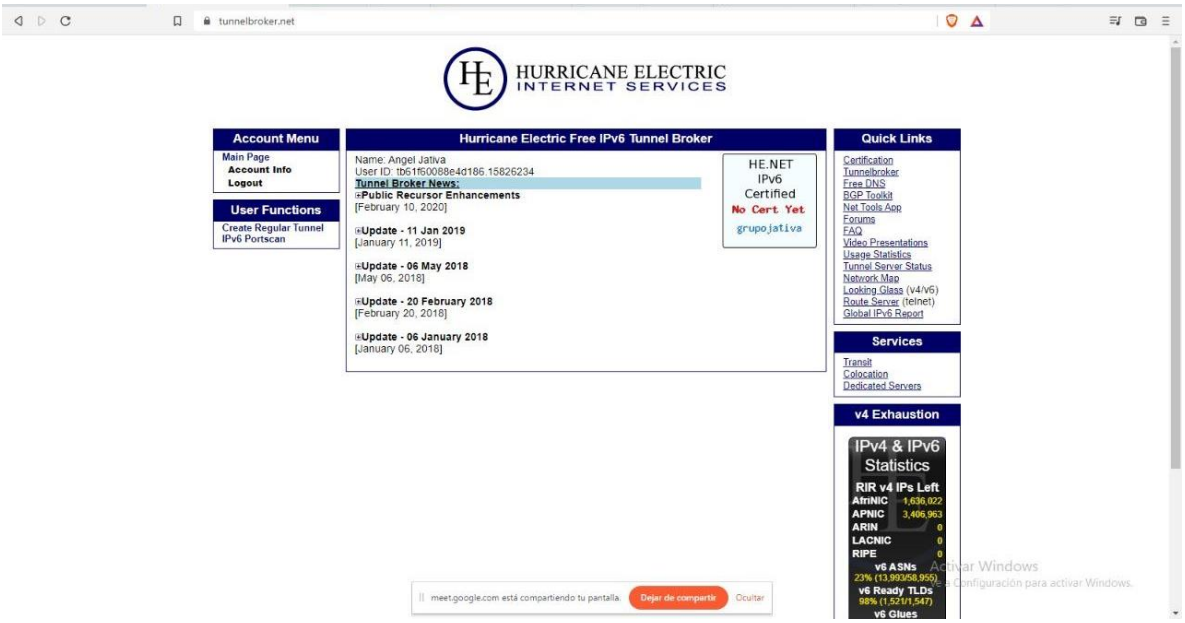


Figura 7.10 Crear una cuenta en https://tunnelbroker.net/

Se procedió a crear el tunnel escogiendo la IP publica en IPv4 para poder obtener una IPv6 y poder tener acceso a internet, lo cual nos permitirá navegar por toda la red del mundo como se puede apreciar en la Figura 7.11.

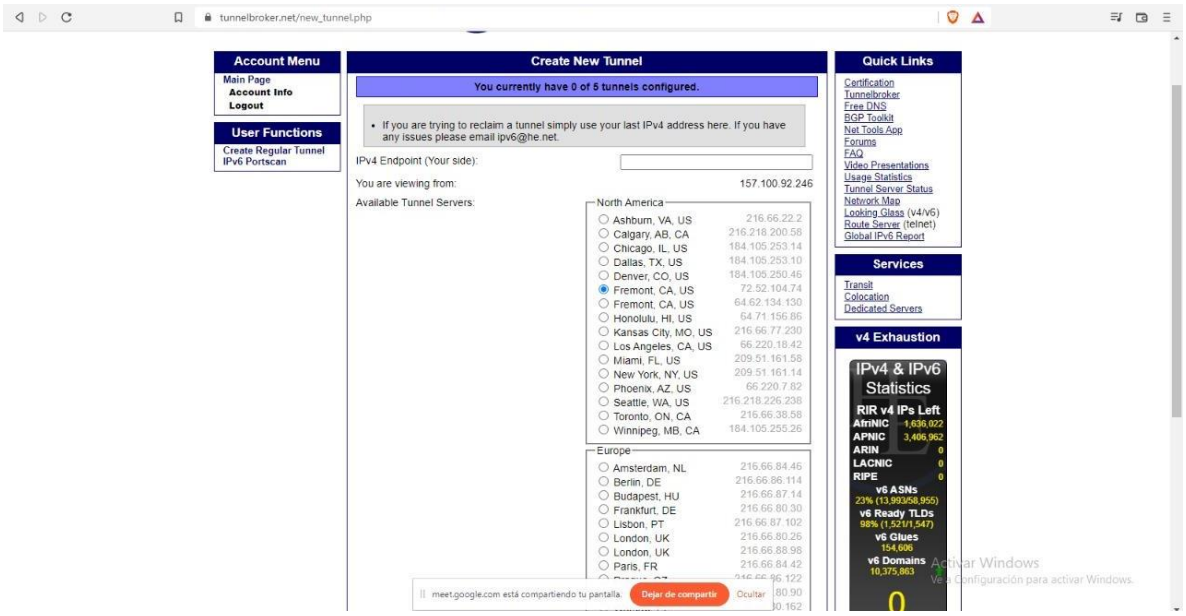


Figura 7.11 Se selecciona create regular tunnel para realizar el túnel.

Figura 7.12 Se escoge la IP pública para poder realizar el túnel en la red.

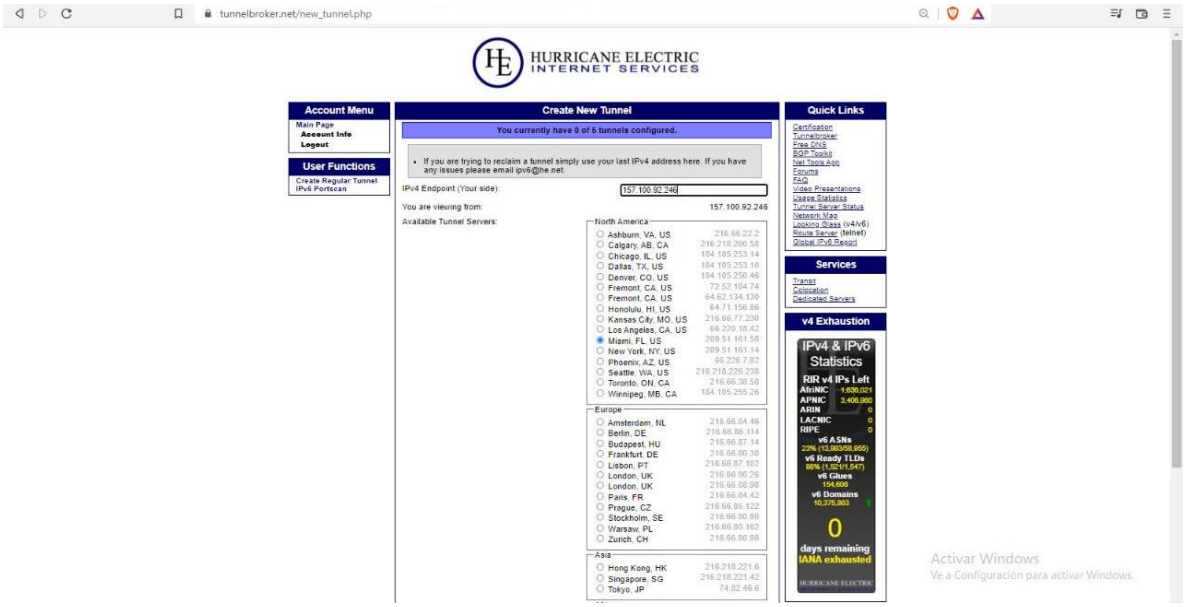


Figura 7.13 Se coloca la IP pública.

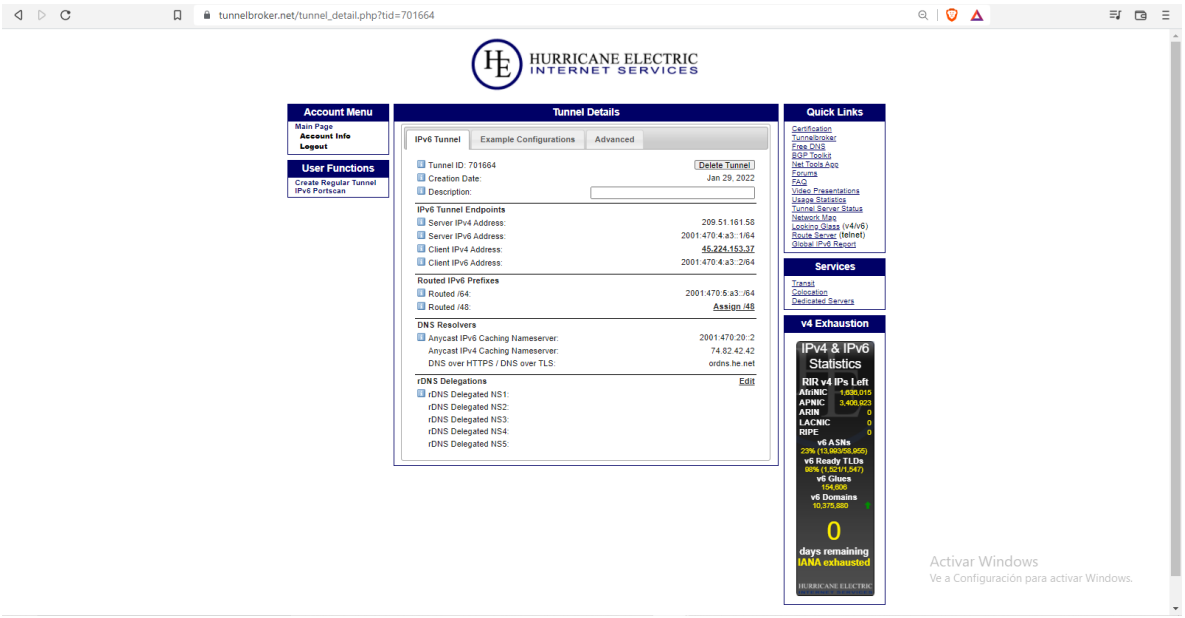


Figura 7.14 Creación de IPv6 para hacer los túneles sobre IPv4.

En esta parte se activan los paquetes de IPv6 dentro del sistema del router Mikrotik, para poder configurar toda la red y poder tener acceso a todos los dispositivos, ya que no vienen por defecto activados como se puede apreciar en la Figura 7.15.

```
 3 X hotspot                6.12
 4   security               6.12
 5   dhcp                   6.12
 6   advanced-tools         6.12
 7 X mpls                   6.12
 8   routeros-mipsbe        6.12
 9   system                 6.12
[admin@rc.psdtec.com] /system package> enable ipv6
[admin@rc.psdtec.com] /system package> print
Flags: X - disabled
 #   NAME                   VERSION                SCHEDULED
 0 X ipv6                   6.12                   scheduled for enable
 1 X routing                6.12
 2   ppp                    6.12
 3 X hotspot                6.12
 4   security               6.12
 5   dhcp                   6.12
 6   advanced-tools         6.12
 7 X mpls                   6.12
 8   routeros-mipsbe        6.12
 9   system                 6.12
[admin@rc.psdtec.com] /system package> /system reboot
Reboot, yes? [y/N]:
```

Figura 7.15 Activación de paquetes IPv6.

Luego de realizar el tunnel en la página nos vamos a la opción de example configuration donde podemos apreciar un código y es el que nos servirá a nosotros para poder configurar nuestro

router Mikrotik en la realización del tunnel, copiamos el siguiente código y lo llevamos al terminal del router para poder aplicarlo como se puede apreciar en las siguientes imágenes.

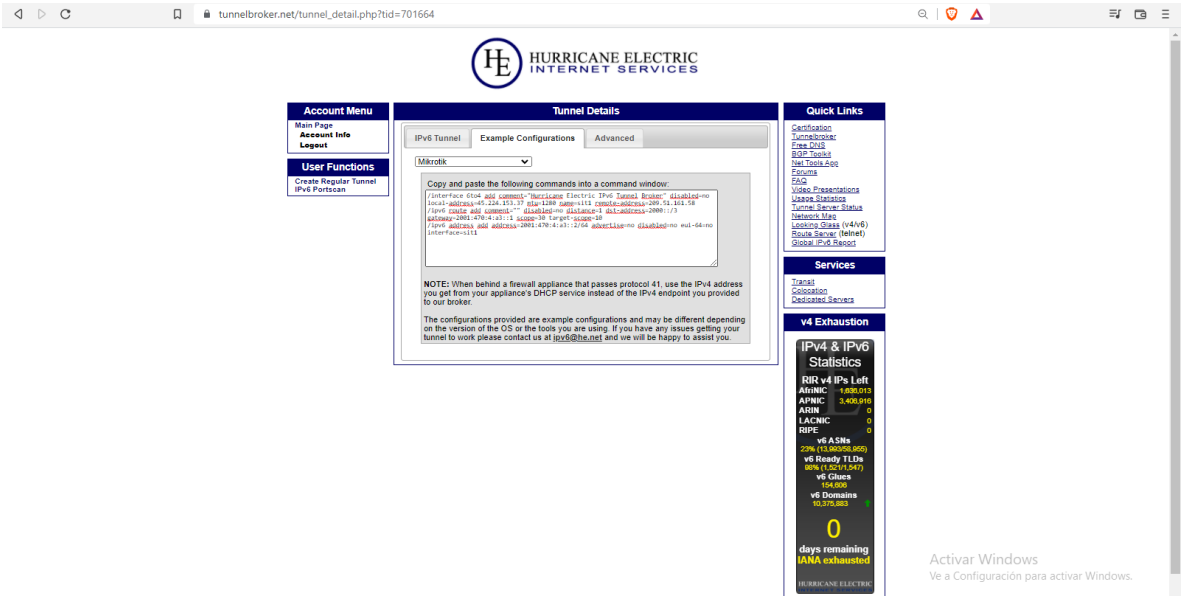


Figura 7.16 Se copia el código para Mikrotic para aplicarlo en el terminal.

```
[admin@CONINTEL] > /interface 6to4 add comment="Hurricane Electric IPv6 Tunnel Bro
ker" disabled=no local-address=45.224.153.37 mtu=1280 name=sitl remote-address=209
.51.161.58
[admin@CONINTEL] > /ipv6 route add comment="" disabled=no distance=1 dst-address=2
000::/3 gateway=2001:470:4:a3::1 scope=30 target-scope=10
[admin@CONINTEL] > /ipv6 address add address=2001:470:4:a3::2/64 advertise=no disa
bled=no eui-64=no interface=sitl
```

Figura 7.17 Colocamos el código que nos generó la página para la realización del tonel.

Una vez realizado los anteriores pasos podemos apreciar que tenemos el tunnel creado de IPv4 a IPv6 por lo cual ya podemos navegar por toda la red de internet, lo podemos comprobar realizando un ping con el siguiente código que se muestra en las siguientes imágenes.

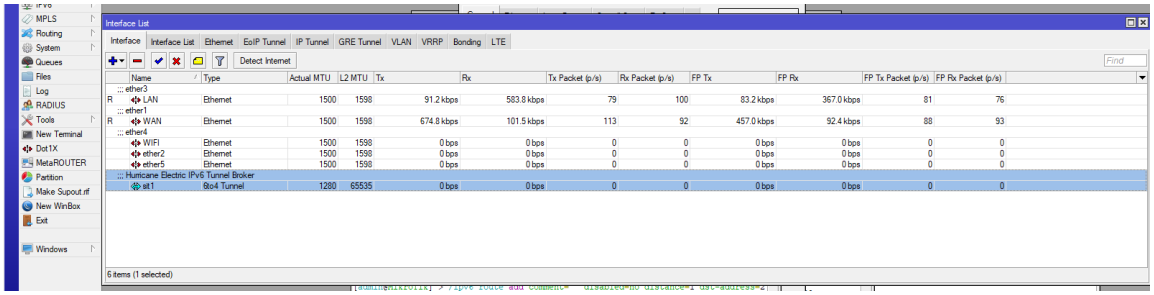


Figura 7.18 Se crea el túnel como se puede apreciar en la imagen.

```
[admin@CONINTEL] > ping [:resolve ipv6.google.com]
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 2800:3f0:4005:40a::200e                    56 120 110ms echo reply
    1 2800:3f0:4005:40a::200e                    56 120 110ms echo reply
    2 2800:3f0:4005:40a::200e                    56 120 109ms echo reply
    3 2800:3f0:4005:40a::200e                    56 120 109ms echo reply
    4 2800:3f0:4005:40a::200e                    56 120 110ms echo reply
    5 2800:3f0:4005:40a::200e                    56 120 109ms echo reply
    6 2800:3f0:4005:40a::200e                    56 120 109ms echo reply
    7 2800:3f0:4005:40a::200e                    56 120 109ms echo reply
    sent=8 received=8 packet-loss=0% min-rtt=109ms avg-rtt=109ms max-rtt=110ms
```

Figura 7.19 Se realiza ping y se puede ver que tenemos acceso a Internet.

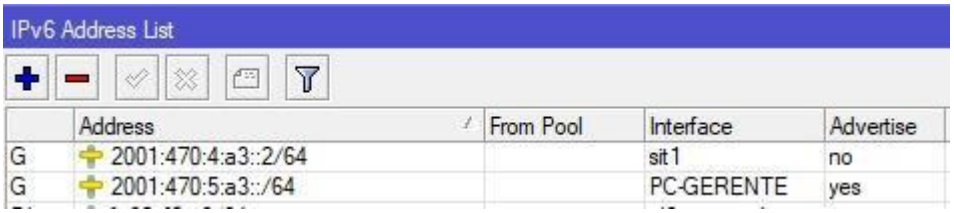


Figura 7.20 Se puede observar que la IPv6 de la PCGERENTE tiene Internet.

En esta parte configuramos las direcciones IPv6 de forma manual ya que son pocos dispositivos y para llevar un mejor control de la red y saber que dispositivo es el que está fallando en caso de ocurra errores futuros en la empresa como se pueden apreciar en la Figura 7.21.

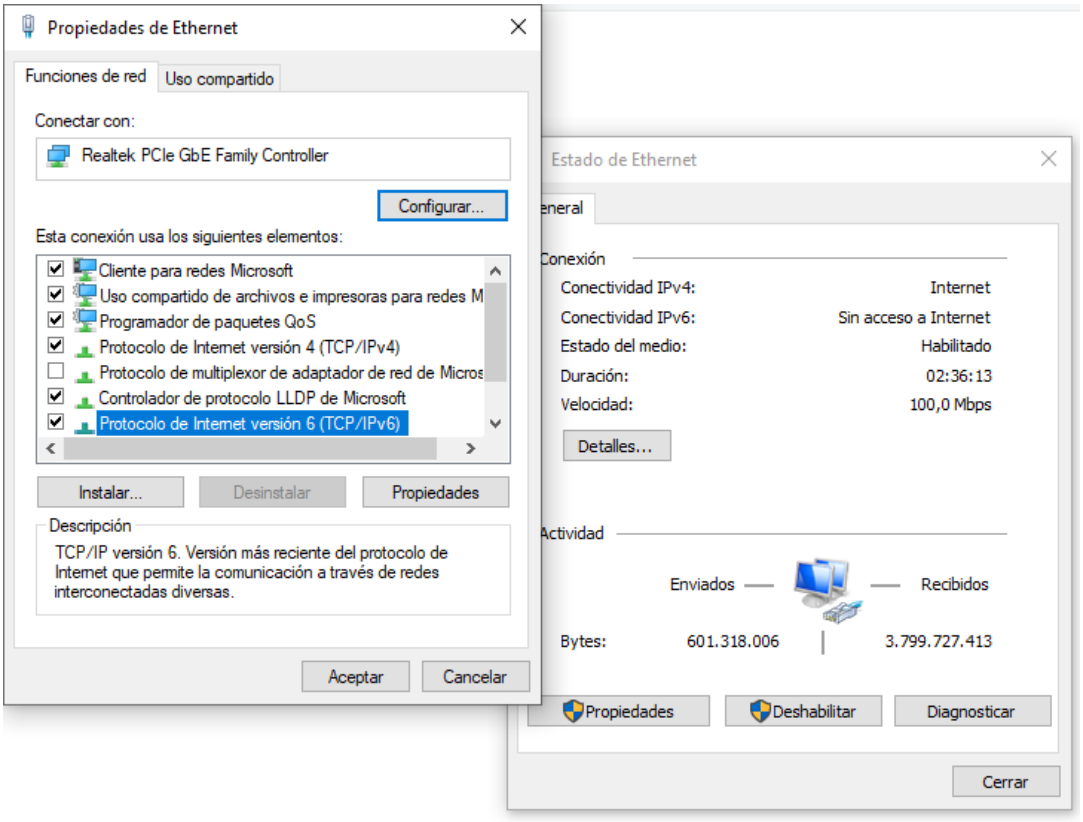


Figura 7.21 Ventana de propiedades de Ethernet, donde se selecciona el protocolo IPv6.

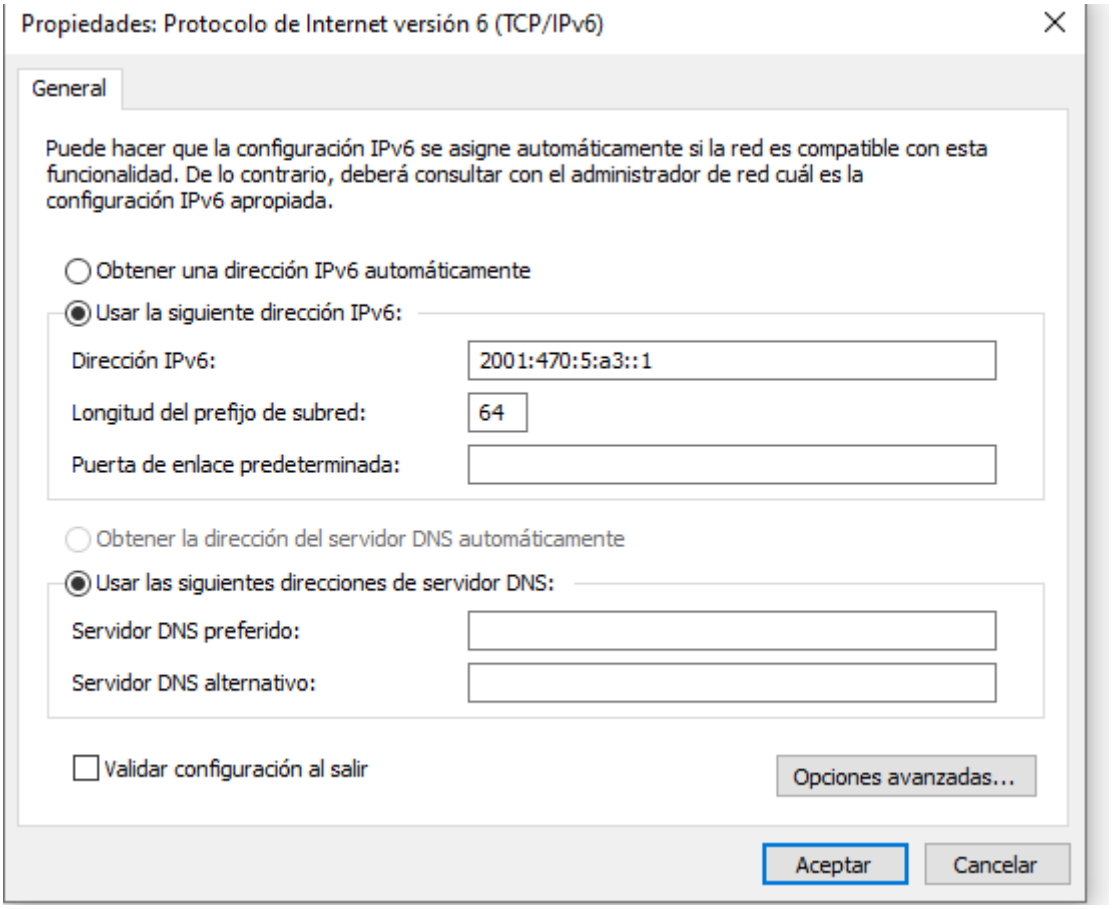


Figura 7.22 Se muestra la ventana de protocolos IPv6.

Luego, una vez configurado todas las IPv6 de los dispositivos comprobamos que tenga conexión entre los equipos para que puedan enviarse paquetes entre sí por medio de un ping como se puede apreciar en la Figura 7.23.

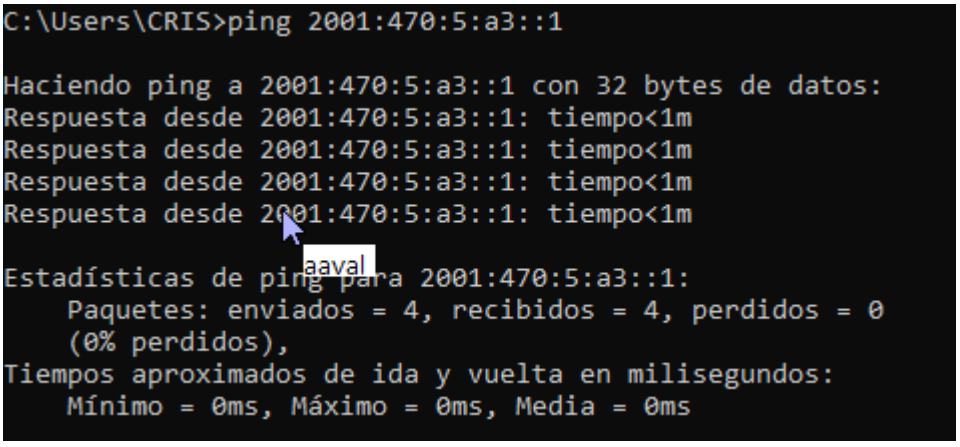


Figura 7.23 Realización de ping de la maquina ventas1(CRIS) a máquina bodega3.

```
[admin@MikroTik] > ping 2001:470:5:a3::2
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 2001:470:5:a3::2                           56 255 1ms   echo reply
    1 2001:470:5:a3::2                           56 255 0ms   echo reply
    2 2001:470:5:a3::2                           56 255 0ms   echo reply
    3 2001:470:5:a3::2                           56 255 0ms   echo reply
    4 2001:470:5:a3::2                           56 255 0ms   echo reply
    5 2001:470:5:a3::2                           56 255 3ms   echo reply
    6 2001:470:5:a3::2                           56 255 0ms   echo reply
    7 2001:470:5:a3::2                           56 255 0ms   echo reply
    8 2001:470:5:a3::2                           56 255 0ms   echo reply
    9 2001:470:5:a3::2                           56 255 0ms   echo reply
    sent=10 received=10 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=3ms
```

aaval

Figura 7.24 Realización ping del terminal mikrotik al router mercusys.

```
[admin@MikroTik] > ping 2001:470:5:a3:690c:55f:7bc0:3468
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 2001:470:5:a3:690c:55f:7bc0:3468           56 255 0ms   echo reply
    1 2001:470:5:a3:690c:55f:7bc0:3468           56 255 0ms   echo reply
    2 2001:470:5:a3:690c:55f:7bc0:3468           56 255 0ms   echo reply
    3 2001:470:5:a3:690c:55f:7bc0:3468           56 255 0ms   echo reply
    4 2001:470:5:a3:690c:55f:7bc0:3468           56 255 0ms   echo reply
    5 2001:470:5:a3:690c:55f:7bc0:3468           56 255 0ms   echo reply
    6 2001:470:5:a3:690c:55f:7bc0:3468           56 255 0ms   echo reply
    7 2001:470:5:a3:690c:55f:7bc0:3468           56 255 0ms   echo reply
    sent=8 received=8 packet-loss=0% min-rtt=0ms avg-rtt=0ms max-rtt=0ms
```

Figura 7.25 Realización ping del terminal mikrotik a la maquina Ventas1(Cris).

```
Adaptador de Ethernet Ethernet:

   Sufijo DNS específico para la conexión. . :
   Dirección IPv6 . . . . . . . . . . . . : 2002:c0a8:bfd:10:690c:55f:7bc0:3468
   Dirección IPv6 temporal. . . . . . . . : 2002:c0a8:bfd:10:8db2:2c8a:8cce:355c
   Vínculo: dirección IPv6 local. . . . . : fe80::690c:55f:7bc0:3468%11
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.0.100
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::c225:2fff:fe0c:914%11
                                       192.168.0.1

Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . :
   Vínculo: dirección IPv6 local. . . . . : fe80::5834:f8f3:46:f026%25
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.12
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : fe80::1%25
                                       192.168.1.1
```

Figura 7.26 IPv6 de la maquina bodega1.

```
C:\Users\CRIS>ping 2001:470:5:a3:e888:6f51:287a:190f

Haciendo ping a 2001:470:5:a3:e888:6f51:287a:190f con 32 bytes de datos:
Respuesta desde 2001:470:5:a3:e888:6f51:287a:190f: tiempo=1ms
Respuesta desde 2001:470:5:a3:e888:6f51:287a:190f: tiempo<1m
Respuesta desde 2001:470:5:a3:e888:6f51:287a:190f: tiempo<1m
Respuesta desde 2001:470:5:a3:e888:6f51:287a:190f: tiempo<1m

Estadísticas de ping para 2001:470:5:a3:e888:6f51:287a:190f:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

Figura 7.27 Ping de la maquina Ventas1(CRIS) a la máquina bodega1.

7.3.3 Direcciones IP.

7.3.3.1 Direcciones IPv4.

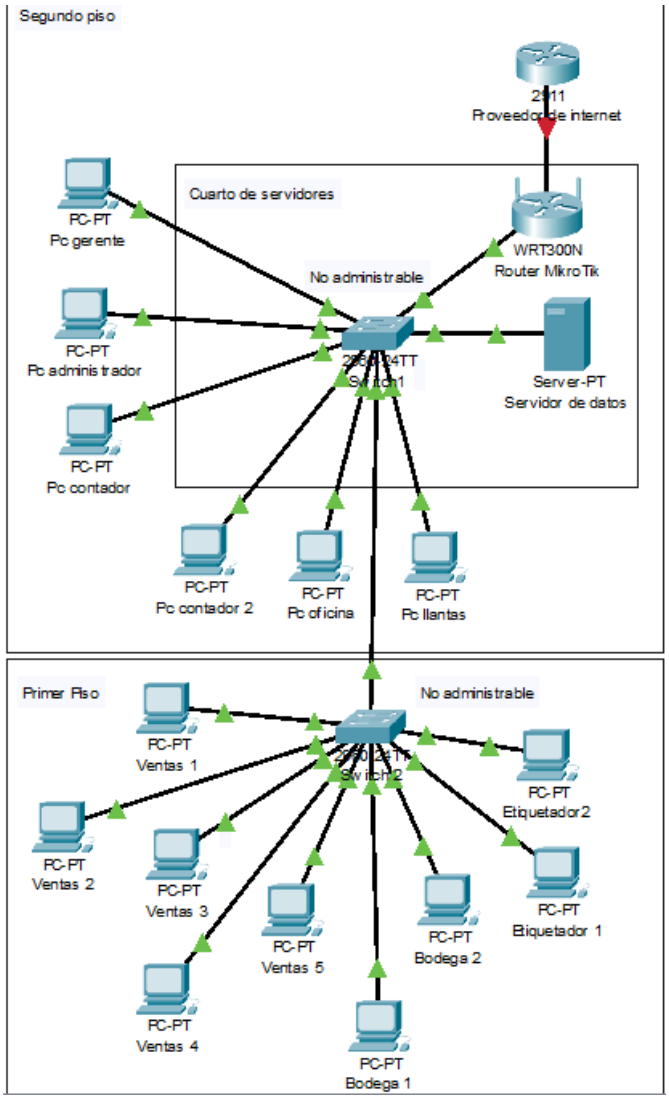


Figura 7.28 Estructura de red IPv4.

Tabla 7.1 Direcciones IPv4.

Servidor	192.168.9.100
Pc gerente	192.168.9.63
Pc administrador	192.168.9.64
Pc contador	192.168.9.80
Pc contador 2	192.168.9.90
Pc oficina	192.168.9.50
Pc llantas	192.168.9.57
Ventas 1	192.168.9.53
Ventas 2	192.168.9.55
Ventas 3	192.168.9.56
Ventas 4	192.168.9.59
Ventas 5	192.168.9.60
Bodega 1	192.168.9.92
Bodega 2	192.168.9.99
Etiquetador 1	192.168.9.96
Etiquetador 2	192.168.9.97
Cable	UTP categoría 5e

7.3.3.2 Direcciones IPv6

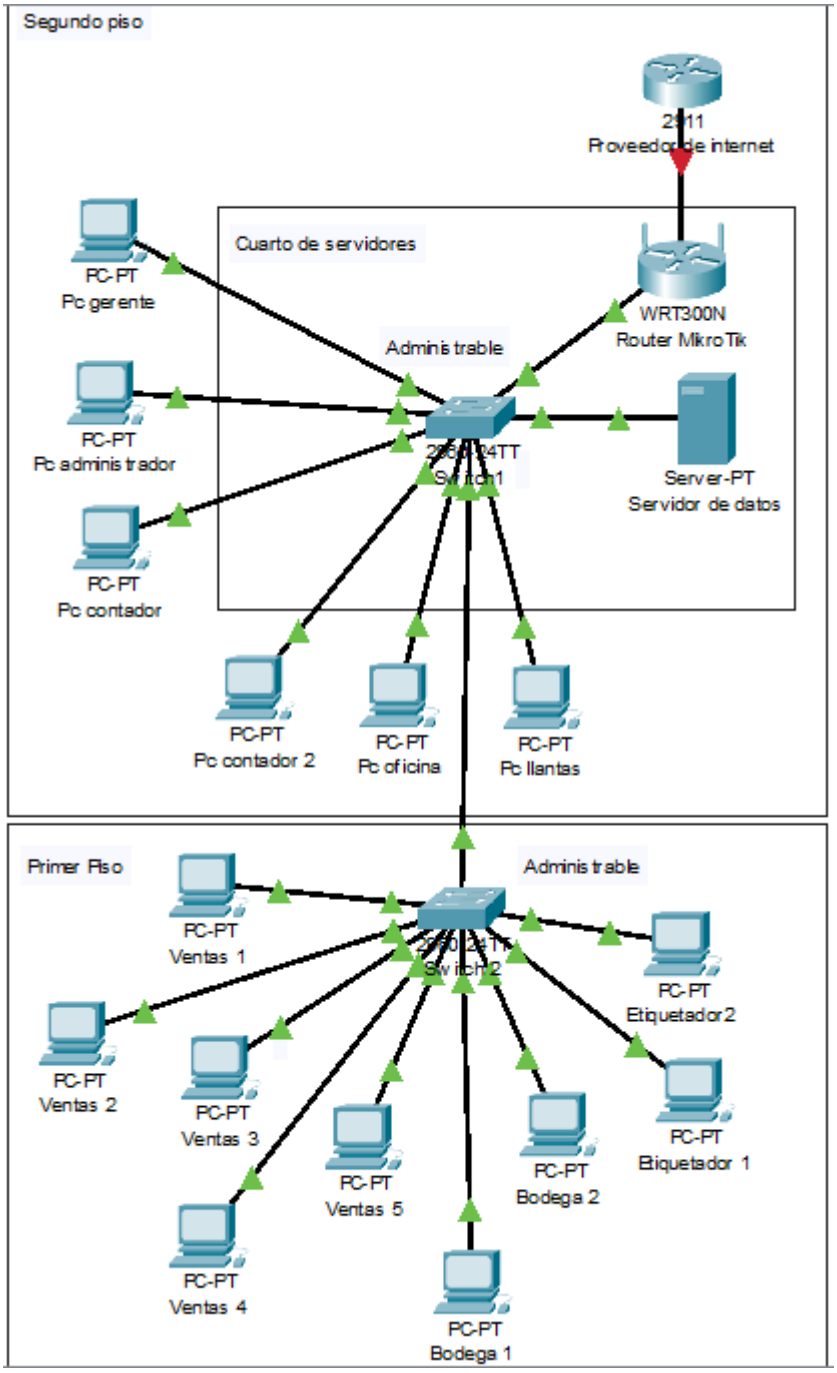


Figura 7.29 Estructura de red IPv6.

Tabla 7.2 Direcciones IPv6.

Servidor	2001:470:5:a3::2
Pc gerente	2001:470:5:a3::3
Pc administrador	2001:470:5:a3::4
Pc contador	2001:470:5:a3::5
Pc contador 2	2001:470:5:a3::6
Pc oficina	2001:470:5:a3::7
Pc llantas	2001:470:5:a3::8
Ventas 1	2001:470:5:a3::9
Ventas 2	2001:470:5:a3::10
Ventas 3	2001:470:5:a3::11
Ventas 4	2001:470:5:a3::12
Ventas 5	2001:470:5:a3::13
Bodega 1	2001:470:5:a3::14
Bodega 2	2001:470:5:a3::15
Etiquetador 1	2001:470:5:a3::16
Etiquetador 2	2001:470:5:a3::17
Cable	Red U/utp Nexxt Cat 6 305m Interior Certifica Gigabit

7.4 TABLA DE COMPROBACIÓN DE LA HIPÓTESIS

Tabla 7.3 Tabla comparativa – Resultados de la aplicación en la empresa

Modelo de estructura de red en protocolos IPv4	Modelo de estructura de red en protocolos IPv6
➢ En la estructura de IPv4 la velocidad de transmisión de datos es de entre 12 a15 Mbits/sec, teniendo pérdida de paquetes.	➢ En modelo de IPv6 la velocidad de transmisión de datos se pudo mejor entre 95.2 a 114 Mbits/sec, por lo tanto, podemos decir que existe un aumento del 87%.
➢ La empresa no contaba con confidencialidad en su red ya que cualquier dispositivo externo podía acceder a esta, a su vez no poseía un cifrado de paquetes.	➢ La empresa cuenta con una red que brinda confidencialidad, debido a que los dispositivos autorizados como lo son el nuevo Mikrotik Router y Mikrotik Switch administrable pueden acceder a esta red y al envío de paquetes de manera autentificada y cifrada.

7.4.1 Verificación de resultados en la migración de IPv4 a IPv6.

Luego procedemos a comparar la velocidad que teníamos con Ipv4 al momento de enviar un paquete por medio de la aplicación ipfer3 que nos permite visualizar el tiempo de transferencia de datos donde se puede apreciar que tenemos un valor de 12 a 15 Mbits/sec. Como se muestra en la Figura 7.28 en el test de velocidad

7.4.1.1 Verificación con IPv4 (Antes).

```
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
Accepted connection from 192.168.9.63, port 50712
[  5] local 192.168.9.56 port 5201 connected to 192.168.9.63 port 50713
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-1.00   sec   893 KBytes  7.29 Mbits/sec
[  5]   1.00-2.00   sec  1.23 MBytes  10.3 Mbits/sec
[  5]   2.00-3.00   sec  1.49 MBytes  12.5 Mbits/sec
[  5]   3.00-4.01   sec  1.46 MBytes  12.1 Mbits/sec
[  5]   4.01-5.00   sec  1.51 MBytes  12.8 Mbits/sec
[  5]   5.00-6.00   sec  1.63 MBytes  13.7 Mbits/sec
[  5]   6.00-7.01   sec  1.77 MBytes  14.8 Mbits/sec
[  5]   7.01-8.01   sec  2.03 MBytes  17.1 Mbits/sec
[  5]   8.01-9.00   sec  1.64 MBytes  13.8 Mbits/sec
[  5]   9.00-10.01  sec  1.34 MBytes  11.2 Mbits/sec
[  5]  10.01-10.16  sec   252 KBytes  13.3 Mbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bandwidth
[  5]   0.00-10.16  sec  0.00 Bytes  0.00 bits/sec                  sender
[  5]   0.00-10.16  sec  15.2 MBytes  12.6 Mbits/sec                  receiver
-----------------------------------------------------------
```

Figura 7.30 Test de velocidad.

Tenemos que en Ipv4 el envió de paquete es visible para las personas y el mensaje no está encapsulado al momento que se realiza una transferencia por lo cual lo comprobamos por medio del programa wireshark que nos permite ver toda la trayectoria de un paquete de principio a fin donde podemos aprecia que hemos hecho un ping a la IP de Google.

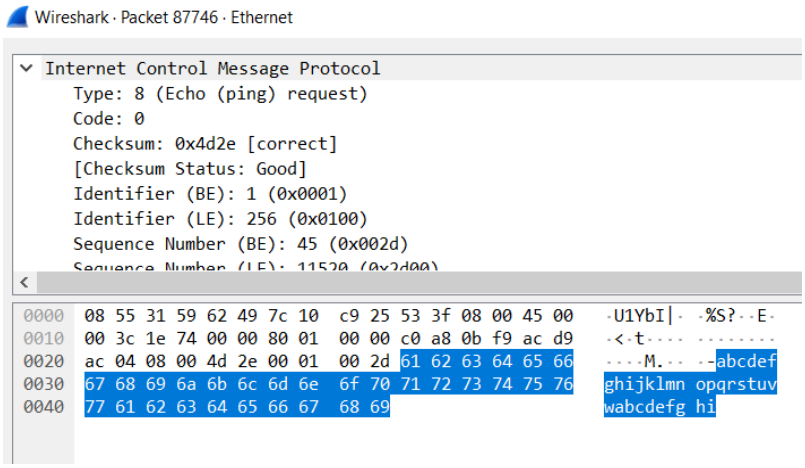


Figura 7.31 Seguridad con IPv4.

Figura 7.32 Ping realizado a Google.

7.4.1.2 Verificación con IPv6 (Después).

En esta parte tenemos la comprobación con el direccionamiento de IPv6 para medir la velocidad de transferencia con el programa ipfer3 lo cual podemos apreciar que tenemos un intervalo de 114 a 95.2 Mbits/sec lo cual es una diferencia enorme de la que teníamos antes como se puede apreciar en la Figura 7.31.

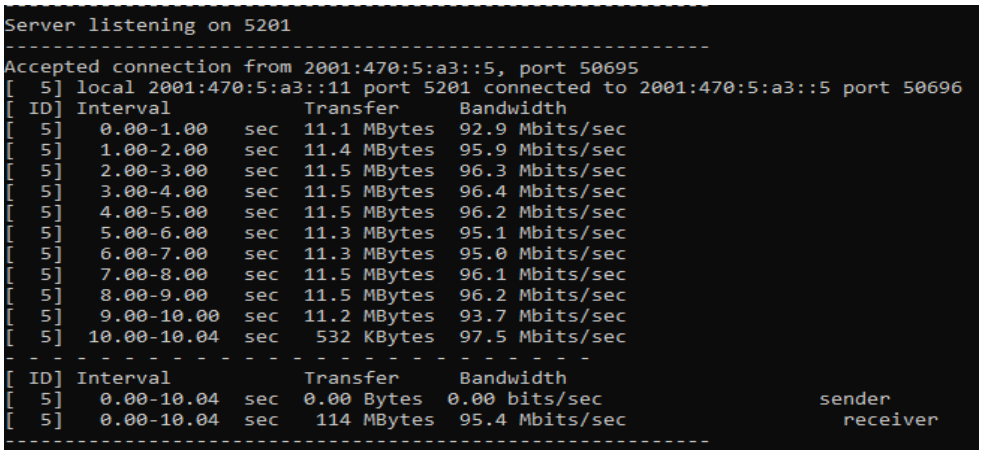


Figura 7.33 IPv6 Test velocidad

Figura 7.34 IPv6 Ping

Tenemos que en IPv6 él envió de paquete no es visible para las personas y el mensaje está encapsulado al momento que se realiza una transferencia por lo cual lo comprobamos por medio del programa wireshark que nos permite ver toda la trayectoria de un paquete de principio a fin como se puede apreciar en la Figura 7.33.

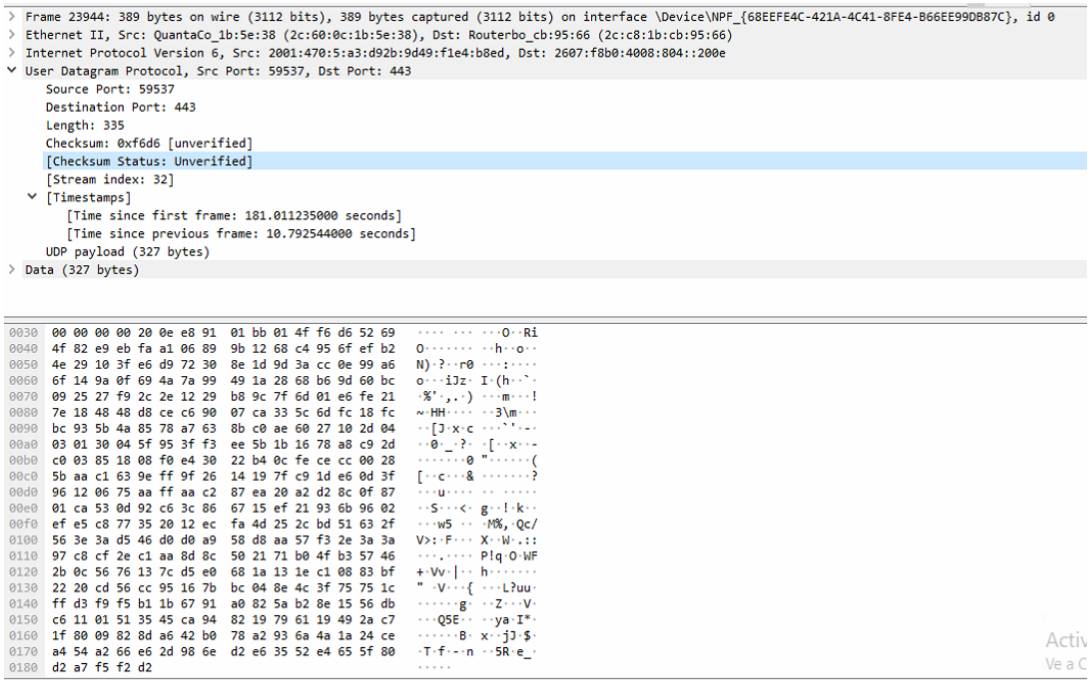


Figura 7.35 IPv6 Seguridad.

7.5 Cálculo de velocidad de envió de datos.

Calculo para obtener el resultado del porcentaje de mejora de la velocidad de envío de datos

Velocidad de envió de datos en IPv4

12-15 Mbits/sec

Velocidad de envió de datos en IPv6

95.2-114 Mbits/sec

Tabla 7.4 Cálculo de velocidad de envío de datos.

Cálculo de velocidad de envió de datos	
Prueba 1	**Prueba 2**
Prueba de velocidad IPv4: $x = 12$ **Prueba de velocidad IPv6:** $y = 95.2$ $$i = y - x$$ $$i = 95.2 - 12 = 83.2$$ $$p = \frac{i}{y} * 100\%$$ $$p = \frac{83.2}{95.2} * 100 = 87.39\%$$ **Porcentaje de mejora de la primera prueba:** $p = 87.39\%$	**Prueba de velocidad IPv4:** $x = 15$ **Prueba de velocidad IPv6:** $y = 114$ $$i = y - x$$ $$i = 114 - 15 = 99$$ $$p = \frac{i}{y} * 100$$ $$p = \frac{99}{114} * 100 = 86.84\%$$ **Porcentaje de mejora de la primera prueba:** $p = 86.84\%$

El porcentaje de mejora en el envío de datos que se pudo obtener en la migración de IPv4 a IPv6 es entre el 86% al 87%.

7.6 Estimación de Costos.

7.6.1 Costo-Beneficio.

Tabla 7.5 Costo-Beneficio.

Cantidad	Objeto	Costo	Beneficio
40 metros	Cable Utp Anera Categoría 6 Cobre Certificado	$25	Soporta una velocidad de trasmisión más alta (10 Gigabits). Su ancho de banda es de mejor calidad (250 MHz). Puede usarse tanto para exteriores como para interiores. Su estructura interna permite una mayor de disminución de ruido y diafonía
1	Mikrotik Switch	$425	Mejore el aislamiento de fallas. Simplifica la gestión de seguridad. Admite la contabilidad de flujos y escalabilidad de alta velocidad. La latencia de red más baja como paquete no tiene que hacer saltos adicionales para pasar a través de un router.

1	Mikrotik Router	$80	Permite un enrutamiento dinámico, balanceo y vinculación de carga y un monitoreo en tiempo real. Cuenta con mecanismos de calidad de servicio avanzada para asegurar la fluidez en el tráfico de la red. Le asigna una Ip publica y estática a tu router. Puertos con capacidad de un Giga-bit
20	Conectores Rj45 Categoría 6	$5	Se usan del mismo tipo y velocidad que el cable de red empleado para evitar incompatibilidad y causar efectos negativos como creación de ruido, interferencia, etc.
1	Malla Para Polvo	$2	Permite el flujo de aire evitando que entre polvo y evitar el ingreso de cualquier agente extraño.
10	Canaletas	$26	Disminuye ruido y diafonía Protege y ordena el cableado realizado.
30	Amarras Plásticas	$3	Permite organizar y fijar el cableado en la instalación realizada
Total		$566	

Una vez realizado el análisis correspondiente se determina que el valor del Costo – Beneficio de haber realizado este proceso es de $ 566, en mismo que se estima recuperar en el tiempo de 3 mes.

8 CONCLUSIONES Y RECOMENDACIONES

8.1 CONCLUSIONES

- Al realizar una búsqueda de exhaustiva de la información necesaria referente a IPv6 y al sistema de cableado estructurado se pudo identificar un sin número de trabajos relacionados a la investigacion, sin embargo, el uso de estas será enfocado en el tipo de red y estructura que se desea establecer con el fin de mejorar el rendimiento de la red, así se busca que la transmisión de datos sea más efectiva.
- Mediante la aplicación de la encuesta se ha podido analizar la preferencia de los involucrados por una red más eficiente y optima con el fin de facilitar él envió de datos de forma más rápida y segura, de esta manera se puede garantizar la integridad, disponibilidad y confidencialidad de la información.
- La transición a IPv6, implica un aumento en la seguridad a nivel de capa de red, ya que el protocolo IPsec se vuelve obligatorio, y esto permite que se cree una estructura de seguridad más fuerte y por ende aplicaciones más seguras.

8.2 RECOMENDACIONES

- Con el fin de que la transición sea factible y óptima antes del proceso se debe diseñar un plan de implementación en donde se considere varios aspectos importantes como el tamaño de la red, diseño de la topología de red, distribución de las direcciones IP, recursos tecnológicos, etc.
- Tomar en cuenta que los dispositivos tecnológicos existentes dentro de la red en protocolos IPv4 puedan tolerar un cambio de protocolos a IPv6, ya que estos requieren características específicas dentro de los dispositivos, caso contrario se los debe renovar por dispositivos de capa 3.
- Dentro del proyecto de cableado estructurado, se consideran políticas y seguridades de utilización dentro de los servicios de navegación para solventar inconvenientes como tolerancia a fallos, escalabilidad, calidad de servicio y seguridad.

9 BIBLIOGRAFÍA

[1] R. A. Chica Mora, *TRANSICIÓN AL PROTOCOLO IPV6, ASPECTOS DE SEGURIDAD INFORMÁTICA PARA TENER PRESENTE,* Bogotá: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, 2020.

[2] P. E. Tello Pérez y L. F. Pineda González, *ANÁLISIS DEL COMERCIO ELECTRÓNICO EN ECUADOR,* Quito: UNIVERSIDAD INTERNACIONAL DEL ECUADOR, 2017.

[3] A. Bejarano Ramirez, D. Miranda Castillo y J. Henriquez Celedon, *Trabajo presentado en la materia de REDES LAN Y WAN (IPv4 vs IPv6),* Maracaibo: Universidad Rafael Belloso Chacín, 2008.

[4] J. RIVERA GUARNIZO, *PLAN DE IMPLEMENTACIÓN PARA LA MIGRACIÓN A IPV6 EN LA RED DE LA FACULTAD DE CIENCIAS ADMINISTRATIVAS DE LA UNIVERSIDAD DE GUAYAQUIL,* Guayaquil, 2015.

[5] D. F. Ramírez Pulido, J. G. Pantoja y B. D. J. Alirio, *DISEÑO DE LA TRANSICIÓN DEL PROTOCOLO IPV4 HACIA IPV6 EN LA AGENCIA COLOMBIANA PARA LA REINTEGRACIÓN-ACR CON BASE EN CONSIDERACIONES DE SEGURIDAD EN IMPLEMENTACIÓN DE IPV6,* Bogotá: Creative Commons, 2015.

[6] E. F. Arévalo Medina y A. L. Bejarano Ccriollo, *EVALUACIÓN DE LOS PROTOCOLOS IGP IPv4 E IPv6 SOPORTADOS POR EL IOS DE CISCO ENFOCADO A LA PRESTACIÓN DEL SERVICIO IPTV EN LA ESPOCH,* Riobamba: ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO, 2016.

[7] D. Pérez, *IPv6: Protocolos de enrutamiento bajo IPv6,* 2015.

[8] C. Cisneros Veloz, *Análisis de los parámetros de calidad en una red de distribución,* Quito: Escuela Politécnica Nacional, 2014.

[9] A. Acosta y S. Aggio, *IPv6 para Operadores de Red,* ISOC-AR, 2014.

[10] C. Garcia, *Análisis de Seguridad en Redes IPv6,* Madrid: Universidad Carlos III, 2014.

[11] J. Lobo y D. Rico, *Implementación de la Seguridad del Protocolo de Internet Versión 6,* UFPSO, 2012.

[12] F. A. Contreras Sánchez y E. G. Romero Maturana, *Guía para el Aseguramiento del Protocolo IPv6,* Dirección de Gobierno Digital, 2021.

[13] M. d. T. d. l. I. y. l. Comunicaciones, *Modelo de Seguridad y Privacidad de la Información e IPv6.*

[14] A. G. SABOGAL ORTIZ, *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,* 2017.

[15] G. Cicileo y R. Gagliano, *IPv6 para todos,* Buenos Aires: Asociacíon Civil Argentinos en internet, 2009.

[16] LACNIC, *Registro de organizaciones que implementan IPv6.*

[17] J. Bermejo, *Hacking Ético, Fases pruebas de Penetración, Edita y Maqueta,* Catilla de la Macha: IN-Nova, 2013.

[18] W. Tomasi, *Comunicaciones y redesde computadores,* España: Pearson Educación, 2004.

[19] W. Stallings, *Comunicaciones y redes de computadores,* España: Pearson Educación, 2004.

[20] A. Tanenbaum y D. Wetherall, *Redes de Computadoras (Quinta Edición),* México: Pearson Educación, 2015.

[21] L. E. CHAVEZ CHIMPAY, «Diseño de un sistema de cableado estructurado para el Hospital Regional de Moquegua.,» Lima, 2018.

[22] L. E. Chavez Chimpay, *Diseño de un sistema de cableado estructurado para el Hospital Regional de Moquegua,* Lima, 2018.

[23] J. Joskowicz, *Cableado Estructurado,* 2013.

[24] J. Gómez, *Redes Locales,* 2011.

[25] J. A. ASTUDILLO GALARZA, *ANÁLISIS SITUACIONAL DE LA INFRAESTRUCTURA TECNOLÓGICA PARA EL FORTALECIMIENTO DEL CENTRO DE DATOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN PEDRO CARBO,* Guayaquil, 2016.

[26] J. D. López Tabares y D. F. Zamora Ospina, «DISEÑO DE UNA RED LAN PARA LA EMPRESA MULTIWEB,» Bogotá, 2019.

[27] J. L. Ceja, J. C. Ramos, C. Mendoza, E. C. Rodíguez y M. V. Félix, «El diseño de la red de internet para el nuevo edificio del ITJMMPyH unidad académica mascota con base en normas internacionales,» *Investigación y Ciencia Aplicada a la Ingeniería,* vol. IV, nº 25, pp. 64-71, 2021.

[28] R. López Bulla, *Enrutamiento y Configuración de Redes,* Bogotá: Catalogación en la fuente Fundación Universitaria del Área Andina, 2018.

[29] Y. A. Beltran Ruiz, L. F. Celeita Gallegos, L. L. Sepúlveda Rondon, C. A. Rios Bohorquez y R. A. Rodríguez, *Implementación servicios de infraestructura IT:DHCP Server, DNS Server y Controlador de Dominio, Proxy no transparente, Cortafuegos, VPN, File Server y Print Server en Zentyal server,* Universidad Nacional Abierta y a Distancia UNAD, 2018.

[30] S. De Luz, «RZ redes zone,» 10 Junio 2021. [En línea]. Available: https://www.redeszone.net/tutoriales/vpn/ipsec-que-es-como-funciona/.

[31] M. J. Pibaque Villacreses, *RED DE DATOS CON QOS Y BALANCEO DE CARGA MEDIANTE LA,* Manabí: UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ, 2019.

[32] EcuRed, *Calidad de servicio.*

[33] C. D. Cable, *Cable UTP categoría 6 ¿Qué es?,* 2021.

[34] O. León, *Despliegue de IPv6 para el desarrollo socio económico en América Latina y el,* Uruguay: LACNIC, 2015.

[35] L. Navarro Caycho, *Enrutamiento y Protocolos de Enrutamiento,* 2012.

10 ANEXOS

ANEXO A: Hojas de vida de los investigadores.

10.1 Hoja de vida del tutor

UNIVERSIDAD TÉCNICA DE COTOPAXI

INFORMACIÓN PERSONAL

CÉDULA	APELLIDOS	NOMBRES	SEXO
1803386950	VILLA QUISHPE	MANUEL WILLIAM	MASCULINO
FECHA DE NACIMIENTO	NACIONALIDAD	ESTADO CIVIL	TIPO DE SANGRE
15-03-1984	ECUATORIANO	SOLTERO	ORH+
DIRECCIÓN PROVINCIA		DIRECCIÓN CANTÓN	
TUNGURAHUA		PILLARO	
DIRECCIÓN CALLES PRINCIPALES		REFERENCIA DOMICILIARIA	No. DE CASA
BOLIVAR		CASA DE DOS PISOS	S/N
CONTACTO	TELÉFONO CONVENCIONAL	TELÉFONO CELULAR	ALTERNATIVO
	032422416	0983855980	
EMAIL PERSONAL		EMAIL INSTITUCIONAL	
William_villa007@hotmail.com			
CONTACTO EN CASO DE REFERENCIA			
PARENTEZCO	NOMBRES Y APELLIDOS	TELÉFONO CONVENCIONAL	
HERMANO	QUISHPE CARMEN	TELÉFONO CELULAR	0980706390
INFORMACIÓN BANCARIA			

INSTRUCCIÓN FORMAL

NIVEL	REGISTRO SENESCYT	INSTRUCCIÓN EDUCATIVA	TÍTULO OBTENIDO	PAÍS DONDE REALIZÓ LOS ESTUDIOS
TERCER	1042-06-705068	UNIVERSIDAD REGIONAL AUTONOMA D ELOS ANDES	INGENIERO EN SISTEMAS E INFORMATICA	ECUADOR
TERCER	1042-04-490189	UNIVERSIDAD REGIONAL AUTONOMA D ELOS ANDES	LICENCIADO EN SISTEMAS COMPUTACIONALES	ECUADOR
CUARTO	1002-16-86076391	ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO	MAGISTER EN INTERCONECTIVIDAD DE REDES	ECUADOR
CUARTO	1042-08-676420	UNIVERSIDAD REGIONAL AUTONOMA D ELOS ANDES	DIPLOMA SUPERIOR EN COMERCIO EXTERIOR	ECUADOR

EXPERIENCIA LABORAL

EXPERIENCIA DOCENTE	INSTITUCIÓN	FACULTAD	MODALIDAD	FECHA DE INGRESO	FECHA DE SALIDA
5 MESES	UNIVERSIDAD TÉCNICA DE AMBATO	CONTABILIDAD Y AUDITORIA	PRESENCIAL	01-06-2012	
2 AÑOS	UNIVERSIDAD TÉCNICA DE AMBATO	CONTABILIDAD Y AUDITORIA	PRESENCIAL	01-10-2012	01-02-2014
5 AÑOS	UNIVERSIDAD TÉCNICA DE COTOPAXI	CIENCIAS AGROPECUARIAS Y RECURSOS NATURALES CIENCIAS DE LA INGENIERIA Y APLICADAS	PRESENCIAL	01-05-2016	ACTUALIDAD

EXPERIENCIA PROFESIONAL	INSTITUCIÓN	CARGO	MODALIDAD	FECHA DE INGRESO	FECHA DE SALIDA
4 años y 6 meses	UNIVERSIDAD REGIONAL AUTONOMA D ELOS ANDES	ADMINSITRADOR DE REDES	PRESENCIAL	2006-07	2011-03

4 meses	SERVICIOS COMUNIKT CEHER SOCIEDAD ANONIMA	JEFE DE SISTEMAS	PRESENCIAL	2011-07	2012-01
2 meses	MEGAPROFER S.A.	TECNICO DE SISTEMAS	PRESENCIAL	2012-02	2012-03
1 AÑO 10 meses	UNIVERSIDAD TECNICA DE AMBATO U.T.A.	ANALISTA DE TECNOLOGIAS DE LA COMUNICACIÓ N E INFORMACION	PRESENCIAL	2014-06	2016-04

CAPACITACIONES

NOMBRE DEL EVENTO	INSTITUCIÓN	DURACIÓ N (HORAS)	APROBACIÓ N /ASISTENCI A	FECHA INICIO	FECHA FIN	PAÍS
ACTUALIZACION EN DOCENCIA E INVESTIGACION UNIVERSITARIA EN BUSQUEDA ESPECIALIZADA DE INFORMACION CIENTIFICA	UNIVERSIDAD REGIONAL AUTONOMA DE LOS ANDES	120	SI	07/03/2018	15/04/2018	ECUADOR
CAPACITACION DE ACTUALIZACION DOCENTE CAREN	UNIVERSIDAD TECNICA DE COTOPAXI	30	SI	06/04/2017	12/08/2017	ECUADOR
I SEMINARIO DE INOCUIDAD DE ALIMENTOS AGROINUSTRIALES	UNIVERSIDAD TECNICA DE COTOPAXI	40	SI	16/01/2017	17/01/2017	ECUADOR
FORTALECIMIENTO DE LA CALIDAD DE LAS FUNCIONES SUSTANTIVAS DE LA UTC	UNIVERSIDAD TECNICA DE COTOPAXI	40	SI	13/03/2017	17/03/2017	ECUADOR
ELABORACIÓN DE PROYECTOS EN FORMATO SEMPLADES	UNIVERSIDAD TÉCNICA DE COTOPAXI, SECRETARIA NACIONAL DE PLANIFICACIÓN Y DESARROLLO	40	SI	04/06/2018	08/06/2018	ECUADOR
CISCO NETWORKING ACADEMY® CYBERSECURITY ESSENTIALS	UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA	30	SI	01/11/2018	18/11/2018	ECUADOR

INTRODUCCIÓN A LA SEGURIDAD CIBERNÉTICA DE CISCO NETWORKING ACADEMY®	ACADEMIA CISCO	15	SI	01/11/2018	18/11/2018	ECUADOR
METODOLOGÍAS AGILES SCRUM	UNIVERSIDAD REGIONAL AUTONOMA DE LOS ANDES	40	SI	18/11/2017	18/01/2018	ECUADOR
GESTIÓN ACADÉMICA MICROCURRICULAR	UNIVERSIDAD TÉCNICA DE COTOPAXI	40	SI	05/03/2018	09/03/2018	ECUADOR

CONGRESOS INTERNACIONALES

NOMBRE DEL EVENTO	INSTITUCIÓN	DURACIÓN (HORAS)	APROBACIÓN /ASISTENCIA	FECHA INICIO	FECHA FIN	PAÍS
I CONGRESO INTERNACIONAL DE INVESTIGACION CIENTIFICA	UNIVERSIDAD TECNICA DE COTOPAXI	40	SI	22/11/2017	24/11/2017	ECUADOR
VI CONGRESO INTERNACIONAL SOBRE TECNOLOGIA E INVESTIGACION CITICI 2048	CITICI, CIMTED	40	SI	16/05/2018	18/05/2018	ARGENTINA

ARTÍCULOS CIENTÍFICOS

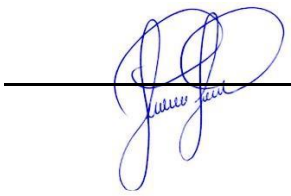
NOMBRE DEL TEMA	INSTITUCIÓN	ISSN	VOLUMEN	FECHA APROBACION	PAÍS
RECONOCIMIENTO FACIAL EN SUB-ESPACIOS: LINEALES Y NO-LINEALES, BASES DE DATOS DE ROSTROS Y MÁQUINA DE VECTORES DE SOPORTE	REVISTA ARJE DE POSTGRADOS UNIVERSIDAD DE CARABOBO	ISSN Versión electrónica 2443-4442, ISSN Versión impresa 1856-9153	22	06/06/2018	VENEZUELA

DATOS ADICIONALES

POSEE DISCACIDAD				TIPO DE DISCAPACIDAD	No. CARNET DE DISCAPACIDAD	IDENTIFICACIÓN ÉTNICA
SI		NO	X			INDIGENA

Certifico que todos los datos anotados son de mi absoluta responsabilidad.

Atentamente,



FIRMA DE RESPONSABILIDAD
ING MANUEL WILLIAM
VILLA QUISHPE, MG

10.2 Hoja de vida de los investigadores

10.2.1 Hoja de vida investigador 1

DATOS PERSONALES

NOMBRES Y APELLIDOS:	Angel Polivio Jativa Reyes
LUGAR Y FECHA DE NACIMIEINTO:	21 de mayo de 1999
CÉDULA DE CIUDADANÍA:	0804231421
SEXO:	Masculino
ESTADO CIVIL:	Soltero
DIRECCIÓN:	Av. Troncal de la Costa
TELÉFONO:	0979955295
E-MAIL:	angel.jativa1421@utc.edu.ec

PERFIL PROFESIONAL

Soy una persona responsable, puntual, creativa y con muy buena disposición para cualquier tarea que se me asigne. Tengo dos años de experiencia en mi campo y me encuentro realizando mi Ingeniería en Sistemas Computacionales.

10.2.2 Hoja de vida investigador 2

DATOS PERSONALES

NOMBRES Y APELLIDOS:	Paul Andrés Montaleza Paucar.
LUGAR Y FECHA DE NACIMIEINTO:	02 de febrero de 1997
CÉDULA DE CIUDADANÍA:	2350192536
SEXO:	Masculino
ESTADO CIVIL:	Soltero
DIRECCIÓN:	Rio putumayo y Av. Tsáchilas
TELÉFONO:	0987128873
E-MAIL:	paul.montaleza2536@utc.edu.ec

PERFIL PROFESIONAL

Soy una persona directa, flexible y con muy buena adaptabilidad para cualquier tarea que se me asigne. Tengo dos años de experiencia en mi campo y me encuentro realizando mi Ingeniería en Sistemas Computacionales.

FORMULARIO DE ENCUESTA

ANEXO B: Formulario de la encuesta.

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

Latacunga 08-2-2022

Tema:

Diseño de la transición del protocolo ipv4 hacia ipv6 en la empresa GrupoJativa con base en consideraciones de seguridad en implementación de ipv6.

Objetivo General:

Implementar una transición de protocolo IPV4 a IPV6 en la empresa GrupoJátiva S.A. ubicada en el cantón Esmeraldas, con base a consideraciones de seguridad de la misma.

Encuesta

1. ¿Alguna vez ha escuchado sobre el direccionamiento de IPv6?
   a) Si b) No

2. ¿Conoce Ud. sobre sobre los beneficios que brinda Ipv6?
   a) Si b) No

3. ¿Cree Ud. que las empresas deberían de trabajar con el protocolo de direccionamiento en IPv6?

a) Si b) No

4. ¿Conoce Ud. de algún proveedor de internet que otorgue Ipv6 dentro del País?

a) Si b) No

5. ¿Considera Ud. que la velocidad de datos aumenta con el direccionamiento de Ipv6?
   a) Si b) No

6. ¿Considera Ud. que la seguridad de datos aumenta con el direccionamiento de Ipv6?
   b) Si b) No

7. ¿Conoce Ud. los métodos para realizar una migración de IPv4 a IPv6?
   a) Si b) No

8. ¿Conoce Ud. cómo está estructurado el protocolo de direccionamiento de Ipv6?
   a) Si b) No

9. ¿Conoce Ud. que protocolo de Seguridad viene integrado en el direccionamiento de IPv6?

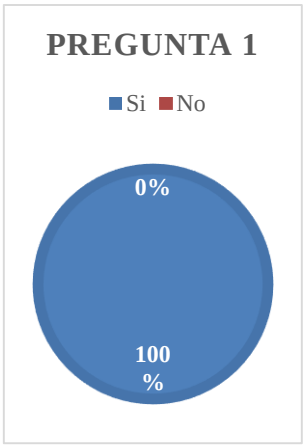
   a) Si b) No

10. ¿Conoce Ud. el protocolo de seguridad IPsec?
    a) Si b) No

RESULTADOS DE ENCUESTA

ANEXO C: Resultados de la encuesta.

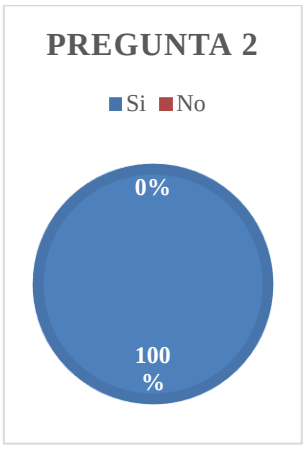
En la primera pregunta: "¿Alguna vez ha escuchado sobre el direccionamiento de IPv6?", obtuvimos el siguiente resultado.



Mediante la tabulación realiza podemos decir que el 100% de la población encuestada ha escuchado alguna vez sobre que es IPv6.

En conclusión, podemos decir que la población tiene un conocimiento base sobre lo que es IPv6.

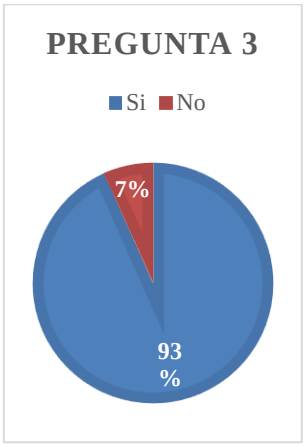
En la segunda pregunta: "¿Alguna vez ha escuchado sobre los beneficios que brinda IPv6?", obtuvimos el siguiente resultado.



Mediante la tabulación realizada podemos decir que el 100% de la población encuestada ha escuchado sobre los beneficios que ofrece IPv6.

En conclusión, podemos decir que la población sabe acerca de los beneficios que tiene IPv6.

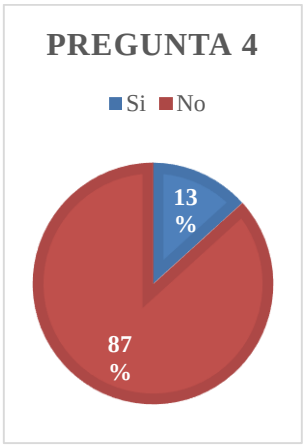
En la tercera pregunta: “¿Cree Ud. que las empresas deberían de trabajar con el protocolo de direccionamiento en IPv6?”, obtuvimos el siguiente resultado.



Mediante la tabulación realizada podemos decir que el 93% de la población desea trabajar con el protocolo de direccionamiento en IPv6.

En conclusión, podemos decir que la mayoría población encuestada al saber sobre que es IPv6 y saber acerca de los beneficios que tiene, desea poder trabajar en IPv6.

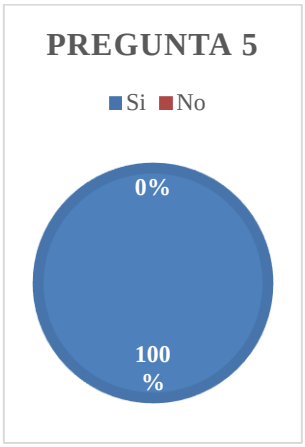
En la cuarta pregunta: “¿Conoce Ud. de algún proveedor de internet que otorgue IPv6 dentro del País?”, obtuvimos el siguiente resultado.



Mediante la tabulación realizada podemos decir que el 87% de la población encuestada no conoce proveedores que ofrezcan IPv6.

En conclusión, podemos decir que la población desconoce sobre posibles proveedores de internet que otorguen una red IPv6.

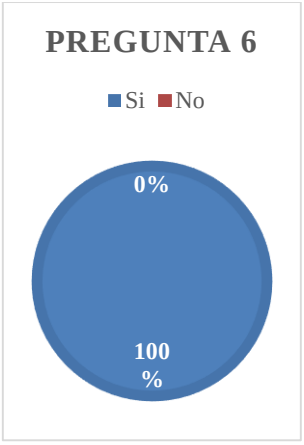
En la quinta pregunta: "¿Considera Ud. que la velocidad de datos aumenta con el direccionamiento de IPv6?", obtuvimos el siguiente resultado



Mediante la tabulación realizada podemos decir que el 100% de la población encuestada considera que IPv6 aumentara la velocidad de datos.

En conclusión, podemos decir que la población considera que al momento de cambiarse a IPv6 aumentara él envió de datos de un puesto de trabajo a otro y agilizara el trabajo que realizan.

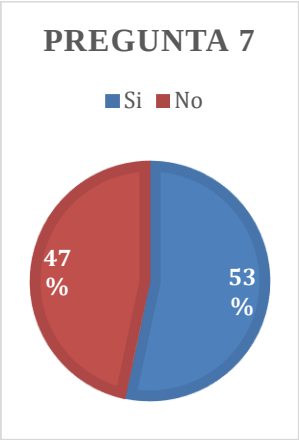
En la sexta pregunta: "¿Considera Ud. que la seguridad de datos aumenta con el direccionamiento de Ipv6?", obtuvimos el siguiente resultado.



Mediante la tabulación realizada podemos decir que el 100% de la población encuestada ha considera que la seguridad aumenta en IPv6.

En conclusión, podemos decir que la población conoce la situación de inseguridad en la que se encuentra y creen que una solución viable seria cambiarse a una red IPv6.

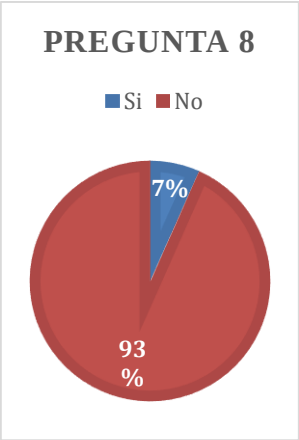
En la séptima pregunta: "¿Conoce Ud. los métodos para realizar una migración de IPv4 a IPv6?", obtuvimos el siguiente resultado.



Mediante la tabulación realizada podemos decir que el 53% de la población encuestada ha saben sobre cuáles son los métodos para realizar una migración de IPv4 a IPv6.

En conclusión, podemos decir que la población tiene un conocimiento de como seria realizar la migración como, por ejemplo: el cambio de equipos a unos más actuales que soporten la red; esto solo se pudo constatar en el equipo técnico de la empresa que además pudieron expresar que no tenían conocimiento sobre la configuración de los equipos para migrar a IPv6.

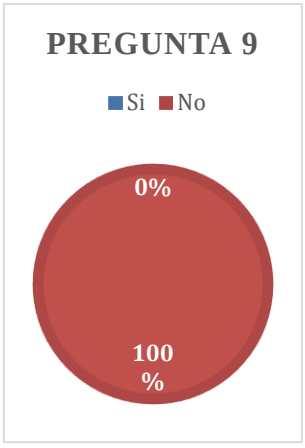
En la octava pregunta: "¿Conoce Ud. que protocolo de Seguridad viene integrado en el direccionamiento de IPv6?", obtuvimos el siguiente resultado.



Mediante la tabulación realizada podemos decir que el 93% de la población encuestada ha no conoce sobre que protocolos de seguridad usa IPv6.

En conclusión, podemos decir que la población que casi nadie sabe sobre que protocolos usa IPv6 excepto en un caso.

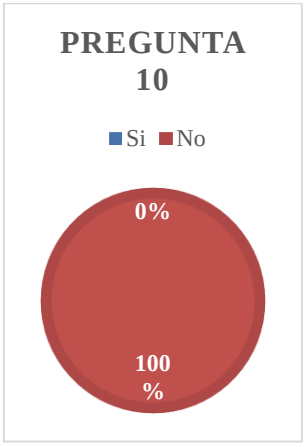
En la novena pregunta: "¿Conoce Ud. cómo está estructurado el protocolo de direccionamiento de IPv6?", obtuvimos el siguiente resultado.



Mediante la tabulación realizada podemos decir que el 100% de la población no conoce de cómo está estructurado el direccionamiento de IPv6.

En conclusión, podemos decir que la población no sabe acerca de cómo se estructura el protocolo de direccionamiento IPv6.

En la décima pregunta: "¿Conoce Ud. el protocolo de seguridad IPsec?", obtuvimos el siguiente resultado.



Mediante la tabulación realizada podemos decir que el 100% de la población encuestada no conoce el protocolo de seguridad IPsec.

En conclusión, podemos decir que la población no sabe que es IPsec o de cómo funciona en IPv6.

ANEXO D: Inventario físico de equipos de computación de la empresa grupo Játiva.

10.2.3 Inventario físico de los equipos.

Empresa Grupo Játiva	
Ruc de la empresa: #	
Toma física de equipos de computación	
Cantidad	Descripción
1	Servidor Intel Core I5 9400F de 16 RAM
11	Computador Core I5 9400F de 4 RAM
1	Computador Intel Pentium(R) G4400 de 4 RAM
2	Computador Intel Core I3 4170F de 4 RAM
1	Computador Intel Core I3 7100F de 4 RAM
1	MikroTik RouterBOARD modelo RB750r2
1	MikroTik Cloud Smart Switch modelo CSS326-24G-2S+RM
Observación: Una vez tomado el inventario físico de los equipos que existen en la Empresa Grupo Játiva, se procede a realizar la migración de las IP de cada equipo a un nuevo diseño de red para la empresa.	

ANEXO E: Estado de estructura de red.

10.2.4 Estado de la estructura de red (Antes – IPv4).

Figura 10.1 Switch TP Link no administrable.

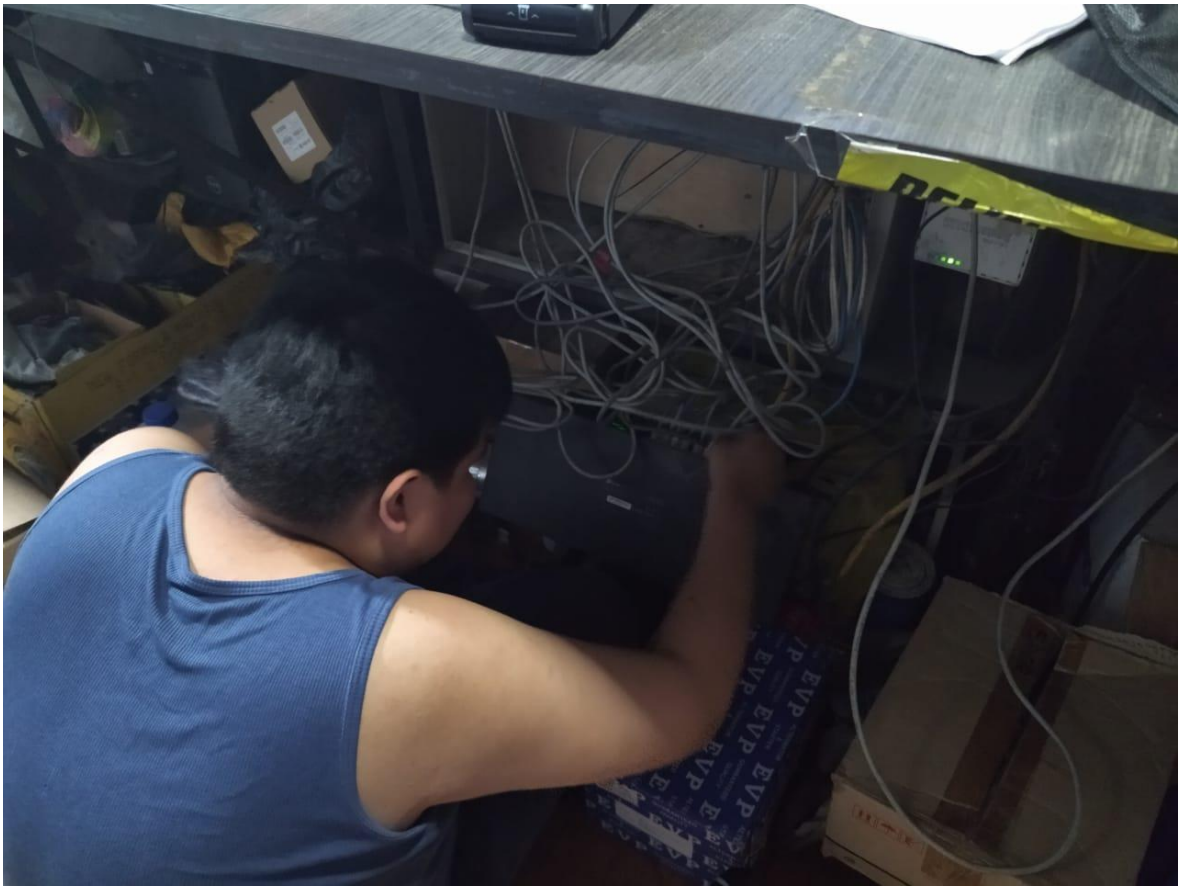


Figura 10.2 Comprobación del estado del cableado.

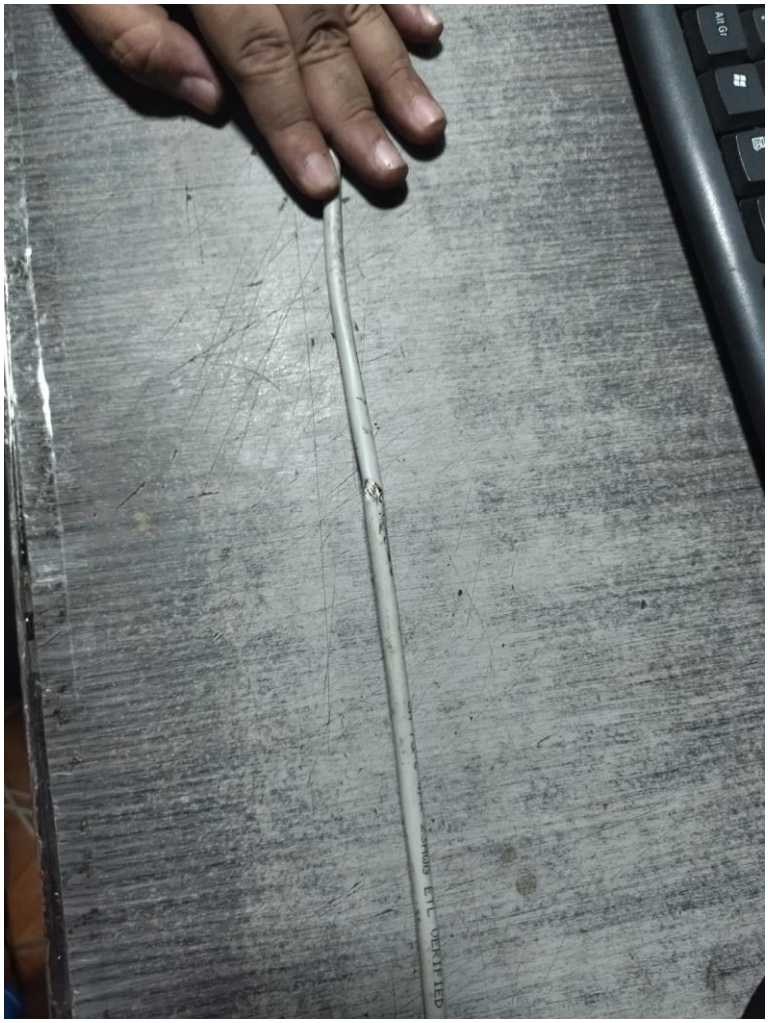


Figura 10.3 Cable categoría 5E

Figura 10.4 Estado del cableado categoría 5E

Figura 10.5 Estado de conectores RJ45.

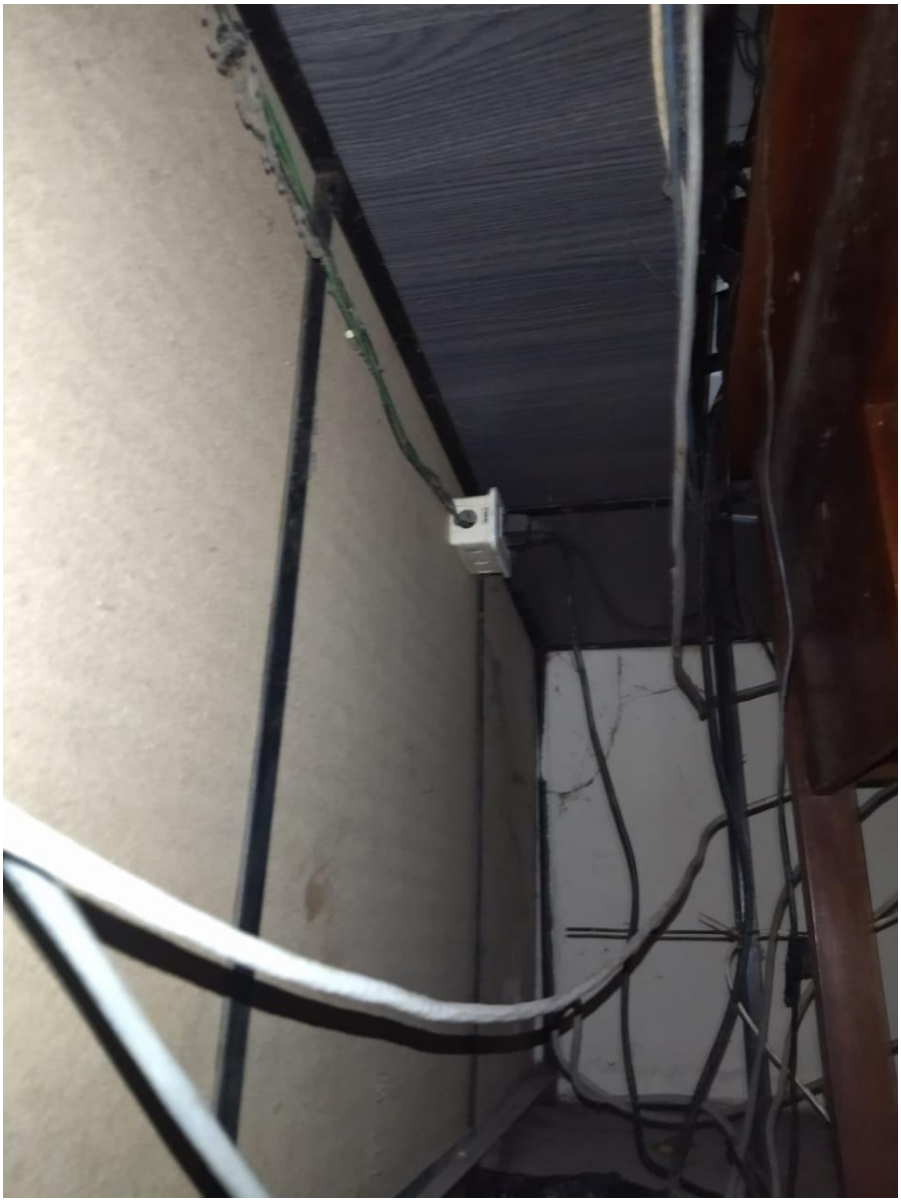


Figura 10.6 Estructura del cableado sin canaletas.

10.2.5 Estructura de la estructura de red (Después – Ipv6)

Figura 10.7 Micro tic Router OS.

Figura 10.8 Canaletas por donde se pasa el cableado.

Figura 10.9 Switch de 16 puertos TP Link.

Figura 10.11 Router ZTE - ZXHNFC70L Proveedor primer piso.

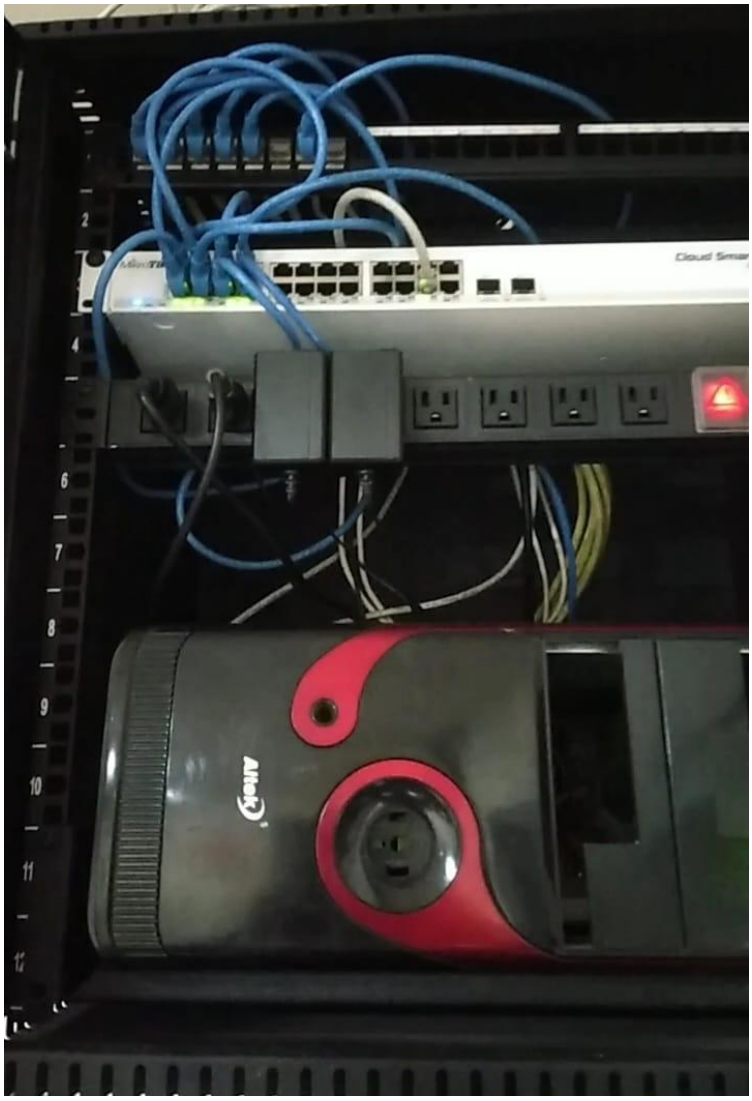


Figura 10.12 Estructura del rack y switch administrable.

Figura 10.13 Estructura de switch administrable.

ANEXO F: Esquema de red antes y después.

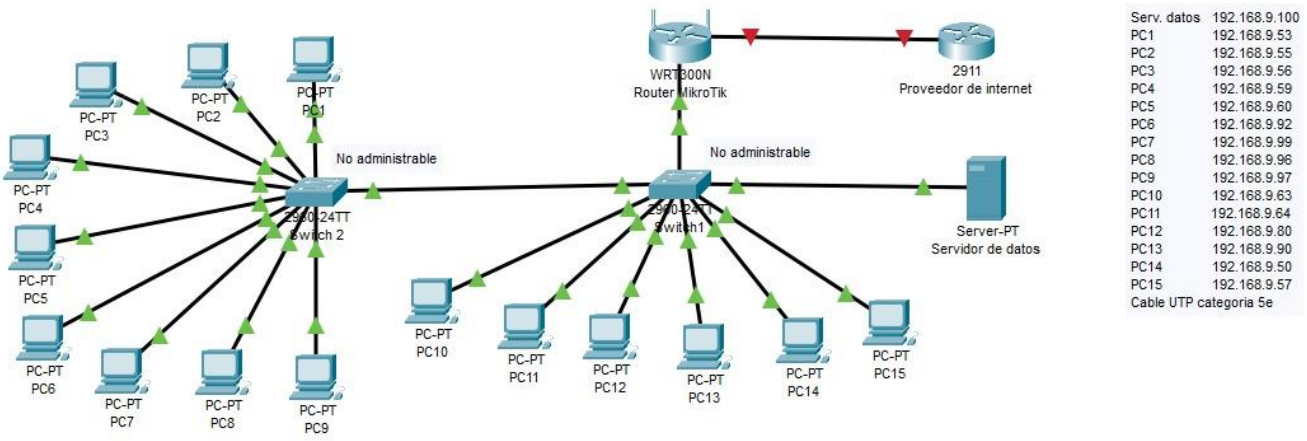


Figura 10.14 Esquema de la red antes (Protocolos IPv4)

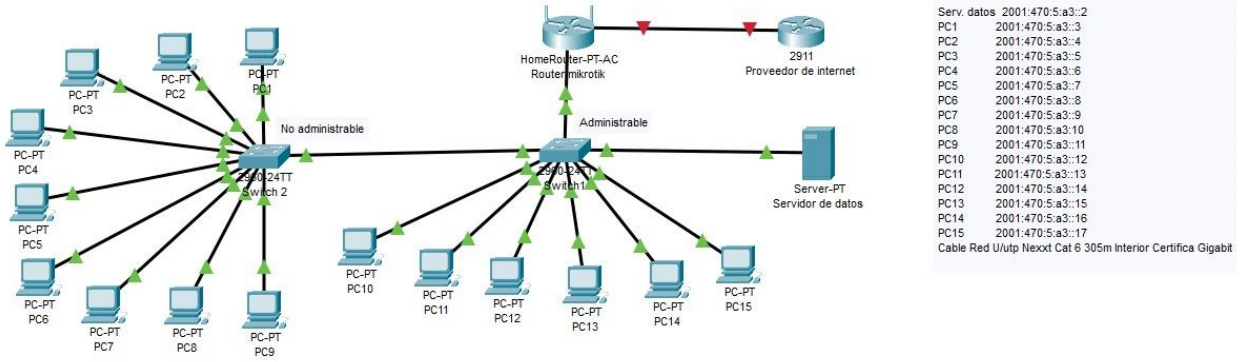


Figura 10.15 Esquema de la red después (Protocolos IPv6)

ANEXO G: Ping realizados desde diversas máquinas de la empresa GrupoJativa para la comprobación de conexión.

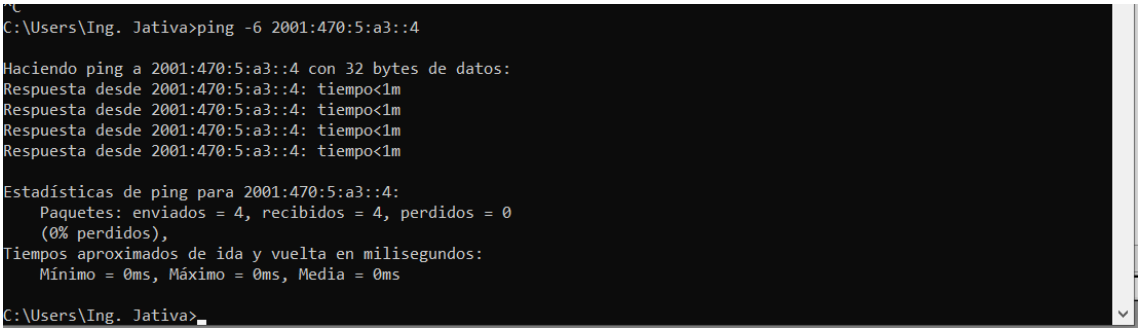


Figura 10.16 En esta parte se realiza ping a la máquina de Caja que está en el segundo piso desde la máquina de Bodega1 lo cual nos da la información que están conectada entre sí.

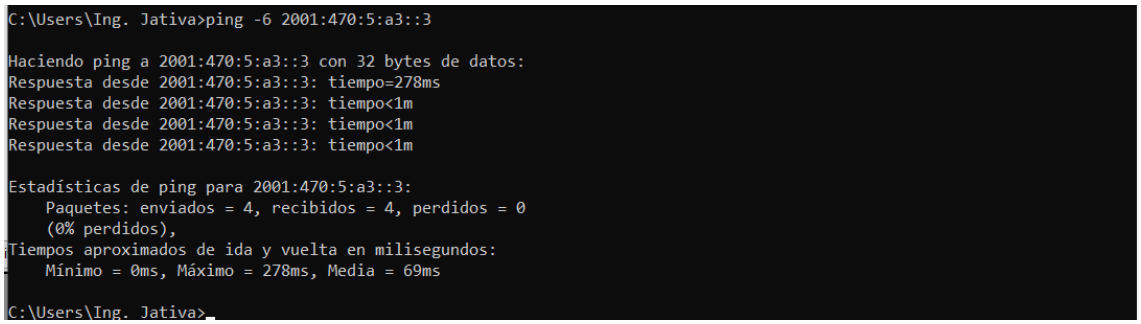


Figura 10.17 En esta imagen apreciamos se realiza ping a la máquina de Ventas1 del segundo piso desde la máquina de Bodega1.

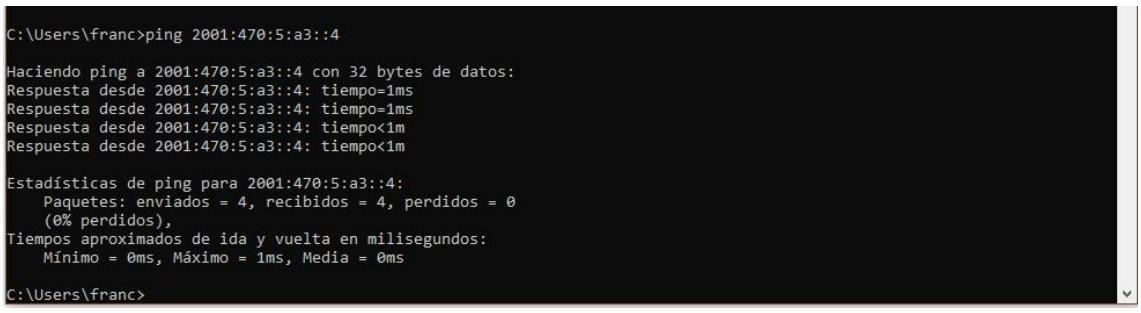


Figura 10.18 En esta imagen se visualiza el ping entre la máquina de Caja del segundo piso con la máquina de Ventas1.

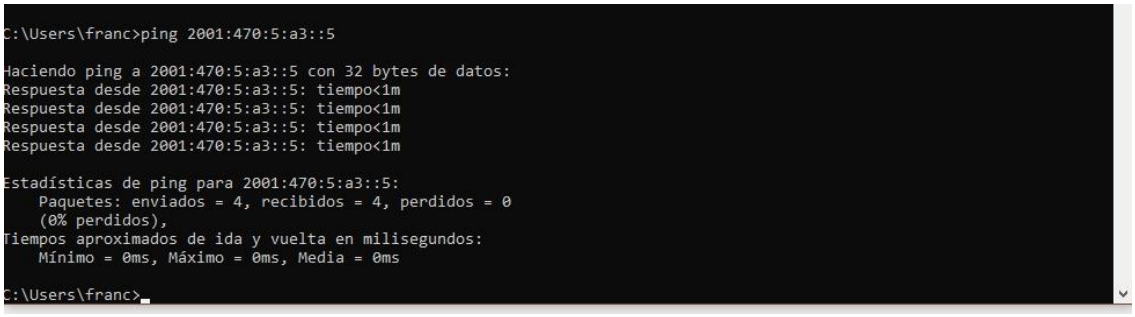


Figura 10.19 En esta imagen se visualiza el ping entre la máquina de Caja del segundo piso con la máquina de Bodega1 del primer piso.

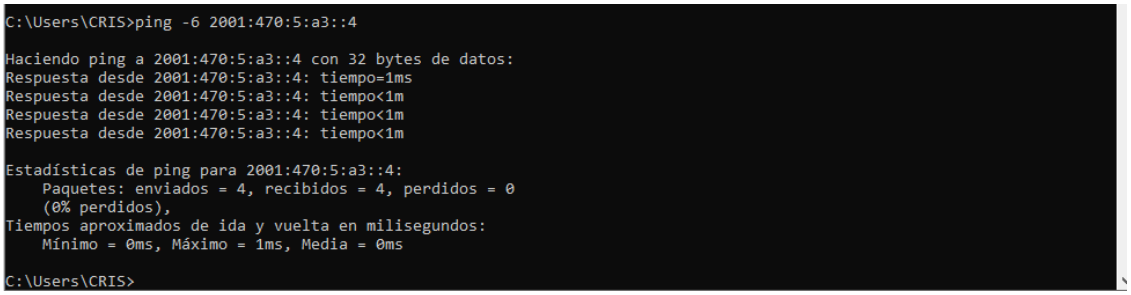


Figura 10.20 En esta imagen se realiza ping a la máquina de Caja que está en el primer piso desde la máquina de Ventas1.

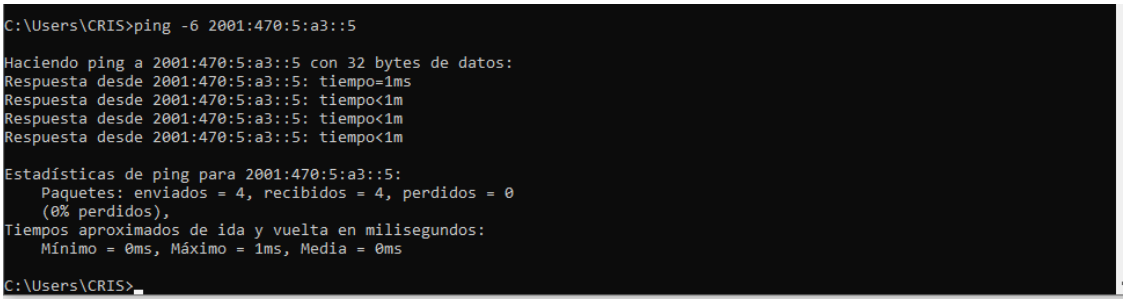


Figura 10.21 En esta imagen se realiza ping a la máquina de Bodega1 que está en el segundo piso desde la máquina de Ventas1.