UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN

TRABAJO MONOGRÁFICO

"Propuesta de un Marco de Referencia para la Transición del Protocolo IPv4 al Protocolo IPv6 mediante el método Dual Stack caso de estudio Facultad de Electrotecnia y Computación (FEC) UNI-RUSB."

PARA OPTAR AL TÍTULO DE
INGENIERO EN COMPUTACIÓN

ELABORADO POR:
Br. Heymer Manrrique Duarte Lagos.
Br. Dayton Enmanuel Martínez Ruiz.

TUTOR:
MSc. Jorge Prado Delgadillo

MANAGUA, NICARAGUA
Diciembre 2021

Dedicatoria

Primeramente, le damos gracias a Dios por prestarnos la vida para llegar al punto de concluir de forma exitosa este paso tan importante como lo es la finalización de nuestra carrera universitaria. De igual manera darle gracias a nuestros padres que han sido un pilar fundamental en nuestro camino, por todo su apoyo, por su aporte a nuestra formación profesional y personal, por todos los sacrificios que han realizado para que podamos llegar hasta donde estamos hoy en día y poder compartir un triunfo más con ellos. Finalmente, pero no menos importante; agradecemos a todos nuestros docentes que aportaron su grano de arena para cultivar en nuestra cabeza lo necesario para ser un profesional competente y una persona con altas capacidades.

Igualmente agradecemos a nuestro tutor por compartir su experiencia y tiempo al guiarnos en la realización de nuestro trabajo monográfico, también agradecemos a todas aquellas personas que a lo largo de este camino han estado firme mostrándonos su ayuda sin esperar nada cambio y confiando en nuestro éxito. Sin ustedes no estaríamos aquí hoy, este éxito es de todos nosotros.

A nuestra querida alma mater, le agradecemos por ser una institución que se preocupa por la calidad de profesionales que se gradúan de esta y por prepararnos para las siguientes etapas venideras en el mundo laboral y profesional.

Resumen

La comunicación entre redes se da gracias a la transmisión de datos a través de dispositivos que hacen de fuentes y destinos, conectados e identificados por direcciones de longitud fija determinadas gracias al Protocolo de Internet (IP, por sus siglas en inglés); en la actualidad la mayoría de redes funcionan bajo la versión 4 de este protocolo, desafortunadamente el número de direcciones IP entregadas en esta versión no fueron suficientes para cumplir con la demanda que trajo consigo el uso creciente de la tecnología en distinto ámbitos, por lo que se vio la necesidad de crear e implementar una nueva versión del Protocolo Internet que dispone de un número elevado de direcciones IP disponibles.

Debido a esto, se ve la necesidad de empezar a trabajar las redes de datos bajo la versión 6 del Protocolo de Internet, pues de esta manera la red no tendrá problemas de crecimientos ya que se podrá adquirir un gran número de direcciones por entidad, además se permitirá un óptimo rendimiento en los servicios ofrecidos y recibidos, pues se tendrá la capacidad para comunicarse con otras redes que no solo trabajen bajo IPv4, sino con IPv6 o con las dos de manera simultánea, por lo menos mientras se realiza el proceso de migración donde se debe asegurar la coexistencia de las dos versiones.

Con base a esto, el propósito de este proyecto es crear un marco de referencia para la transición del Protocolo IPv4 al Protocolo IPv6 mediante el método dual stack caso de estudio FEC-UNI-RUSB, a través de la elaboración y validación del inventario de hardware y software de la entidad, el desarrollo de un plan diagnóstico de la infraestructura de red sobre el que se trabaja para terminar un plan de trabajo que describa el paso a paso a seguir en el proceso de adopción de IPv6. Todo esto con base en la información y necesidad existente en la Facultad de Electrotecnia y Computación, entidad tomada como referencia en el desarrollo de las actividades planteadas.

El proceso correspondiente para la transición a IPv6 permite a la entidad tener una mirada general de la infraestructura de red interna y saber que tan preparada se encuentra para realizar la migración, determinando el porcentaje de hardware y

software con el nuevo protocolo, conociendo cuales son las necesidades y cambios importantes a realizar antes de empezar con el proceso y definir un previo plan de trabajo que permita organizar las actividades específicas, de esta manera se empieza con el primer paso en el proceso de la transición.

Finalmente, el documento mostrado a continuación ayudará a las entidades interesadas en el proceso de migración a IPv6, mostrando un ejemplo en la ejecución de la etapa de planificación, que servirá de guía para iniciar el proceso de transición.

Índice de contenido

Índice de Ilustraciones

Índice de tabla

1 INTRODUCCION

El protocolo de Internet (IP, por sus siglas en inglés) es un conjunto de reglas para las comunicaciones de datos digitales, su objetivo principal es la transmisión de paquetes de datos, clasificado funcionalmente en la capa de red según el modelo internacional OSI. Su función principal es el envío bidireccional de etiquetas entre el origen y destinos dentro de una red que conectan dispositivos que soportan este protocolo. Dichas etiquetas utilizadas por el protocolo IP son llamadas formalmente direcciones IP y son un conjunto de números asignados a cada dispositivo que haga parte de una red de datos; las direcciones IP no son siempre las misma para cada equipo, pueda que se asigne una diferente cada vez que un dispositivo se conecte a la red, de esta manera son llamadas direcciones IP dinámicas, por el contrario, si es necesario que la etiqueta sea siempre la misma se llamara IP fija.

Los sistemas de internet se basan en protocolos que permiten enviar información entre dispositivos y actualmente se utiliza el protocolo de internet versión 4 (de ahora en adelante IPv4), este dispone aproximadamente de 40 millones de direcciones IP, muchas de las cuales se agotaron según la Corporación de Internet para la Asignación de Nombres y Números (ICANN, por sus siglas en inglés). Por ello, alrededor de los años 90 el Grupo de Trabajo de Ingeniería de Internet (IETF, por sus siglas en inglés) desarrollo el Protocolo de Internet versión 6, o IPv6, el cual dispone de más o menos 340 sextillones de direcciones IP.

El presente trabajo se presenta una propuesta para la planeación de la transición del protocolo de Internet y entregar un punto de partida, para aquellas pequeñas empresas que deseen empezar a desarrollar el diseño para la migración de protocolos de internet, dando así un gran salto para el uso de las nuevas tecnologías que se implementan.

2 JUSTIFICACION

Se plantea a la Facultad de Electrotecnia y Computación de la Universidad Nacional de Ingeniería (UNI, Nicaragua), la necesidad de iniciar la transición de su infraestructura de servicios informáticos (equipos y aplicaciones) hacia IPv6, con el fin de ser partícipes de la nueva generación del uso del nuevo protocolo, permitiendo así seguirse consolidando y volverse un referente nacional en la aplicación de estas nuevas tecnologías, ya que dentro de sus objetivos busca mantenerse a la vanguardia de las nuevas tecnologías que contribuyan a un mejor desempeño en el manejo de la información, y así avanzar en un proceso de innovación que permita disponer de una mayor calidad en el transporte de los paquetes de datos.

La implementación de esta versión del protocolo IPv6 en entidades estatales es importante ya que hará que estén a la vanguardia en redes de datos a nivel nacional y permitiendo a su vez no quedar excluido del mundo bajo el protocolo de internet versión 4. Se busca seguir con la evolución tecnológica con la que ha ido avanzando las redes en el ámbito de los protocolos de internet más específicamente en la tendencia “The Internet of Things” (IoT), de esta manera, poder brindarle a la institución mayor calidad en los servicios, además permitirá el acceso a un mayor números de aplicaciones de internet, ya que si una red solo funciona con el protocolo IPv4 no se podrá acceder a ningún servicio que posea solamente el protocolo IPv6, lo que hará que la red se vuelva limitada para los usuarios.

Con la migración del protocolo IPv4 al protocolo IPv6 cada entidad cuenta con la posibilidad de tener un mayor número de dispositivos conectados a la red, de manera adicional el nuevo protocolo mejorara la seguridad de la red y facilitara la aparición de nuevas aplicaciones y servicios sobre la red. Finalmente, los aportes en ingeniería están basados en el rendimiento y la calidad de servicios, que en la actualidad son puntos críticos para el desarrollo en redes y solución de servicios.

3 OBJETIVOS

3.1 GENERAL.

- Proponer un marco de referencia que permita la transición del protocolo versión 4 (ipv4) al protocolo de internet versión (ipv6) mediante el método Dual Stack caso de estudio Facultad de Electrotecnia y Computación (UNI).

3.2 ESPECIFICOS.

- Identificar las tecnologías que se requieren para la transición de ipv4 a ipv6 utilizando la metodología **PDCA.**
- Analizar el despliegue de la infraestructura actual de la red de la Facultad de Electrotecnia y Computación.
- Diseñar la topología de red en el simulador cisco packet tracer para la Facultad de Electrotecnia y computación.
- Aplicar el método de transición de Dual Stack para la coexistencia de los dos protocolos internet.
- Generar documentación que sirva como una propuesta metodológica a la Universidad Nacional de Ingeniería para la transición de IPv4 a IPv6 a todas las áreas y recintos de nuestra alma mater.

4 MARCO TEORICO

En el presente marco teórico definiremos una serie de definiciones claves utilizadas para el desarrollo de nuestro trabajo monográfico estableciendo las bases necesarias para el entendimiento de cada uno de los protocolos que se pondrán en marcha en este proyecto.

4.1 Red de Datos.

Son redes de comunicación que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos. Las redes de datos se diseñan y construyen en arquitectura que pretenden servir a sus objetivos de uso. Las redes de datos, generalmente, están basadas en la comunicación de paquetes y se clasifican de acuerdo a su tamaño, la distancia que cubre y su arquitectura física. (ecured, s.f.)

La industria de la computación es relativamente joven, comparada con otras industrias, aún en el área de telecomunicaciones, como por ejemplo la telefonía. Sin embargo, la rapidez de crecimiento y el abaratamiento de costos hacen que hoy en día las computadoras están al alcance de la gran mayoría de las personas y de prácticamente todas las empresas. Junto con la proliferación de computadoras, surgió la necesidad de interconectarlas, para poder intercambiar, almacenar y procesar información. (ecured, s.f.)

4.1.1 Tipos de Topologías de Redes de Datos.

En el mundo de las redes los programadores y desarrolladores consideran en la planificación y estructuración de redes, solamente ocho tipos de topología de red y sus características. Estas son árbol o jerárquica, bus, anillo o circular, estrella, malla, y Punto a punto, veamos.

4.1.1.1 Topología de Árbol.

Este tipo de topología es vista como una colección de redes en forma de estrella, pero muy organizado. Dependiendo de su jerarquía se establece la construcción en función de los nodos periféricos individuales llamados hojas. Los nodos transmiten y reciben datos de otro nodo y no gestionan repeticiones. Muy diferente a otras topologías donde únicamente se encargan de distribuir.

Los nodos individuales se aíslan de la red a través de una falla que se causa en la ruta de conexión del propio nodo. El fallo permite aislar al nodo hoja, pero si falla el enlace completo la sección puede quedar aislada ocasionando algún tipo de corte de transmisión. (tecnoinformatic, s.f.)

Esto sucede generalmente por el exceso de tráfico, de manera que es importante desarrollar nodos centrales que ayuden a mantener un menú de información distinto a los que se conectan en la red. Se forma entonces una estructura de red que transmite paquetes de datos a todos los nodos, permitiendo usarlo como conectores.

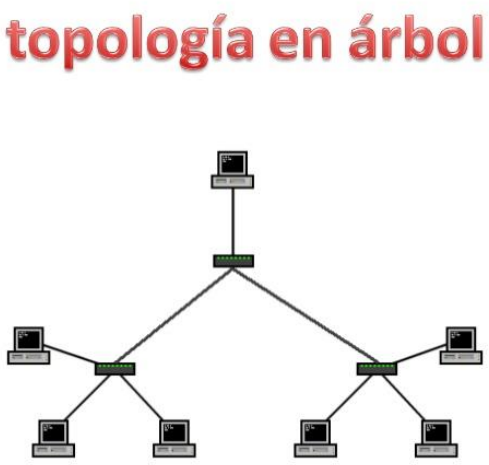

Ilustración 1. Topología árbol

4.1.1.2 Topología de Bus.

Llamado también “conducto común”, “lineal” o “line”, es una de las variantes más interesantes que existe en los tipos de topologías de red y sus características, se considera una de las más fáciles de desarrollar. La estructura consiste en un canal de comunicación PtoP que conecta a los usuarios y los asocia de manera constante entre dos puntos finales.

Funciona similar al llamado teléfono de lata que usa los niños para jugar y comunicarse. Cuando el sistema de telecomunicaciones se realiza de manera conmutada se establece un círculo permanente. En términos entendibles funciona similar a un teléfono, cuando es programado únicamente para que emita llamadas a un número determinado y de manera permanente.

Esta comunicación permanece hasta que sea necesario, se puede liberar cuando se requiera. Es como desarticular la comunicación de un sistema, después que ha realizado una labor y quedado entonces sin conexión. (tecnoinformatic, s.f.)

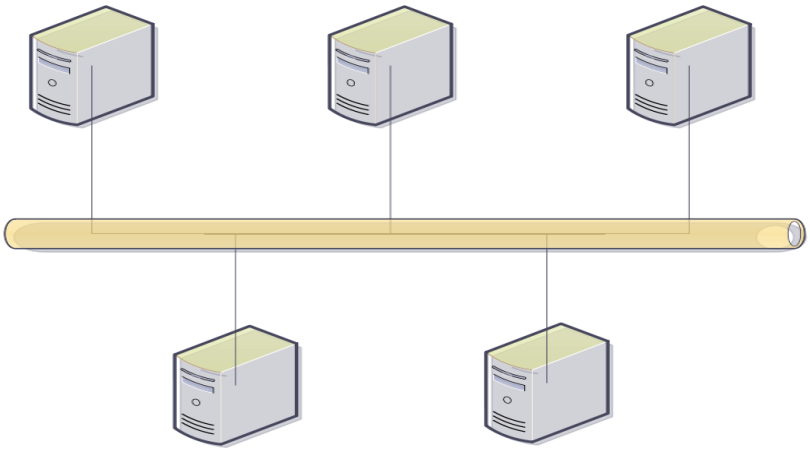

Ilustración 2. Topología de Bus

4.1.1.3 Topología de Anillo.

Es una red que permite organizar y ordenar las redes de una forma más estable. Cada nodo se conecta con otros nodos formando una única transmisión y comunicación. Entonces se forma también una ruta única entre los nodos permitiendo manejar paquetes de datos individuales.

La topología de anillo puede ser unidireccional a pesar que exista el tráfico en ambos sentidos o girando en forma circular, creando una especie de anillo. También se puede estructurar de forma bidireccional, donde el anillo permite proporcionar una sola ruta entre dos nodos.

Estas rutas de transmisión pueden ser interrumpidas en ocasiones si algunos de los nodos presentan un problema. Entre las ventajas se encuentra que cada dispositivo tiene acceso al token, teniendo la oportunidad de transmitir sin inconvenientes. (tecnoinformatic, s.f.)

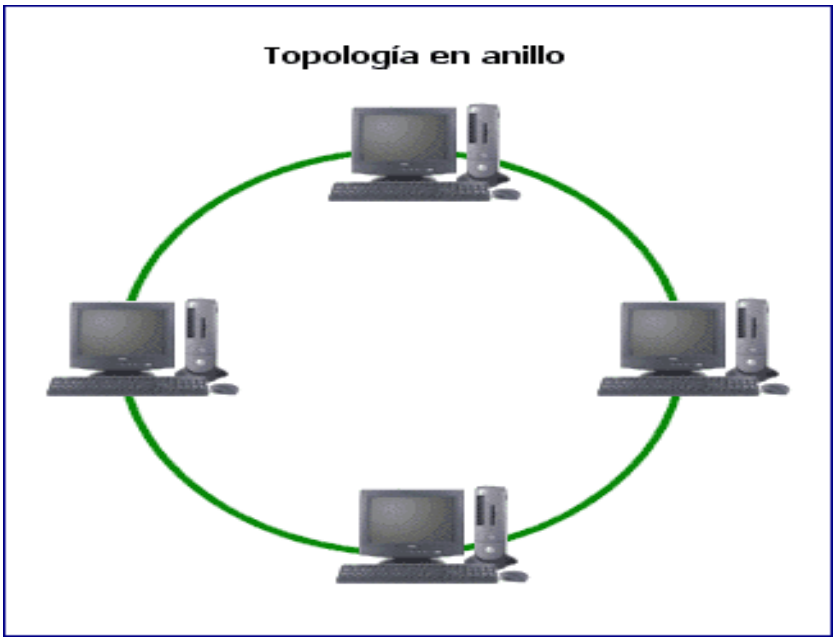

Ilustración 3. Topología de Anillo

4.1.1.4 Topología de Estrella.

Los tipos de topologías y sus características permiten ofrecen una variedad de configuraciones fundamentadas en las necesidades del usuario o empresa. En este caso la topología en estrella o star como también se le llama, limita la posibilidad de que una red colapse. Esto se hace conectando todos los nodos a un nodo central.

Este nodo central envía las transmisiones que recibe a cualquier nodo periférico y a todos los nodos que se encuentren en la red. Los nodos periféricos se comunican con los otros, transmitiendo únicamente desde el nodo central. Si existiera una falla en la línea de conexión de algún nodo, el nodo central solamente provocaría su propio aislamiento

El único problema es que el nodo central se recarga soportando una cantidad de tráfico considerable. Por eso este tipo de topología estructural de redes es recomendada en sistemas pequeños y no en sistemas de transmisión que generan cantidades de tráfico y mucho volumen en el envío y recibo de datos. (tecnoinformatic, s.f.)

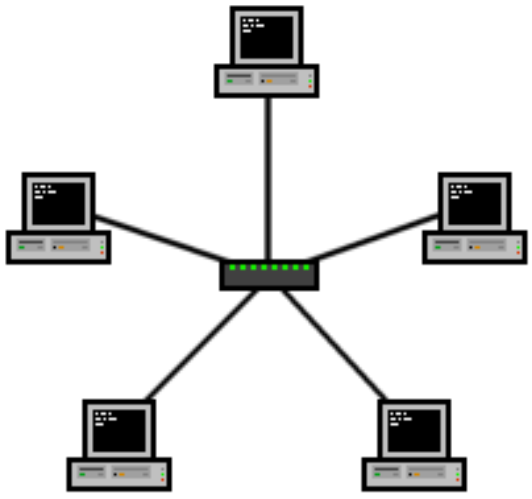

Ilustración 4. Topología de Estrella

4.1.1.5 Topología de Malla.

Esta topología de red es una forma de conexión similar a la anterior donde cada nodo está conectado a todos los nodos. Permite llevar los mensajes de un nodo a otro por diversos canales. Cuando la red malla está totalmente conectada, no se produce ninguna interrupción en la comunicación. También permite a cada servidor establecer sus propias conexiones con el resto de los servidores.

La ventaja en este tipo de topología de red y sus características es, que no se estructura a atreves de un nodo central, esto crea un pronóstico en el cual las fallas son limitadas. Permitiendo realizar mantenimiento en periodos más largos. Otra ventaja es que si llega a desaparecer la conexión no afecta a los nodos de redes.

La red malla resulta muy confiable, disminuye la redundancia y la confianza es tolerante para fallos superiores. Una de las desventajas de este tipo de topología de red, es que son un poco costosas para su instalación. Requieren interconexión de cada uno de los nodos con el resto de los nodos.

Esto permite aumentar las interfaces mayores a las que deben disponer cada uno. Por eso es importante estructurar la topología en función de la conexión tipo cable o inalámbrica. La redundancia de las rutas hacia un mismo destino disminuye la frecuencia de ocurrencia de fallos. (tecnoinformatic, s.f.)

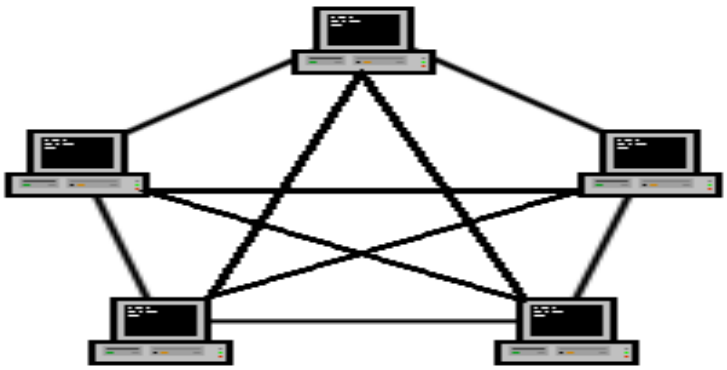

Ilustración 5. Topología de Malla

4.1.1.6 Topología Punto a Punto.

Llamada también “Point to Point Protocol” o “Peer-to-Peer”, representa los tipos de topologías de red y sus características, que utilizan redes de largo alcance (WAN), los algoritmos de encadenamiento son un tanto complicados. Lo errores se corrigen en los nodos intermedios y en los extremos.

Las redes punto a punto son aquellas que responden a un tipo de arquitectura de red en las que cada canal de datos se usa para comunicar únicamente dos computadoras, en clara oposición a las redes multipunto, en las cuales cada canal de datos se puede usar para comunicarse con diversos nodos.

Los dispositivos de red actúan de manera similar y de pares entre sí. Cada dispositivo toma el rol de emisor o de receptor. La complejidad de este sistema le permite establecer independencia en una petición de mensaje. Los roles suelen invertirse y el receptor se convierte en emisor.

Las estaciones reciben únicamente los mensajes emitidos por los nodos de la red. Identifican a la estación receptora según la dirección emisora. Las conexiones entre los nodos se realizan con uno o varios sistemas de transmisión. Estos pueden enviarlas a diferentes velocidades, permitiendo trabajar de forma paralela. Los nodos intermedios pueden generar tráfico según el tipo de mensaje que envían.

Los retardos se deben al tránsito de los mensajes a través de los nodos intermedios. El costo de instalación depende de la cantidad de cables que se necesiten para la conexión principal y el número de enlaces entre las conexiones. (tecnoinformatic, s.f.)

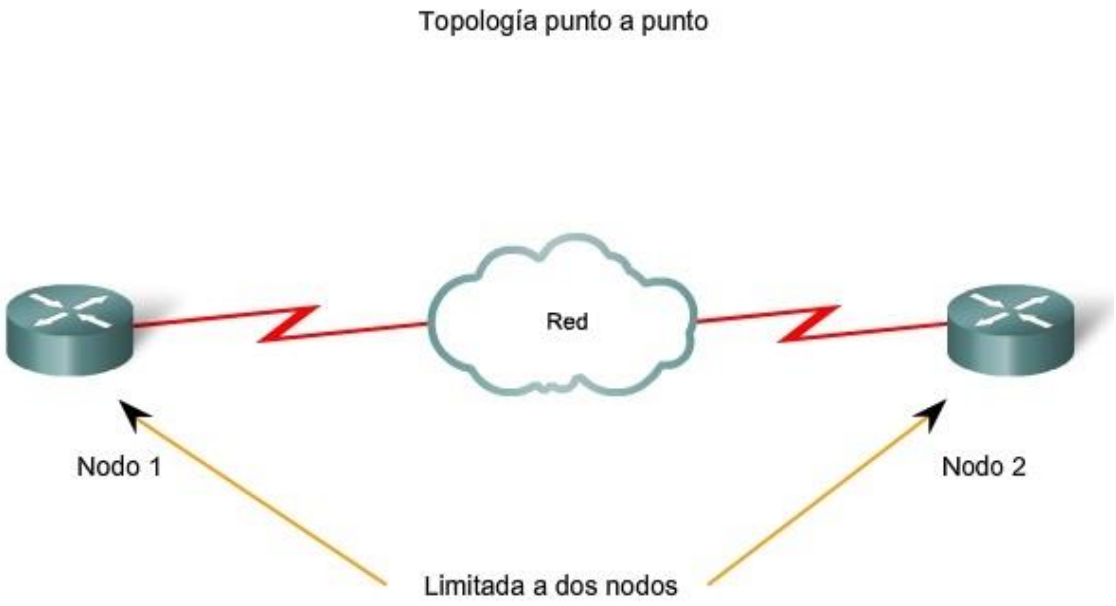

Ilustración 6. Topología Punto a Punto

4.2 Protocolo de Internet.

El protocolo de Internet, conocido por sus siglas en inglés IP, es el protocolo principal de la familia de protocolos de Internet y su importancia es fundamental para el intercambio de mensajes en redes informáticas. El protocolo no orientado a la conexión, publicado en 1974 por el Instituto de Ingeniería Eléctrica y Electrónica (IEEE) y especificado como estándar en RFC 791, fue concebido principalmente para garantizar el éxito en el envío de paquetes de un emisor a un destinatario. Para este fin, el protocolo de Internet establece un formato que determina el tipo de descripción que tienen estos paquetes de datos (también llamados datagramas IP). (ionos.es, s.f.)

4.2.1 Protocolo de internet versión 4 o IPv4.

IP significa protocolo de internet que se utiliza para entregar datagramas entre host en una red. Típicamente, es un método por el cual los datos serán enviados de un dispositivo de computadora a otro dispositivo de computadora a través de internet. IPv4 es la cuarta versión del protocolo de internet que fue adaptado y ahora se utiliza ampliamente en la comunicación de datos a través de diferentes tipos de redes. Se considera como uno de los protocolos básicos de los métodos de trabajo en red basados en estándares en internet y fue la primera versión que se implementó para la producción durante la época de ARPANET. IP significa un protocolo que se basa en redes de capas con conmutación de paquetes, al igual que Ethernet. Proporciona una conexión lógica entre diferentes dispositivos de red al proporcionar identificación para cada dispositivo. (speedcheck, s.f.)

IPv4 utiliza un esquema de direcciones de 32 bits que permite un total de 2 a la potencia de 32 direcciones o un poco más de 4 mil millones de direcciones. Esto se basa en el modelo del mejor esfuerzo. El modelo se asegura de que se evite la entrega por duplicado. Todos estos aspectos son manejados por la capa superior de transporte. Esta versión de IP se utiliza como base internet, y se establece todas las reglas y regulaciones para las redes informáticas que funcionan bajo el principio de intercambio de paquetes. La responsabilidad de este protocolo es establecer conexiones entre dispositivos informáticos, servidores y dispositivos móviles basados en direcciones IP. En el intercambio de información en IPv4, se lleva a cabo por los paquetes IP se dividen en dos grandes campos, el encabezado y el campo de datos. El campo se utiliza para transportar información importante, mientras que un encabezado contiene todas las funciones del protocolo. (speedcheck, s.f.)

Protocolo de Internet es uno de los principales protocolos en el conjunto de protocolos TCP/IP. Este protocolo funciona en la capa de red del modelo OSI y en la capa de Internet del modelo TCP/IP. Por lo tanto, este protocolo tiene la responsabilidad de identificar hosts basados en sus direcciones lógicas y para dirigir los datos entre ellos a través de la red subyacente.

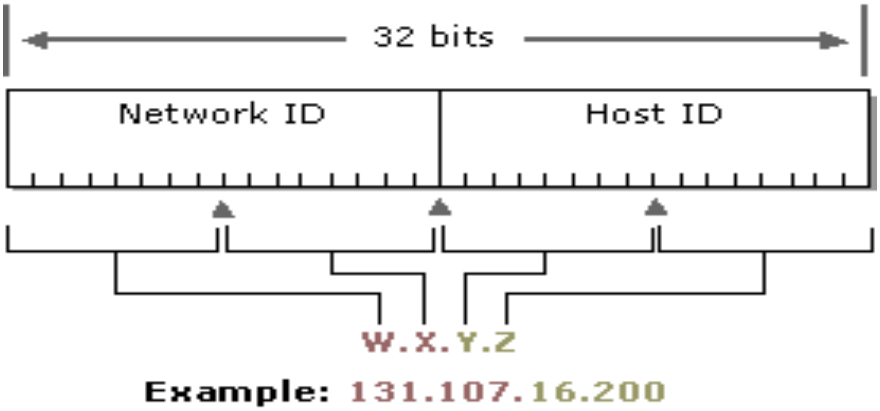

Ilustración 7. Ejemplo de cómo esta estructura una dirección IP

4.2.2 Direcciones IP.

Una dirección IP es un identificador o número único que se le asigna a un equipo o dispositivo electrónico cuando utiliza el protocolo IP. “Dirección IP” proviene de “Internet Protocol”, traducido al español “Protocolo de Internet”; de esta forma, “Dirección IP” significa “**Dirección del Protocolo de Internet**”. (aleashop, s.f.)

4.2.3 Clases de direcciones IPv4.

Las direcciones se organizan en **clases A, B y C** que son diferentes rangos de IP. Se utilizan las direcciones IP de una clase u otra en función del tamaño de la red en la que se vayan a usar:

4.2.3.1 Clase A: direcciones IP que van de la 0.0.0.0 a la 127.255.255.255.

4.2.3.2 Clase B: direcciones IP que van de la 128.0.0.0 a la 191.255.255.255.

4.2.3.3 Clase C: direcciones IP que van de la 192.0.0.0 a la 223.255.255.255.

4.2.4 Tipos de direcciones IPv4.

Sin la dirección IP (Internet Protocol) sería imposible navegar por Internet, puesto que este número único, que se asigna a cada dispositivo que se conecta a la Red, es imprescindible para que puedan comunicarse entre ellos (es cómo nuestra dirección postal para recibir cartas físicas). Además, existen dos tipos de direcciones IP: la IP privada y la IP Pública**.**

4.2.4.1 Direcciones IPv4 Públicas.

Las direcciones IPv4 públicas constituyen el espacio de direcciones de Internet. Estas son distribuidas para ser globalmente únicas. El principal propósito de este espacio de direcciones es permitir la comunicación usando IPv4 sobre Internet. (lacnic.net, s.f.)

Las direcciones IPv4 públicas son direcciones que se enrutan globalmente entre los enrutadores de los ISP (proveedores de servicios de Internet). Sin embargo, no todas las direcciones IPv4 disponibles pueden usarse en Internet.

Las direcciones públicas son indispensables para conectarse a internet, y resultan visibles para cualquier internauta; suele ser la que se asigna al router o al módem.

4.2.4.1.1 Clases de direcciones IPv4 Publicas.

- **Clase A:** 1.0.0.0 a 126.255.255.255
- **Clase B:** 128.0.0.0 a 191.255.255.255
- **Clase C:** 192.0.0.0 a 223.255.255.255

4.2.4.2 Direcciones IPv4 Privadas.

Algunos rangos de direcciones IPv4 han sido reservados para la operación de redes privadas. Cualquier organización puede usar estas direcciones IPv4 en sus redes privadas sin la necesidad de solicitarlo a algún Registro de Internet. La principal condición establecida para el uso de direcciones IPv4 privadas es que los dispositivos que usen estas direcciones IPv4 no necesiten ser alcanzados desde Internet. (lacnic.net, s.f.)

En Internet, una red privada es una red de computadoras que usa el espacio de direcciones IP especificadas en el documento RFC 1918. A los equipos o terminales puede asignárseles direcciones de este espacio cuando deban comunicarse con otros terminales dentro de la red interna/privada (una que no sea parte de Internet/red pública) pero no con Internet directamente. (wikipedia, s.f.)

Las direcciones privadas solo son visibles desde una red interna, pero no desde internet. Se utilizan generalmente para identificar los puestos de trabajo de las empresas. Se pueden utilizar tantas como se necesiten; no es necesario contratarlas. (aleashop, s.f.)

4.2.4.2.1 Clases de direcciones IPv4 Privadas.

Existen ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas.

- Las direcciones IP privadas de clase A: **10.0.0.1 a 10.255.255.254** hacen posible la creación de grandes redes privadas que incluyen miles de equipos.

- IP privadas de clase B: **172.16.0.1 a 172.31.255.254** permiten la creación de redes privadas de tamaño medio.

- Las IP privadas de clase C: **192.168.0.1 a 192.168.0.254** posibilitan establecer pequeñas redes privadas.

4.2.5 Protocolo de internet versión 6 o IPv6.

IPv6 es la versión más reciente del protocolo de internet (IP), el protocolo de comunicaciones que proporciona un sistema de identificación y ubicación para las computadoras en las redes y enruta el tráfico a través de internet. IPv6 fue desarrollado por el Grupo de Trabajo de Ingeniería de Internet (IETF) para hacer frente al problema largamente anticipado del agotamiento de la dirección IPv4. IPv6 está destinado a reemplazar IPv4. (en.wikipedia.org, s.f.)

4.2.5.1 Direcciones IPv6

Una dirección IPv6 tiene un tamaño de 128 bits y se compone de ocho campos de 16 bits, cada uno de ellos unidos por dos puntos. Cada campo debe contener un número hexadecimal, a diferencia de la notación decimal con puntos de las direcciones IPv4. En la figura siguiente las X representan números hexadecimales. (https://docs.oracle.com/, s.f.)

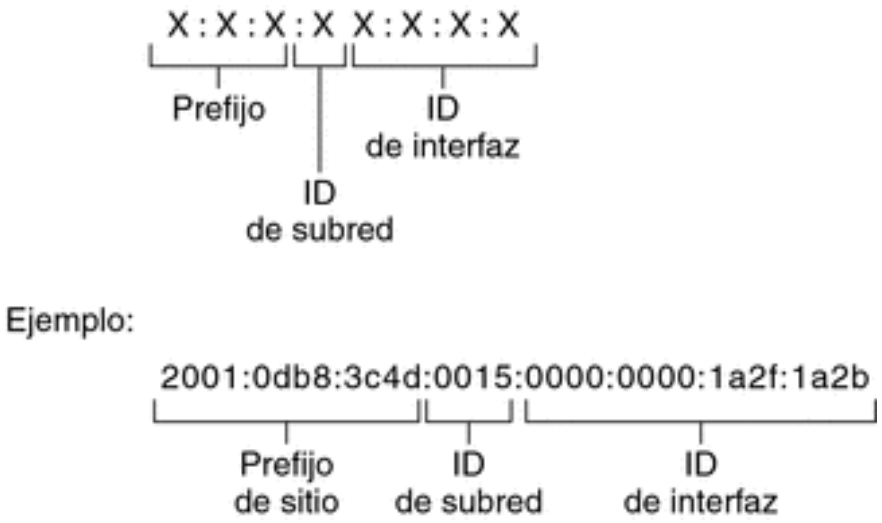

Ilustración 8. Formato de dirección IPv6

4.2.5.2 Clases de Direcciones IPv6.

IPv6 reconoce tres tipos de direcciones: unicast, multicast y anycast. El tipo de dirección define el destino de la comunicación, es decir, a cuántos receptores debe ser entregado el paquete.

4.2.5.3 Dirección IPv6 de Unidifusión.

una dirección de unidifusión IPv6 identifica de forma exclusiva una interfaz en un dispositivo habilitado para IPv6. Un paquete que se envía a una dirección unidifusión es recibido por la interfaz que tiene asignada esa dirección. Como sucede como IPv4, las direcciones IPv6 de origen deben ser dirección unicast.

Los tipos de direcciones IPv6 de unidifusión más comunes son las direcciones de unidifusión globales (GUA) y las direcciones de unidifusión link-local.

4.2.5.4 Dirección IPv6 de Unidifusión Global.

Las direcciones de unidifusión globales son similares a las direcciones IPv4 públicas. Estas son direcciones enrutables de Internet globalmente exclusivas. Las direcciones de unidifusión globales pueden configurarse estáticamente o asignarse de forma dinámica.

4.2.5.5 Dirección IPv6 Unidifusión Link-local.

Las direcciones link-local se utilizan para comunicarse con otros dispositivos en el mismo enlace local. Con IPv6, el término “enlace” hace referencia a una subred. Las direcciones link-local se limitan a un único enlace. Su exclusividad se debe confirmar solo para ese enlace, ya que no se pueden enrutar más allá del enlace. En otras palabras, los enrutadores no reenvían paquetes con una dirección de origen o de destino link-local.

4.2.5.6 Dirección IPv6 de Multidifusión.

Identifican varias interfaces. Cuando un paquete está dirigido a una dirección de multidifusión se entrega en todos los interfaces del grupo identificado con esa dirección. Las direcciones de multidifusión no se pueden utilizar como direcciones de origen.

4.2.5.7 Dirección IPv6 de Difusión por Proximidad.

Identifican a un conjunto de interfaces, normalmente de nodos diferentes. Un paquete enviado a una dirección de difusión por proximidad se entrega únicamente a una de las interfaces identificadas con esa dirección. Esta interfaz coincide con la de menor coste según la definición de métrica de encaminamiento. Este hecho permite equilibrar la carga entre distintos nodos. Las direcciones de difusión por proximidad sólo se utilizan como direcciones de destino y sólo se asignan a encaminadores.

4.3 VLAN

En la actualidad, una red física local o LAN (Local Area Network), está compuesta principalmente por computadoras y equipos de enlace (fundamentalmente switches y routers), capaces de establecer la comunicación entre los dispositivos.

En ocasiones, es necesaria la división o segmentación de la red local para facilitar su administración, y en este sentido, lo deseable es no tener que realizar grandes cambios en la infraestructura física de la red.

Una VLAN, acrónimo de virtual LAN o Red de Área Local Virtual, es una tecnología para crear redes lógicas independientes dentro de una misma red física. Son útiles para reducir el dominio de difusión de la información, y ayudan en la administración de la red, separando segmentos lógicos (las oficinas o departamentos de una organización, por ejemplo) que deberían estar relacionados solo entre ellos. Una VLAN está formada por dos o más dispositivos, que se comportan como si

estuviesen conectados al mismo conmutador, aunque se encuentren físicamente enlazados a diferentes switches de la misma red de área local.

Cada VLAN individual recibe su propio dominio de difusión (broadcast), de manera que, si un dispositivo envía una difusión dentro de la VLAN, todos los demás participantes de ese segmento (y solo esos) reciben el mensaje. La difusión no se transmite más allá de los límites de la red virtual. (infotecs, s.f.)

4.4 DHCP

DHCP significa Protocolo de configuración de host dinámico. Es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma dinámica (es decir, sin intervención particular). Sólo tiene que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red.

El protocolo DHCP sirve principalmente para distribuir direcciones IP en una red, pero desde sus inicios se diseñó como un complemento del protocolo BOOTP (Protocolo Bootstrap), que se utiliza, por ejemplo, cuando se instala un equipo a través de una red (BOOTP se usa junto con un servidor TFTP donde el cliente encontrará los archivos que se cargarán y copiarán en el disco duro). Un servidor DHCP puede devolver parámetros BOOTP o la configuración específica a un determinado host. (sites.google, sites.google, s.f.)

4.5 VTP

VTP son las siglas de VLAN Trunking Protocol, un protocolo de mensajes de nivel 2 usado para configurar y administrar VLANs en equipos Cisco. Permite centralizar y simplificar la administración en un domino de VLANs, pudiendo crear, borrar y renombrar las mismas, reduciendo así la necesidad de configurar la misma VLAN en todos los nodos. El protocolo VTP nace como una herramienta de administración para redes de cierto tamaño, donde la gestión manual se vuelve inabordable.

VTP opera en 3 modos distintos:

4.5.1 Servidor

Es el modo por defecto. Desde él se pueden crear, eliminar o modificar VLANs. Su cometido es anunciar su configuración al resto de switches del mismo dominio VTP y sincronizar dicha configuración con la de otros servidores, basándose en los mensajes VTP recibidos a través de sus enlaces trunk. Debe haber al menos un servidor. Se recomienda autenticación MD5.

4.5.2 Cliente

En este modo no se pueden crear, eliminar o modificar VLANs, tan sólo sincronizar esta información basándose en los mensajes VTP recibidos de servidores en el propio dominio. Un cliente VTP sólo guarda la información de la VLAN para el dominio completo mientras el switch está activado. Un reinicio del switch borra la información de la VLAN.

4.5.3 Transparente

Desde este modo tampoco se pueden crear, eliminar o modificar VLANs que afecten a los demás switches. La información VLAN en los switches que trabajen en este modo sólo se puede modificar localmente. Su nombre se debe a que no procesa las actualizaciones VTP recibidas, tan sólo las reenvía a los switches del mismo dominio. (sites.google, sites.google, s.f.)

4.6 DNS

DNS son las iniciales de Domain Name System (sistema de nombres de dominio) y es una tecnología basada en una base de datos que sirve para resolver nombres en las redes, es decir, para conocer la dirección IP de la máquina donde está alojado el dominio al que queremos acceder.

Cuando un ordenador está conectado a una red (ya sea Internet o una red casera) tiene asignada una dirección IP. Si estamos en una red con pocos ordenadores, es

fácil tener memorizadas las direcciones IP de cada uno de los ordenadores y así acceder a ellos, pero ¿qué ocurre si hay miles de millones de dispositivos y cada uno tiene una IP diferente? Pues que se haría imposible, por eso existen los dominios y las DNS para traducirlos.

Por lo tanto, el DNS es un sistema que sirve para traducir los nombres en la red, y está compuesto por tres partes con funciones bien diferenciadas.

Cliente DNS: está instalado en el cliente (es decir, nosotros) y realiza peticiones de resolución de nombres a los servidores DNS.

Servidor DNS: son los que contestan las peticiones y resuelven los nombres mediante un sistema estructurado en árbol. Las direcciones DNS que ponemos en la configuración de la conexión, son las direcciones de los Servidores DNS.

Zonas de autoridad: son servidores o grupos de ellos que tienen asignados resolver un conjunto de dominios determinado (como ejemplo los .ni o los .org).

4.7 Servidor Web

Un servidor web es un software que forma parte del servidor y tiene como misión principal devolver información (páginas) cuando recibe peticiones por parte de los usuarios.En otras palabras, es el software que permite que los usuarios que quieren ver una página web en su navegador puedan hacerlo.

Para el funcionamiento correcto de un servidor web necesitamos un cliente web que realice una petición http o https a través de un navegador como Chrome, Firefox o Safari y un servidor donde esté almacenada la información.

El proceso sería el siguiente:

Tras la primera consulta por parte del usuario hacia una web, se establece una conexión entre el servidor DNS y el ordenador que realiza la consulta o petición. Este servidor DNS responde con la dirección IP correcta del servidor web donde está alojado el contenido solicitado.

El siguiente paso sería solicitar el contenido al servidor web mediante el protocolo HTTP/HTTPS.

Una vez que el servidor web ha recibido la solicitud del contenido solicitado por el cliente web, deberá procesar la solicitud hasta encontrar el contenido solicitado dentro del dominio correspondiente.

Envía el contenido solicitado al cliente web que lo solicitó. (webempresa, s.f.)

4.8 Protocolo Dot1q

El protocolo IEEE 802.1Q, también conocido como dot1Q, fue un proyecto del grupo de trabajo 802 de la IEEE para desarrollar un mecanismo que permita a múltiples redes compartir de forma transparente el mismo medio físico, sin problemas de interferencia entre ellas (Trunking) o enlace troncal. Es también el nombre actual del estándar establecido en este proyecto y se usa para definir el protocolo de encapsulamiento usado para implementar este mecanismo en redes Ethernet. Todos los dispositivos de interconexión que soportan VLAN deben seguir la norma IEEE 802.1Q que especifica con detalle el funcionamiento y administración de redes virtuales.

4.8.1 Formato de la Trama

802.1Q en realidad no encapsula la trama original, sino que añade 4 bytes al encabezado Ethernet original. El valor del campo EtherType se cambia a 0x8100 para señalar el cambio en el formato de la trama.

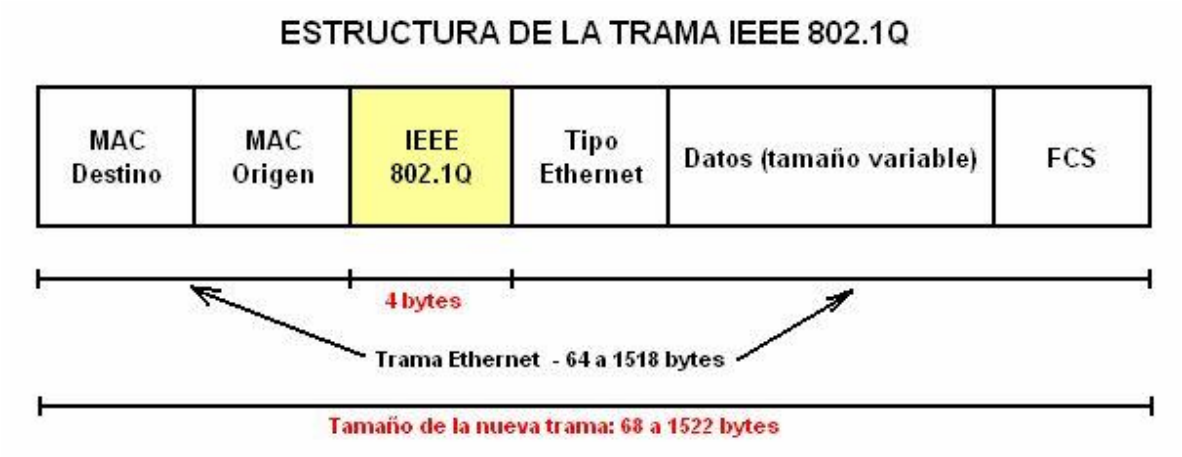

Ilustración 9. Estructura de la trama protocolo Dot1q

4.8.2 Tipos de puerto en los switches

Existen dos tipos de puertos:

Puertos de acceso: Se conectan las estaciones directamente. Mapean el puerto a una VLAN programada. Cuando entra una trama Ethernet se le añade el TAG de 802.1Q. Cuando sale una trama 802.1Q se le quita el TAG, para que llegue a la estación correspondiente con el formato IEEE 802.3 original.

Puertos 1Q Trunk: Se utilizan para conectar Switches entre si y que pase el tráfico de diferentes VLANs a través de ellos. Las tramas que le llegan y que salen llevan el Tag 802.1Q. (cdrbenitest.blogspot, s.f.)

4.9 Mecanismo de Transición.

Los mecanismos de transición a IPv6 son las tecnologías que facilitan y facilitarán la transición de Internet de su infraestructura IPv4 al sistema de direccionamiento de nueva generación IPv6.

4.9.1 Mecanismo de Transición por Túneles.

Los túneles proporcionan un mecanismo que permite establecer conexiones IPv6 sobre una red IPv4 (y viceversa). Los túneles se utilizan cuando un equipo desea acceso a la red IPv6 existente. Para ello el equipo deberá crear un túnel a través de IPv4 con un router que tenga tanto acceso a IPv6 como IPv4. Este método se está utilizando en la actualidad por parte de algunos ISPs que sólo dan conexión IPv4 para que cualquiera pueda tener acceso a la red IPv6. (sites.google.com, s.f.)

También permiten unir redes IPv6 utilizando la infraestructura IPv4 existente. Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4 (y viceversa). Los extremos finales del túnel siempre son los responsables de realizar la operación de encapsulado y desencapsulado del paquete IPv6 en IPv4. (sites.google.com, s.f.)

El tunneling es una técnica de integración y transición intermedia, y no debe considerarse como una solución definitiva. El objetivo final debe ser una arquitectura IPv6 nativa. (sites.google.com, s.f.)

4.9.2 Mecanismo de Transición Dual Stack.

El método Dual Stack permite hacer coexistir ambas tecnologías de red sobre un mismo enlace, particularmente útil para implementar con toda tranquilidad IPv6 en una red local sin alterar en principio el funcionamiento de IPv4. (ediciones-eni, s.f.)

Al diseñar IPv6, sus creadores contemplaron que el mismo debería convivir con IPv4 durante un período indeterminado. Por esta causa, a los dispositivos con soporte IPv6 es posible añadirles el nuevo direccionamiento junto al de IPv4. Esta posibilidad se conoce cómo doble pila (Dual Stack en inglés). De esta forma, al iniciar una conexión TCP/IP el equipo terminal elegirá cual direccionamiento utilizar en función de la disponibilidad y desempeño de cada protocolo por parte del equipo o servicio remoto que se requiera alcanzar y la red de tránsito. (nic.cr, s.f.)

IPv6 nativo en Doble pila es el método de transición recomendado. Las principales ventajas sobre los otros mecanismos son que IPv4 continúa operando con

normalidad mientras se introduce IPv6 a la red, y en esencia, la implementación de IPv6 será definitiva, que no requerirá retirarse posteriormente. (nic.cr, s.f.)

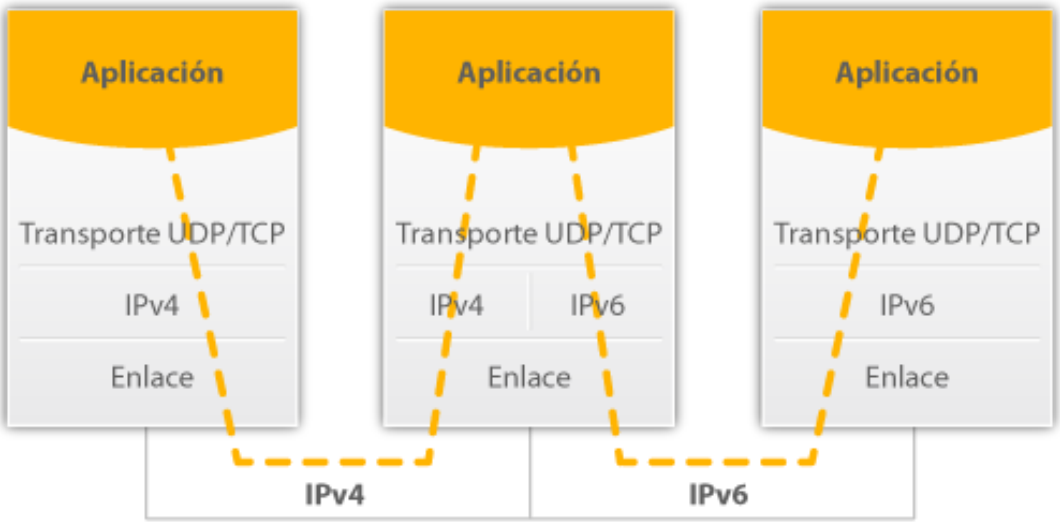

Ilustración 10. Método Dual Stack

4.10 Packet Tracer.

Packet Tracer es una herramienta de simulación visual multiplataforma diseñada por Cisco System que permite a los usuarios crear topologías e imitar redes informáticas modernas. El software permite a los usuarios simular la configuración de enrutadores y conmutadores Cisco mediante una interfaz de líneas de comando simulada. (en.wikipedia.org, s.f.)

Cisco Packet Tracer es un poderoso programa de simulación de red que permite a los estudiantes experimentar con el comportamiento de la red y hacer preguntas de “qué pasaría si”. Como parte integral de Networking Academy, Packet Tracer proporciona capacidades de simulación, visualización, autoría, evaluación y colaboración y facilita la enseñanza y el aprendizaje de conceptos tecnológicos complejos. (ecured, s.f.)

Packet Tracer complementa el equipo físico en el aula al permitir a los estudiantes crear una red con una cantidad casi limitada de dispositivos, fomentando la práctica,

el descubrimiento y la resolución de problemas. El entorno de aprendizaje basado en la simulación ayuda a los estudiantes a desarrollar habilidades del sigo XXI, como la toma de decisiones, el pensamiento creativo y crítico y la resolución de problemas. (ecured, s.f.)

En este programa se crea la topología física de la red simplemente arrastrando los dispositivos a la pantalla. Luego clickando en ellos se puede ingresar a sus consolas de configuración. Allí están soportados todos los comandos del Cisco OS e incluso funciona el “tab completion”. Una vez completada la configuración física y lógica de la red, también se puede hacer simulaciones de conectividad (pings, tracerouters, etc) todo ello desde la misma consola incluida. (ecured, s.f.)

4.11 Metodología PDCA

La metodología PDCA es una herramienta también conocida como ciclo de mejora de Deming, la cual se usa normalmente en procesos de mejora continua. Habitualmente se representa en forma de rueda para mostrar su componente cíclico, ya que es una metodología que podemos usar una y otra vez para mejorar de forma progresiva.

5 Diseño Metodológico.

Se definió como metodología el ciclo **PDCA** el cual está compuesto por cuatro fases que son: **Planear**, **Hacer**, **Verificar** y **Actuar**. Es representada mediante una forma cíclica lo cual asegura la mejora progresiva del proceso al cual es aplicada.

Esta metodología es seleccionada debido a todas las bondades que ofrece, y a su adaptabilidad en cualquier ambiente; nos brinda la flexibilidad necesaria para cumplir con todos los requerimientos para el éxito de la transición de protocolo de internet versión 4 al protocolo de internet versión 6. Adicionalmente, su componente cíclico nos brinda el resultado más óptimo para cada fase, lo que asegura un resultado satisfactorio para las expectativas del presente trabajo.

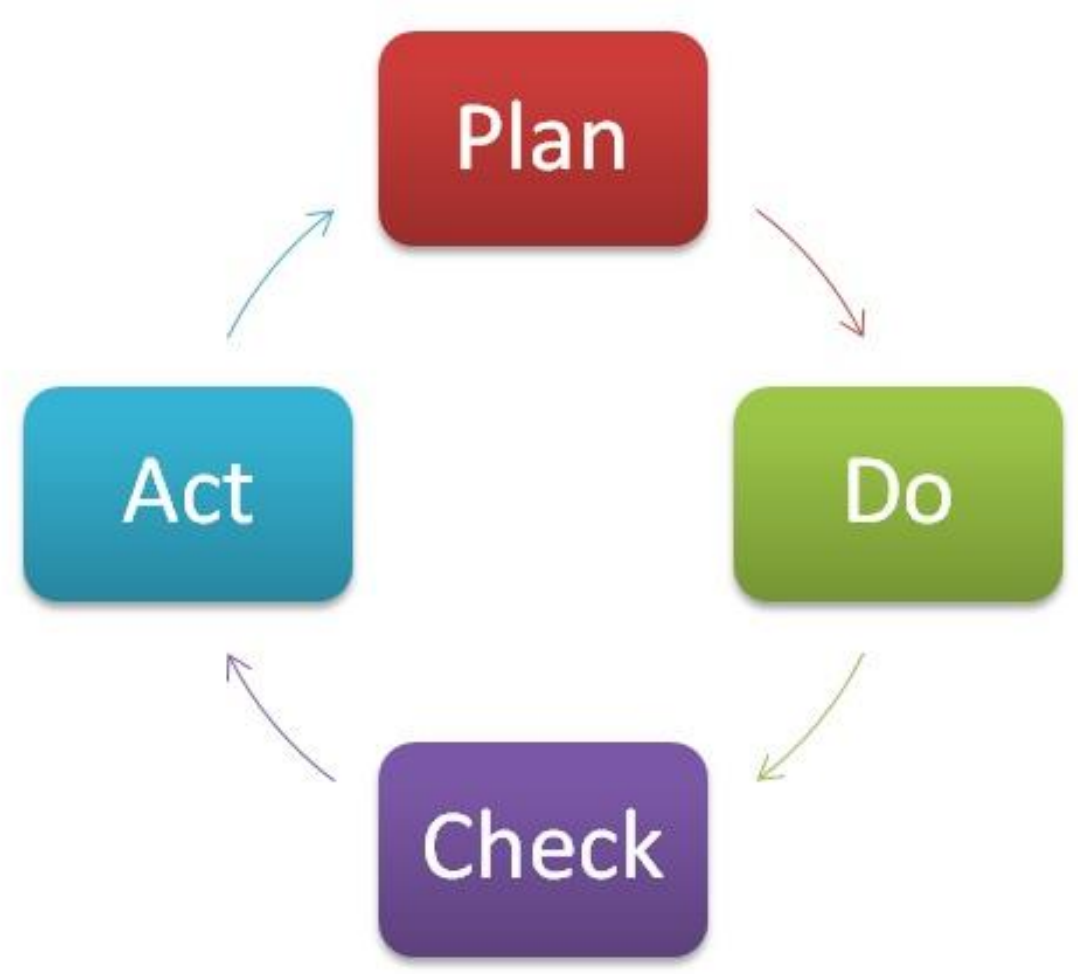

Ilustración 11. Metodología PDCA

5.1 Fase de Análisis.

En esta fase nos enfocaremos en cumplir los objetivos específicos 1 y 2 del presente trabajo.

Esto lo lograremos utilizando diversas técnicas de recolección de información, la cual será procesada y mostrada de una forma fácil de comprender con el objetivo de enterarnos del estado actual del área de interés para este trabajo; como lo es la Facultad de Electrotecnia y Computación de la Universidad Nacional de Ingeniería.

Es de vital importancia tener presentes los puntos clave de la problemática y así poder plantear soluciones viables para estos inconvenientes, de esta forma, podremos evitar malos funcionamientos o detener las labores diarias de esta facultad cuando se esté realizando el proceso de migración.

5.1.1 Determinar el problema.

Actualmente todos los recintos de la Universidad Nacional de Ingeniería trabajan bajo el protocolo ipv4 lo que limita la cantidad de equipos conectados en sus redes, así también, restringe las posibles de conexiones con entidades que trabajen bajo el protocolo ipv6. El número de entidades que se unen al uso de este protocolo aumenta día con día debido a las bondades que este presta.

Esto horilla a nuestra alma mater la cual es un referente nacional en ciencias y tecnología a dar el salto hacia el futuro en el uso del protocolo IPv6 para poder integrarse con empresas y organizaciones que ya adoptaron por él cambio hacia IPv6.

5.1.2 Recolección De Datos.

Consideramos la recolección de datos el primer paso para poder completar el trabajo propuesto en el presente documento.

Siendo la recolección de datos una parte fundamental en la implantación de cualquier proceso o nueva funcionalidad en una organización debemos conocer las

particularidades de cómo funciona la topología actual, que elementos utiliza para funcionar, cómo están organizados y si estos cumplen con los requisitos para funcionar en la nueva topología deseada.

5.1.2.1 Inventarios de activos Informáticos de la Facultad de Electrotecnia y Computación.

Mediante un proceso de inventariado se determina el estado físico actual de los dispositivos conectados a la red de la Facultad de Electrotecnia y Computación.

En este inventario nos enfocamos a todos los equipos que se conecten a la red como lo son: equipos de cómputo, switches, servidores. Es de suma importancia saber si estos equipos soportan o no un ambiente ipv6. También se debe obtener el sistema operativo instalado en cada dispositivo final y si este tiene compatibilidad con ipv6.

Esta información asegura que las funciones de las áreas migradas no se verán interrumpidas por causa de nuestro trabajo.

5.1.2.2 Entrevista con el personal técnico de la dirección nic.ni

Gracias a que el nic.ni es uno de los interesados en realizar esta migración, y debido a la sensibilidad de la información manejada por esta dirección de la Universidad Nacional de Ingeniería parte de la información requerida se nos fue entregada vía entrevista y a criterio del nic.ni. no se nos brinda información de ubicación, sistema operativo ni modelo de los servidores, switches de distribución ni del enrutador.

Solo se nos asegura que estos cumplen los requisitos solicitados para nuestro proyecto. La información que se nos brinda de esta entrevista, la detallamos a continuación:

5.1.2.3 Dispositivos intermediarios.

En la presente tabla se muestra los modelos de los dispositivos intermediarios utilizados en la Facultad de Electrotecnia y Computación.

No	Equipo	Marca	Modelo	Ubicación	Versión IP	Soporta IPv6
1	Switch	Cisco	WS-C2960+24TC-L	FEC-ASA	4	SI
2	Switch	Cisco	WS-C2960+24TC-L	SEC-FEC	4	SI
3	Switch	Cisco	WS-C2960-24TC-S	SAREC-1	4	NO
4	Switch	Cisco	WS-CE500-24TT	SAREC-2	4	NO
5	Switch	Cisco	WS-C2960-24TT-L	Dpto-Eo	4	NO
6	Switch	Cisco	WS-C2960-48TC-S	Laboratorio Leyda Montenegro	4	NO
7	Switch	Cisco	WS-C2950T-48-SI	Laboratorio de Redes	4	NO

Tabla 1. Dispositivos Intermediarios FEC.

5.1.2.4 Dispositivos de cómputos finales.

En la siguiente tabla se muestra información de los dispositivos de cómputos finales que están en uso actualmente en la Facultad de Electrotecnia y Computación.

DECANATURA						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
1	Equipo desktop	HP	HP EliteDest 705-G2-MT	Windows 10	4	SI
1	Equipo desktop	DELL	OPTIPLEX 3046	Windows 10	4	SI
1	Equipo desktop	LENOVO	THINKCENTRE	Windows 10	4	SI
VICE-DECANATURA						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
2	Equipo desktop	Hp	ELITE DESK 705G2 MT	Windows 10	4	SI
				Windows 10		
SECRETARIA DE LA FEC						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**

5	Equipo desktop	Dell	OPTIPLEX 3046	Windows 10	4	SI
DEPARTAMENTO DE ASA						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
5	Equipo desktop	Lenovo	THINKCENTRE	Windows 10	4	SI
3	Equipo desktop	HP	ELITE DESK 705G2 MT	Windows 10	4	SI
2	Equipo desktop	Dell	XPS	Windows 10	4	SI
DEPARTAMENTO DE L&S						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
3	Equipo desktop (CLON)			Windows 10	4	SI
1	Equipo desktop	HP	HP COMPAQ DC 5800 MT	Windows 10	4	SI
2	Equipo desktop	Dell	XPS	Windows 10	4	SI

1	Equipo desktop	Dell	OPTIPLEX 3046	Windows 10	4	SI
1	Equipo desktop	Dell	OPTIPLEX 7010	Windows 10	4	SI
2	Equipo desktop	Lenovo	THINKCENTRE	Windows 10	4	SI
LABORATORIO LEYDA MONTENEGRO						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
4	Equipo desktop	HP	ELITE DESK 705G2 MT	Windows 10	4	SI
6	Equipo desktop	DELL	XPS	Windows 10	4	SI
1	Equipo desktop	LENOVO	THINKCENTRE	Windows 10	4	SI
11	Equipo desktop (CLON)			Windows 10	4	SI
1	Equipo desktop	DELL	OPTIPLEX 7010	Windows 10	4	SI
LABORATORIO DE REDES						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**

10	Equipo desktop	HP	ELITE DESK 705G2 MT	Windows 10	4	SI
8	Equipo desktop	DELL	OPTIPLEX 7010	Windows 10	4	SI
1	Equipo desktop	LENOVO	THINKCENTR E	Windows 10	4	SI
DPTO. DE SISTEMA DIGITALES Y TELECOMUNICACIONES						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
4	Equipo desktop	LENOVO	THINKCENTRE	Windows 10	4	SI
1	Equipo desktop	DELL	XPS	Windows 10	4	SI
1	Equipo desktop	HP	ELITE DESK 705G2 MT	Windows 10	4	SI
1	Equipo desktop	DELL	OPTIPLEX 7010	Windows 10	4	SI
DEPARTEMENTO DE ELECTRONICA						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
2	Equipo desktop	HP	ELITE DESK 705G2 MT	Windows 10	4	SI
1	Equipo desktop	DELL	OPTIPLEX 7010	Windows 10	4	SI

1	Equipo desktop	LENOVO	THINKCENTRE	Windows 10	4	SI
1	Equipo desktop (CLON)			Windows 10	4	SI
DEPARTAMENTO DE ELECTRICA						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
3	Equipo desktop	HP	ELITE DESK 705G2 MT	Windows 10	4	SI
1	Equipo desktop	LENOVO	THINKCENTRE	Windows 10	4	SI
4	Equipo desktop	DELL	OPTIPLEX 7010	Windows 10	4	SI
1	Equipo desktop (CLON)			Windows 10	4	SI
LABORATORIO DE SIMULACION ELECTRONICA						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
30	Equipo desktop	HP	ELITE DESK 705G2 MT	Windows 10	4	SI
LABORATORIO DE AUTOMATIZACION						

Cantidad	Equipo	Marca	Modelo	SO	Versión IP	Soporta IPv6
2	Equipo desktop	DELL	OPTIPLEX 3046	Windows 10	4	SI
LABORATORIOS DE SISTEMAS DIGITALES Y MICROPROCESADORES						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
4	Equipo desktop	DELL	OPTIPLEX 3046	Windows 10	4	SI
LABORATORIO DE ELECTRONICA ANALOGICA						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
1	Equipo desktop	LENOVO	THINKCENTRE	Windows 10	4	SI
LABORATORIO DE CIRCUITOS ELECTRICOS Y SEÑALES						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
1	Equipo desktop	LENOVO	THINKCENTRE	Windows 10	4	SI

LABORATORIO DE TELECOMUNICACIONES						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
2	Equipo desktop	DELL	OPTIPLEX 3046	Windows 10	4	SI
LABORATORIO DE MAQUINAS ELECTRICAS						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
1	Equipo desktop (CLON)			Windows 10	4	SI
LABORATORIO DE INFORMATICA RODRIGO QUINTANA						
Cantidad	**Equipo**	**Marca**	**Modelo**	**SO**	**Versión IP**	**Soporta IPv6**
30	Equipo desktop	DELL	XPS	Windows 10	4	SI

Tabla 2. Dispositivos de Cómputos Finales FEC.

5.1.2.5 Organización de información.

Luego de recolectar todos los datos necesarios para comenzar el proceso de migración. Se debe implementar el uso de herramientas de diagramado, nosotros utilizaremos un diagrama de árbol en el cual definimos las tareas a realizar para conseguir el objetivo deseado.

5.1.2.6 Valoración de Datos Recopilados.

El objetivo de esta etapa es procesar la información y presentarla de una forma fácil de comprender.

En esta fase se estudió la información recopilada de la entrevista e inventario elaborados previamente y se evaluaron cada uno de los puntos sensibles para llevar a cabo la transición.

5.1.2.6.1 Sistemas Operativos en equipos de cómputo.

Como podemos observar en el siguiente grafico se da a conocer que el sistema operativo el cual usan los equipos de cómputo de la Facultad de Electrotecnia y Computación es el sistema operativo Windows 10.

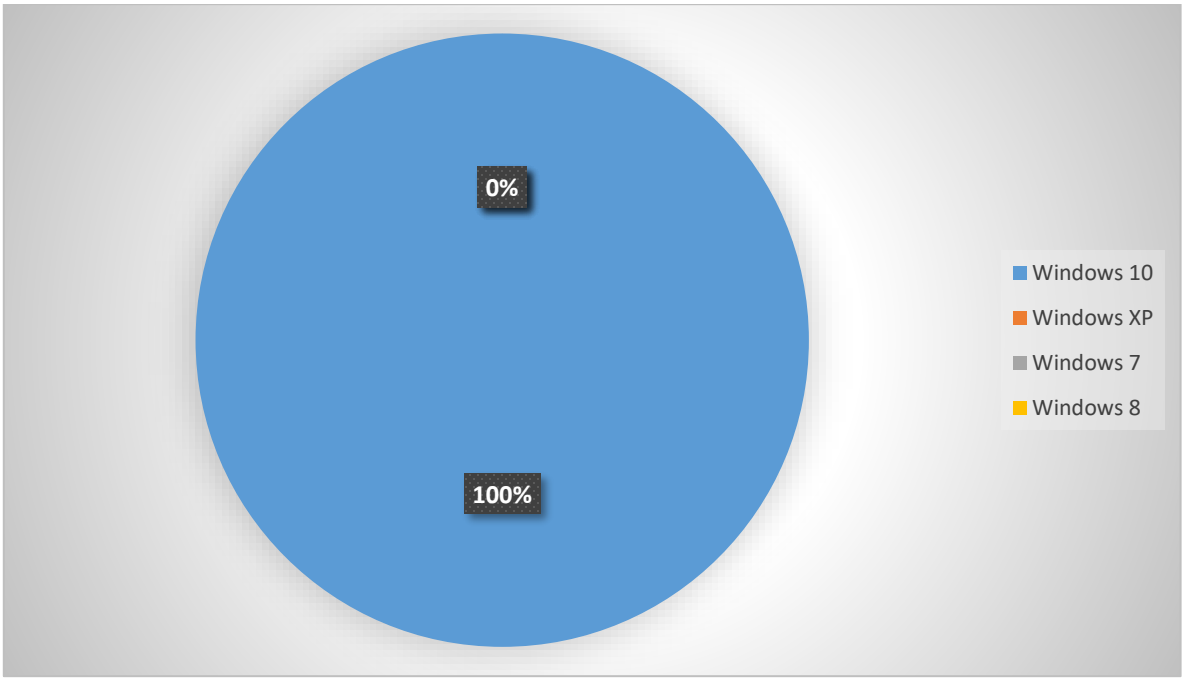

Ilustración 12. Estadística de Sistema Operativo de equipos de cómputos.

5.1.2.6.2 Soporte IPv6 en equipos de cómputo.

Como se muestra en la siguiente grafico se da a conocer que todos los equipos de cómputos finales soportan IPv6 y están listo para ser parte de este cambio en la infraestructura de red.

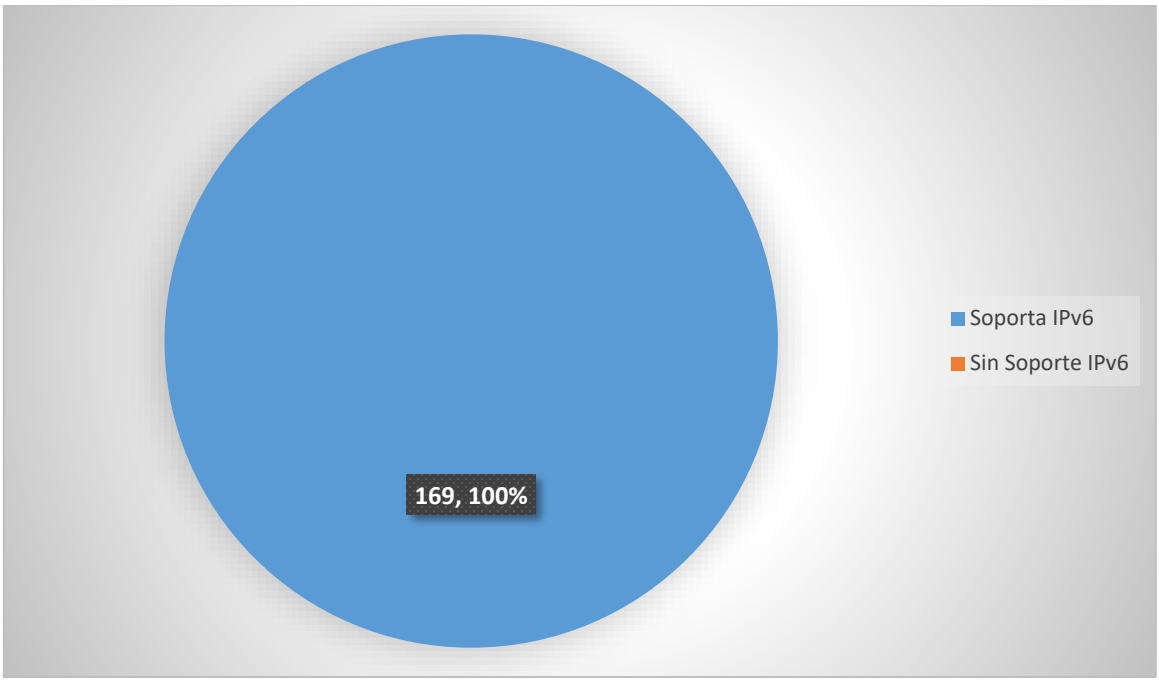

Ilustración 13. Soporta IPv6 por equipo final.

5.1.2.6.3 Soporte IPv6 en equipos de comunicación (switch).

Como se observa en la siguiente figura de acuerdo con la información brindada por los ingenieros encargado de ver la administración de red vemos que el 71% de equipos intermediarios instalados en la Facultad de Electrotecnia y Computación no soporta el protocolo IPv6. Véase ilustración 14.

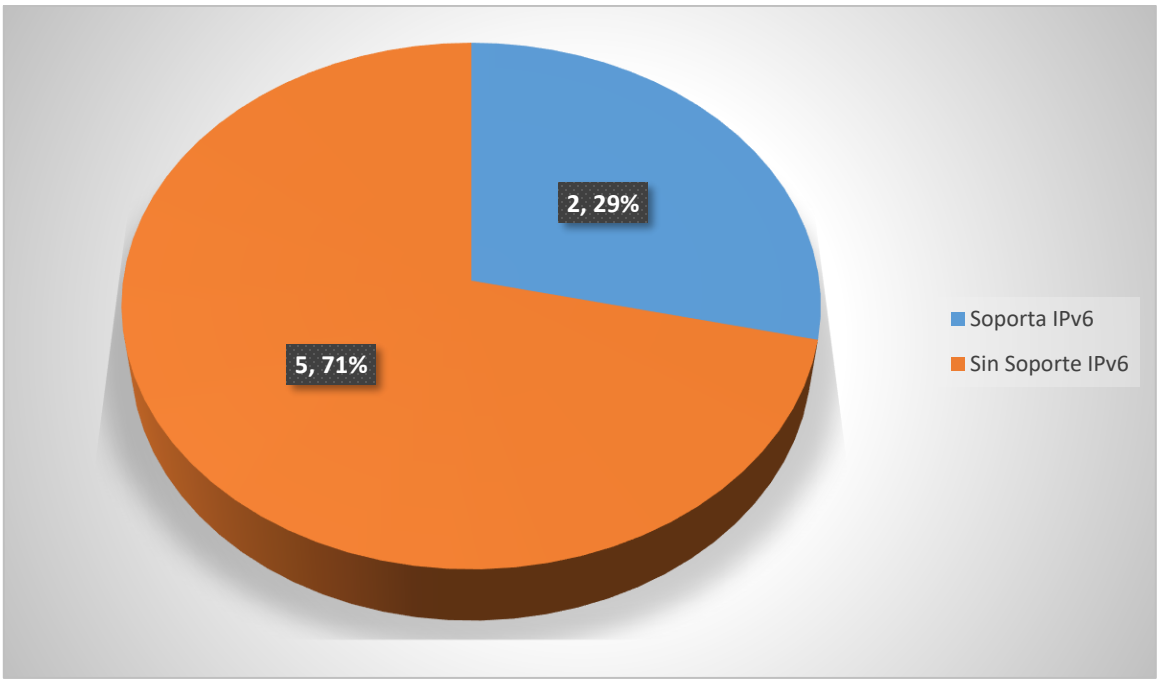

Ilustración 14. Soporte IPv6 en switches

5.1.2.7 Estimación de costo.

Dentro del proceso de transición se ve la necesidad de invertir económicamente en equipos de switches que sean capaces de soportar ambos protocolos de red para garantizar que la migración sea correcta. Como una actividad primordial es la estimación de costo de los equipos intermediarios teniendo en cuenta las características generales tanto del hardware como software de los equipos.

5.1.2.7.1 Sugerencias de Equipos para la transición a IPv6.

Si bien la facultad debe seguir funcionando de la manera que actualmente funciona, se sugiere empezar con la compra de los equipos que si soporten ambos protocolos de red para comenzar a implementar el nuevo protocolo de internet. A continuación, se mostrará unas series de equipo de switches intermediarios que soportan ambos protocolos de red.

Equipo	Modelo	Característica técnica	Precio
Switch (Cisco)	SRW224G4P-K9-NA	Los nuevos switches gestionados de la serie 300 Cisco Small Business ofrecen un rendimiento superior para satisfacer las necesidades de su pequeña empresa. IPv4/IPv6, HTTP, SNTP, TFTP, DNS, BOOTP, Bonjour.	U$ 529
Switch (Cisco)	WS-C2960X-24TS-L	Switch Administrable Capa L2 Cisco Catalyst, 24 puertos Gigabit 10/100/1000, 04 puertos Gigabit para fibra SFP, escritorio, rack-mountable, capacidad de switching 216 Gbps, VLANs : 1023, IPv6 support, IEEE 802.1x, Cisco IOS LAN Base Software	U$ 1,625
Switch (Cisco)	WS-C2960X-48FPS-L	Switch Administrable capa L2 CISCO Catalyst 2960-X con 48 puertos PoE (740W) 10/100/1000, 04 puertos para fibra SFP Gigabit , Dual Core CPU , Memoria DRAM de 512MB, Memoria Flash de	U$ 3,999

		128MB, capacidad de switching 216 Gbps, VLANs : 1023, IPv6 support, IEEE 802.1x, soporta fuente de poder redundante externa (RPS), LAN Base Cisco IOS Software	
Switch (Cisco)	WS-C2960S-48TS-L	Conmutación Layer 2, auto-sensor por dispositivo, asignación dirección dinámica IP, alimentación mediante Ethernet (PoE), negociación automática, soporte BOOTP, soporte ARP, equilibrio de carga, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP, soporte para Syslog, soporte DiffServ, Broadcast Storm Control, soporte IPv6, Multicast Storm Control, Unicast Storm Control, admite Rapid Spanning Tree Protocol (RSTP), admite Multiple Spanning Tree Protocol (MSTP), snooping DHCP, soporte de Dynamic Trunking Protocol (DTP), soporte de Port Aggregation Protocol (PAgP), soporte de Access Control List	U$ 3,959

		(ACL), Quality of Service (QoS), PoE+, Protocolo de control de adición de enlaces (LACP), Port Security, MAC Address Notification, Remote Switch Port Analyzer (RSPAN)	

Tabla 3. Sugerencia de Equipos Intermediarios FEC.

5.2 Definición de las tareas realizadas.

Transición de infraestructura de servicio informáticos hacia ipv6.

- Recolección de información.
  - Realizamos entrevistas con el personal técnico del nic.ni
  - Obtuvimos tablas con los modelos de los switches intermedios.
- Inventario de equipos.
  - Solicitamos acceso a las áreas afectadas por el alcance del proyecto
  - Extrajimos información necesaria por equipo.
    - Intermedio
    - Final
- Valoración de inventario.
  - Comprobamos si los equipos actuales cumplen con los requisitos necesarios para el proyecto.
- Propuesta de equipos para sustituir los que no cumplen los requisitos.
  - Investigamos los equipos que cumplen con los requisitos y realizamos una propuesta de compra que satisfaga la relación costo/beneficio

- Realizamos mapa topológico de la infraestructura actual.
    - Obtuvimos previamente la información (ubicación) de los equipos (inventario).
    - Realizamos análisis de red.
    - Creación de vlan en equipos intermedios.
    - Administración de vlan mediante protocolo vtp (se centraliza).
    - Crear sub interfaces para el transporte de datos de vlan en el enrutador.
    - Encapsulamiento de vlan mediante protocolo dot1q.
    - Configuración DHCP.
    - Configuración servidor WEB.
    - Configuración servidor dns.
- Realizamos mapa topológico de la infraestructura propuesta.
    - Definimos el tipo de topología.
    - Modelado de nueva topología.
    - Ejecución de metodología de migración.
        - Método Dual Stack.
    - Configuración de los servicios deseados en la nueva topología.
- Realizamos pruebas de la nueva topología para asegurar su funcionamiento.
    - Probamos comunicación ipv4 e ipv6.
    - Probamos conexión DNS.
    - Probamos conexión hacia la web.

5.2.1 Representación en diagrama.

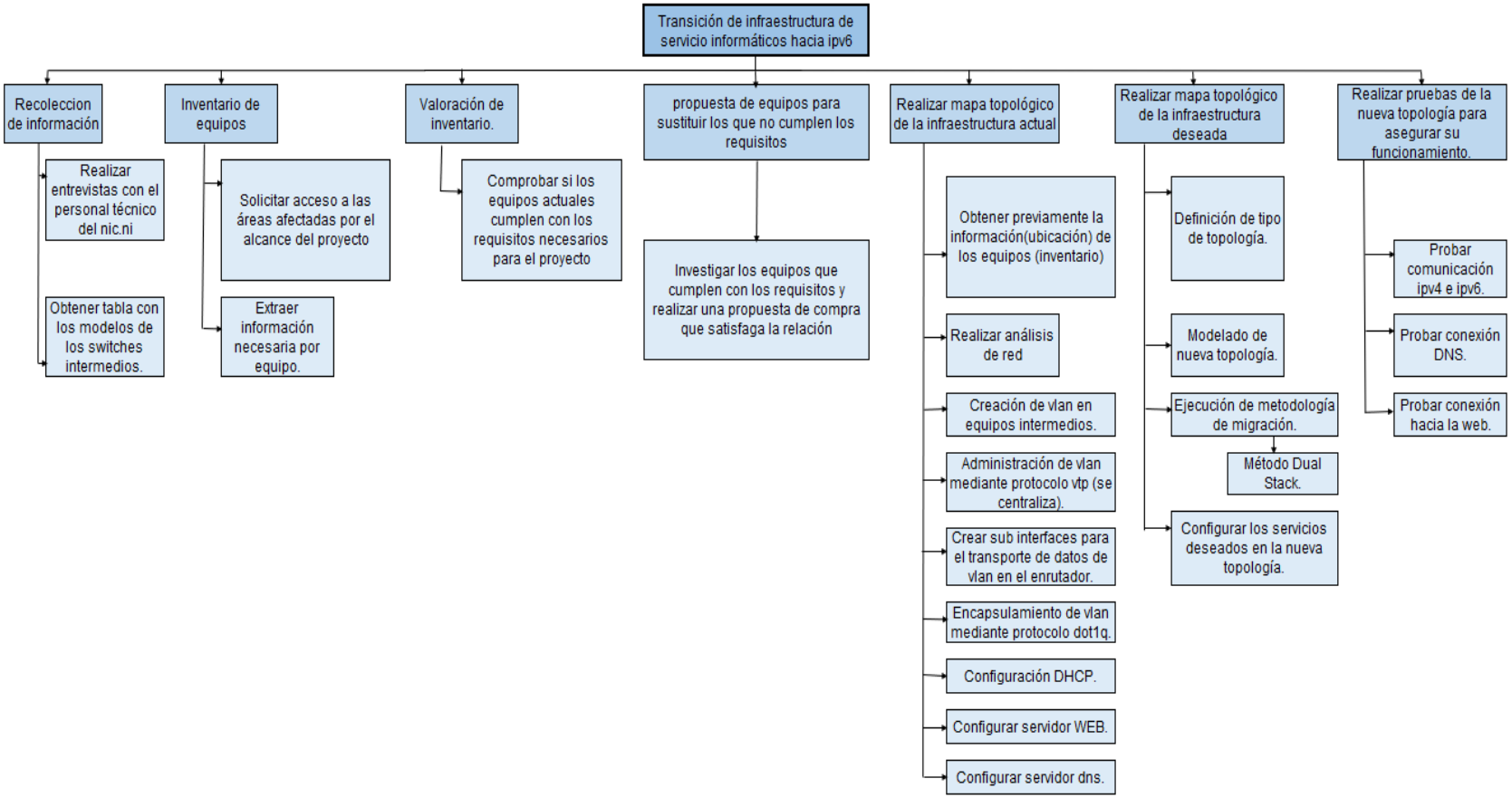

Ilustración 15. Representación de Diagrama de árbol.

5.2.2 Definición de secuencia de tareas.

A continuación, representamos la secuencia deseada para alcanzar una migración exitosa, incluimos la documentación elemental requerida para el correcto planteamiento de las necesidades del área afectada. Así también algunos de los posibles inconvenientes que podemos encontrar al desarrollar estas actividades.

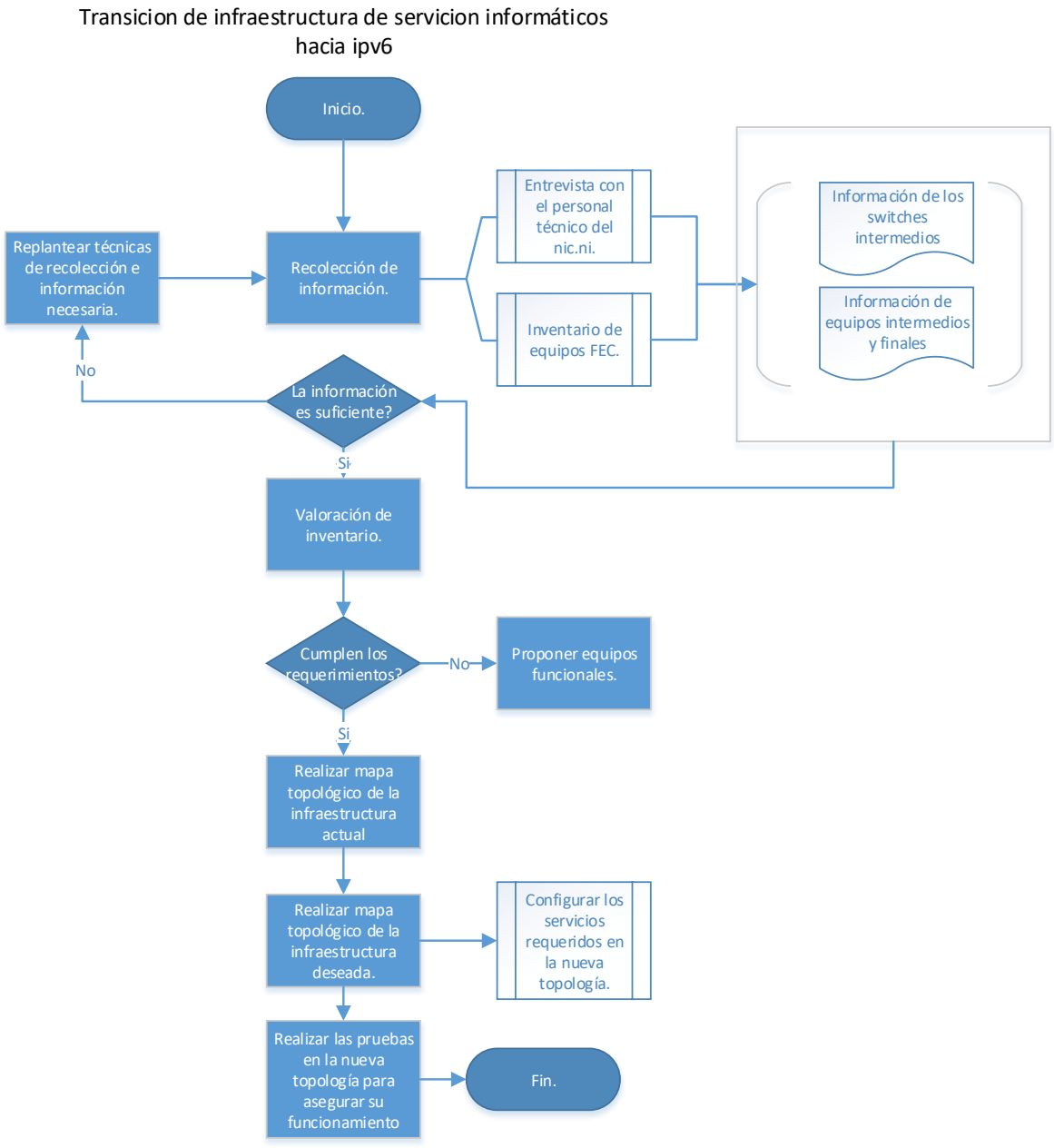

Ilustración 16. Diagrama de flujo de las tareas definidas.

Como documentación requerida definimos la distribución de los switches intermedios y la información de los equipos intermedios y finales. Esto debido a las decisiones que se deben tomar en base a esta información, cabe destacar que los métodos utilizados para generar esta información pueden variar. Pero como mencionamos anteriormente, la información en sí misma no puede ser omitida.

5.3 Desarrollar soluciones.

5.3.1 Mecanismo de Transición.

Los mecanismos de transición a IPv6 son las tecnologías que facilitan y facilitarán la transición de Internet de su infraestructura IPv4 al sistema de direccionamiento de nueva generación IPv6.

5.3.1.1 Mecanismo de Transición por Túneles.

Los túneles proporcionan un mecanismo que permite establecer conexiones IPv6 sobre una red IPv4 (y viceversa). Los túneles se utilizan cuando un equipo desea acceso a la red IPv6 existente. Para ello el equipo deberá crear un túnel a través de IPv4 con un router que tenga tanto acceso a IPv6 como IPv4.

El tunneling es una técnica de integración y transición intermedia, y no debe considerarse como una solución definitiva. El objetivo final debe ser una arquitectura IPv6 nativa.

5.3.1.2 Mecanismo de Transición Dual Stack.

El método Dual Stack permite hacer coexistir ambas tecnologías de red sobre un mismo enlace, particularmente útil para implementar con toda tranquilidad IPv6 en una red local sin alterar en principio el funcionamiento de IPv4.

IPv6 nativo en Doble pila es el método de transición recomendado. Las principales ventajas sobre los otros mecanismos son que IPv4 continúa operando con normalidad mientras se introduce IPv6 a la red, y en esencia, la implementación de IPv6 será definitiva, que no requerirá retirarse posteriormente. (nic.cr, s.f.)

5.3.2 Análisis de la topología actual de la red y su funcionamiento.

La red de datos en la Facultad de Electrotecnia y Computación actualmente funciona bajo una combinación de topología de bus y estrella, en que los switches están conectados en forma lineal llegando a formar una topología de estrella en los switches de acceso que dan conexión a los dispositivos finales.

La red de datos de la Facultad de Electrotecnia y Computación se comunica desde el switch principal ubicado en el sótano del edificio Rigoberto López Pérez donde se conecta al enlace por medio de fibra óptica OS2 monomodo que soporta velocidades de transmisión de hasta 10 gigabit ethernet por segundo (gbps). El switch principal conecta al switch de distribución ubicado en la parte norte de la Universidad Nacional de Ingeniería ubicado en el centro de datos de la administración del nic.ni donde se da acceso a cada uno de los diferentes switches que dan conexión a las diferentes áreas de la Facultad de Electrotecnia y Computación.

La conexión desde el switch de distribución hacia los switches de acceso ubicado en el departamento de arquitectura y sistema de aplicación y al laboratorio de cómputo Leyda Montenegro se conecta por medio de fibra óptica con velocidad máxima de conexión de hasta 10 Gbps cabe mencionar que las velocidades de transporte de datos varían entre las áreas de la facultad y a criterio de los ingenieros de administración de red.

El resto de switches de acceso conectados al switch de distribución se conectan mediante cable utp categoría 6 que soportan velocidades de hasta 1 gbps. Estas velocidades soportadas por los distintos medios de conexión son suficientes dentro de un área de trabajo o en este caso dentro de la Facultad de Electrotecnia y Computación para llevar a cabo sus tareas según los administradores de red.

La Facultad de Electrotecnia y Computación está conectada por medio de diferentes segmentos de red IPv4 por lo cual se asignan direcciones IP de forma automática mediante el protocolo DHCP según el área de trabajo que está conformada, por los cual más adelante se mostrara información más detallada creada por los autores de

este documento para tener una mayor comprensión de como esta está organizada la topología actual.

Se debe mencionar que la topología mostrada en la siguiente **ilustración 17** fue creada por los autores de este documento para poder mostrar de una manera más representativa y poder generar una mayor compresión y visualización de cómo está conformado el diseño dentro de la Facultad de Electrotecnia y Computación. Esté diseño topológico se realizó con la información recopilada de las fases anteriores mediante entrevista a los ingenieros en la administración de red de la NIC.NI.

5.3.2.1 Tabla de que switch alimenta cada oficina.

En la siguiente tabla se muestra la ubicación de los equipos que se conectan a cada switch para el transporte de datos.

Ubicación de los Switch	Área que alimenta
Dpto. ASA	• Profesores del Dpto. ASA. • Vice Decanatura. • Sala de uso múltiple.
Secretaría FEC	• Oficina de secretaria FEC. • Decanatura. • Docentes de Dpto. Eléctrica. • Laboratorio de Simulación. • Servicios Administrativos. • Laboratorio de Electrónica Digital.
Sarec-fec-1	• Docentes del Dpto. Lenguaje y Simulación.
Sarec-fec-2	• Docentes del Dpto. Lenguaje y Simulación.

Dpto. EO	• Docentes del Dpto. Electrónica. • Laboratorio de Telecomunicaciones.
Laboratorio Leyda Montenegro.	• Laboratorio Leyda Montenegro. • Enlace a Laboratorio de Redes.
Laboratorio Redes	• Laboratorio de Redes. • Laboratorio de Hardware.
SotanoNIC.NI (parte norte)	• Enlace a laboratorio de Rodrigo Quintana.
Laboratorio Eléctrica Rodrigo Quintana	• Laboratorio de Eléctrica Rodrigo Quintana.

Tabla 4. Ubicación de switch y que área alimenta.

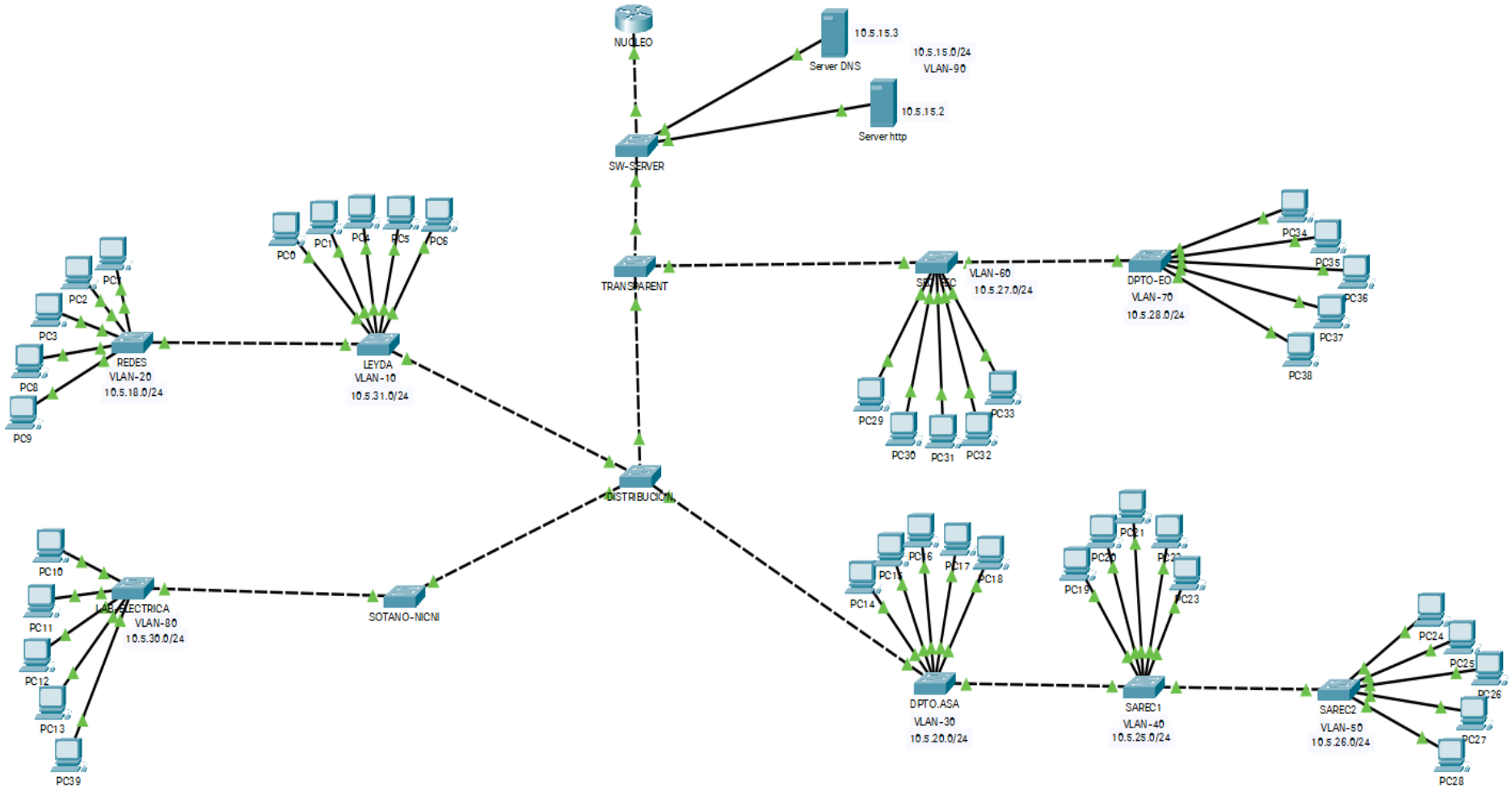

Ilustración 17. Representación de topología actual.

5.3.2.2 Tabla de conexiones Lógica de los switches.

Los switches son equipos que funcionan dentro de la capa 2 del modelo OSI donde realizan el compartimento de trama dentro de la infraestructura de red y son los encargados de las conexiones con los equipos finales por lo cual debemos tener claro la configuración de cada uno de ellos. En la siguiente tabla definiremos como está conectado y configurado cada uno de los switches en la topología.

La información que contiene esta tabla son datos creados por los autores del proyecto para brindar información más detallada de cómo funcionan y como se configuran cada equipo intermediario.

Ubicación Equipos	Nombre del Switch	Subred IPv4	Direccionamiento IP	Vlan ID	Puerto Trunk
Dpto. Asa	ASA	10.5.31.0/24	DHCP	Vlan 30	23-24
Secretaría FEC	SECRETARIA-FEC	10.5.27.0/24	DHCP	Vlan 60	23-24
Sarec-fec-1	SAREC1	10.5.25.0/24	DHCP	Vlan 40	23-24
Sarec-fec-2	SAREC2	10.5.26.0/24	DHCP	Vlan 50	24
Dpto. EO	DPTO-EO	10.5.28.0/24	DHCP	Vlan 70	24
Laboratorio Leyda Montenegro	LEYDA	10.5.31.0/24	DHCP	Vlan 10	23-24
Laboratorio Redes	REDES	10.5.18.0/24	DHCP	Vlan 20	24

SotanoNIC.NI (parte norte)					23-24
Laboratorio Eléctrica Rodrigo Quintana	LAB-ELECTRICA	10.5.30.0/24	DHCP	Vlan 80	24

Tabla 5. Conexiones lógicas de switches de acceso.

5.3.2.3 Conexión del switch al puerto del enrutador.

En esta sección se describirá la conexión de interfaces física y la creación de las interfaces virtuales al enrutador para el transporte de datos atreves de las diferentes VLANs.

Al igual que con tabla anterior esta información es a nivel de topología en el simulador de cisco packet tracer totalmente creada por los autores de este documento para dar una mejor representación de cómo funciona los diagramas topológicos.

Interfaz física del router	**Interfaz Virtual**	**Vlan Asociada a la Interfaz Virtual**	**Nombre del Pool Asociado**	**Segmento IPv4 Asociado al Pool**
FasEthernet0/0	FasEthernet0/0.10	VLAN 10	Pool 10	10.5.31.0/24
FasEthernet0/0	FasEthernet0/0.20	VLAN 20	Pool 20	10.5.18.0/24

FasEthernet0/0	FasEthernet0/0.30	VLAN 30	Pool 30	10.5.20.0/24
FasEthernet0/0	FasEthernet0/0.40	VLAN 40	Pool 40	10.5.25.0/24
FasEthernet0/0	FasEthernet0/0.50	VLAN 50	Pool 50	10.5.26.0/24
FasEthernet0/0	FasEthernet0/0.60	VLAN 60	Pool 60	10.5.27.0/24
FasEthernet0/0	FasEthernet0/0.70	VLAN 70	Pool 70	10.5.28.0/24
FasEthernet0/0	FasEthernet0/0.80	VLAN 80	Pool 80	10.5.30.0/24

Tabla 6. Conexión lógica del switch central al router.

5.4 Implementación del mecanismo de transición.

5.4.1 Aplicación del método Dual Stack.

La aplicación de este método nos asegura la coexistencia entre los protocolos IPv4 e IPv6. Una de las bondades más recalcables de este método de transición es la escalabilidad con la que se puede aplicar ya que no se prescinde del protocolo IPv4. Esto nos permite mantener compatibilidad con entidades que trabajen aun con IPv4 y nos asegura una migración nativa hacia IPv6 cuando IPv4 esté totalmente desfasado.

Para la coexistencia de IPv4 e IPv6 los equipos instalados dentro de la infraestructura de red deben de soportar ambas tecnologías sobre un mismo enlace

donde los equipos modernos en la actualidad ya traen este nuevo servicio para la coexistencia de ambos protocolos.

Como primera instancia para que los equipos en una red funcionen deben hacerse una serie de configuraciones tanto en IPv4 como en IPv6. Por defecto tantos los router como los switches vienen en un entorno de trabajo para configurarse bajo IPv4 por lo que debemos habilitar el protocolo IPv6 sobre el mismo nodo donde está en funcionamiento IPv4.

Como primera instancia a la hora de empezar a implementar IPv6 sobre el mismo nodo donde tenemos IPv4 debemos entrar en la **CLI** de los equipos al modo de configurar global para poder habilitar el uso de IPv6 mediante el comando **IPv6 unicast-routing** por lo que de manera automática habilita el protocolo IPv6.

Después que los equipos tengan habilitado ambos protocolos de internet en los distinto nodos empezaremos a configurar cada uno de los servicios que deseemos integrar en nuestra red.

Para poder asignar direcciones IP a las interfaces de cada equipo final debemos configurar en los equipos intermediarios (switches y router) una serie de pasos lógicos que permitan dar conexión a los dispositivos finales. En el caso que decidamos que las direcciones IP se asignen automáticamente debemos habilitar y configurar el protocolo DHCP para IPv4 y DHCPv6 para asignar direcciones IPv6 automáticamente.

Como veremos en las fases siguiente que ambos protocolos tanto IPv4 como IPv6 entraran en funcionamiento en las interfaces de los equipos de cómputos donde también definiremos cada una de las conexiones lógicas a los dispositivos intermediarios.

5.4.2 Diseño de la topología de red con el método Dual-Stack.

En esta etapa se plantea la propuesta del diseño topológico de la red de transporte de datos de la Facultad de Electrotecnia y Computación generando un gran cambio con respecto al diagrama anterior y proponiendo una gran mejora en la red, generando más confiabilidad mejor escalabilidad y funcionalidad en la red configurando los dispositivos para que puedan trabajar con las nuevas tecnologías que mejoran el uso de estas.

Los dispositivos mostrados en esta nueva propuesta funcionan en un entorno de doble pila soportando el uso del protocolo de internet versión 6 (IPv6) lo cual mejorara el problema de falta de direcciones IP como el caso del protocolo de internet versión 4 (IPv4) y poder conectar con equipos que tengan implementado el protocolo IPv6 ya sea en una red local o hacia internet de manera global.

El tipo de topología propuesta es de tipo estrella extendida donde el router se conecta al switch central que será utilizado como el conmutador principal donde tendrá la información central de cada uno de las vlans creadas que están asignadas a las interfaces de los switches de acceso que son los equipos que dan comunicación a los equipos finales.

El enrutador es el encargado de proporcionar direcciones IP a cada equipo a través de las diferentes vlans configuradas en cada switch por medio del protocolo DHCP y DHCPv6 exceptuando los servidores DNS y HTTP ya que esto poseen direcciones IP estáticas. Las PC representan oficinas y laboratorios de los cuales están conectados en cada switch de acceso según su ubicación.

En el diseño de la topología propuesta se configuran un servidor dns y un servidor web que poseen un entorno de trabajo bajo el método dual stack donde ambos servidores funcionaran bajo el protocolo IPv4 e IPv6.

Como ejemplo en un entorno de trabajo que se está llevando a cabo una migración de servicios, el servidor web que contiene un aplicativo web se podrá acceder de cualquier equipo de cómputo final que posea una dirección IP ya sea que tenga asignada una dirección IPv4 o una dirección IPv6.

Los segmentos IP asignados a las interfaces de los switches de acceso para cada vlans según el área de trabajo dentro de la Facultad de Electrotecnia y Computación a los que estén conectados estarán funcionando bajo el método dual stack donde cada vlans posee un segmento diferente. La información de estos segmentos asignados a las diferentes vlans y las interfaces asignadas en modo trunk se mostrarán más adelante de manera detallada.

En la siguiente ilustración se muestra la topología propuesta soportando el protocolo de internet versión 4 y el protocolo de internet versión 6. Como se muestra en la imagen se diseñó una topología diferente con respecto a la topología anterior utilizando el tipo de topología de estrella extendida.

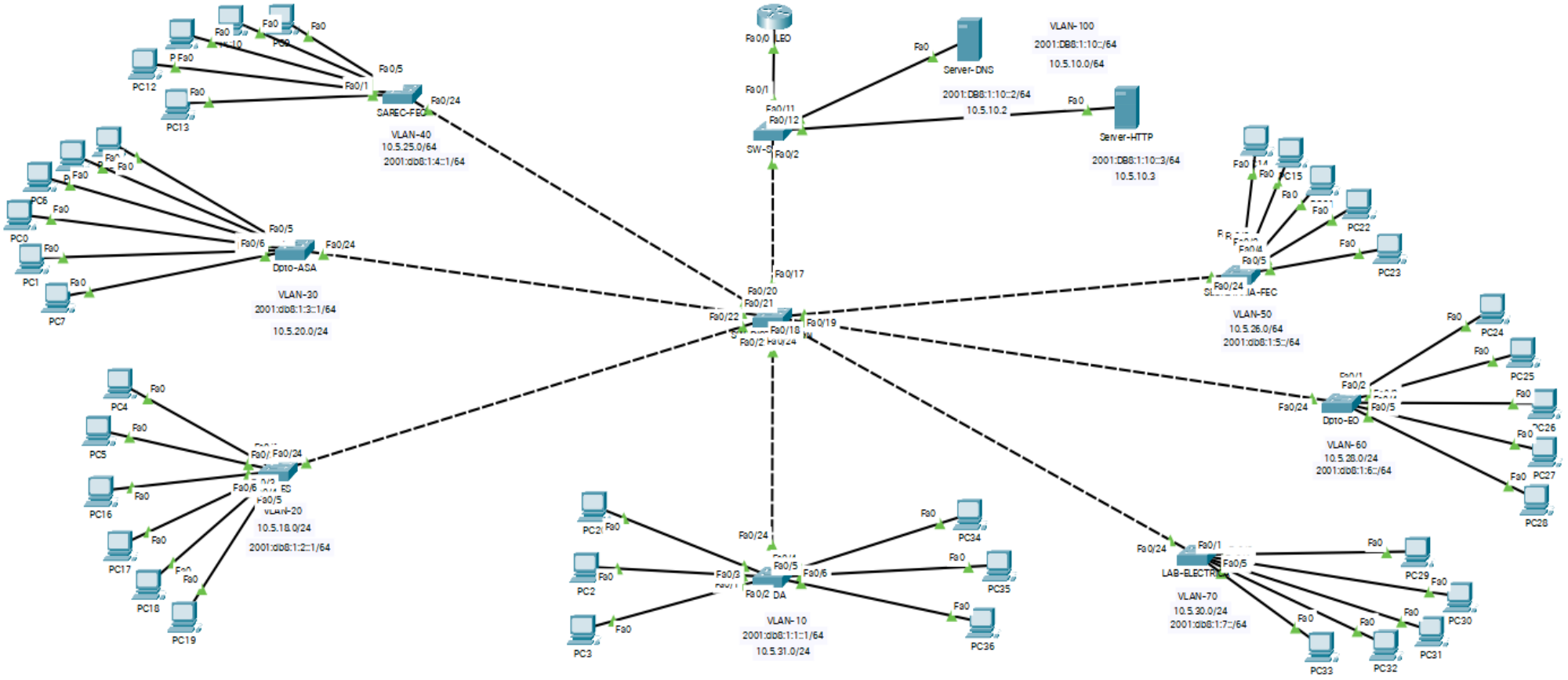

Ilustración 18. Representación de topología propuesta.

5.4.2.1 Conexión Lógica con IPv4.

En la siguiente tabla definiremos como está conectado y configurado cada uno de los equipos en la topología con el protocolo IPv4 con la nueva topología.

Ubicación Equipos	Nombre del Switch	Subred IPv4	Direccionamiento IP	Vlan ID	Puerto Trunk
Laboratorio Leyda Montenegro.	LEYDA	10.5.31.0/24	DHCP	Vlan 10	24
Laboratorio Redes	REDES	10.5.18.0/24	DHCP	Vlan 20	24
Dpto. Asa	ASA	10.5.20.0/24	DHCP	Vlan 30	24
SAREC-FEC	SAREC-FEC	10.5.25.0/24	DHCP	Vlan 40	24
Secretaría FEC	SECRETARIA-FEC	10.5.26.0/24	DHCP	Vlan 50	24
Dpto. EO	Dpto-EO	10.5.28.0/24	DHCP	Vlan 60	24
Laboratorio Eléctrica Rodrigo Quintana	LAB-ELECTRICA	10.5.18.0/24	DHCP	Vlan 70	24
Sótano del edificio RLP	SW-SERVER			Vlan 100	1-2

Tabla 7. Conexión lógica IPv4 de los swithches en la topología propuesta.

5.4.2.2 Conexión Lógica con IPv6.

En la siguiente tabla definiremos como está conectado y configurado cada uno de los equipos en la topología con el protocolo IPv6 con la nueva topología.

Ubicación Equipos	Nombre del Switch	Subred IPv4	Direccionamiento IP	Vlan ID	Puerto Trunk
Laboratorio Leyda Montenegro	LEYDA	2001:db8:1:1::0/64	DHCPv6	Vlan 10	24
Laboratorio Redes	REDES	2001:db8:1:2::0/64	DHCPv6	Vlan 20	24
Dpto. Asa	ASA	2001:db8:1:3::0/64	DHCPv6	Vlan 30	24
SAREC-FEC	SAREC-FEC	2001:db8:1:4::0/64	DHCPv6	Vlan 40	24
Secretaría FEC	SECRETARIA-FEC	2001:db8:1:5::0/64	DHCPv6	Vlan 50	24
Dpto. EO	Dpto-EO	2001:db8:1:6::0/64	DHCPv6	Vlan 60	24
Laboratorio Eléctrica Rodrigo Quintana	LAB-ELECTRICA	2001:db8:1:7::0/64	DHCPv6	Vlan 70	24
Sótano del edificio RLP	SW-SERVER	2001:DB8:1:10::0/64	DHCPv6	Vlan 100	1-2

Tabla 8. Conexión lógica IPv6 de los switches en la topología propuesta.

5.5 Fase de Verificación.

En esta fase se hace una verificación de los resultados en las fases anteriores con los cuales haremos una serie de pruebas demostrando los resultados esperados. Estas son las pruebas que se realizan sobre los equipos, los cuales serán tomados como demostración del funcionamiento correcto.

PRUEBA	DESCRIPCION DE LA PRUEBA	RESULTADO
1	Prueba de conexión con IPv4	Exitoso
2	Prueba de conexión con Ipv6	Exitoso
3	Prueba hacia el servidor web con direccionamiento IPv4	Exitoso
4	Prueba hacia el servidor web con direccionamiento IPv6	Exitoso
5	Prueba hacia el servidor web con nombre de dominio definido.	Exitoso

Tabla 9. Pruebas de verificaciones.

La fase de verificación de resultados se realiza desde el simulador de cisco packet tracer donde haremos unas pruebas para comprobar la conexión de los protocolos de internet versión 4 y del protocolo de internet versión 6.

5.5.1 Verificación por IPv4.

Como parte de las verificaciones de conexión de datos bajo el protocolo IPv4 lo haremos mediante el protocolo ICMP, lo cual haremos ping desde un equipo de escritorio que se encuentra en el departamento de arquitectura y sistema de aplicación a un equipo que se encuentra en laboratorio Leyda Montenegro como podemos observar en la siguiente ilustración.

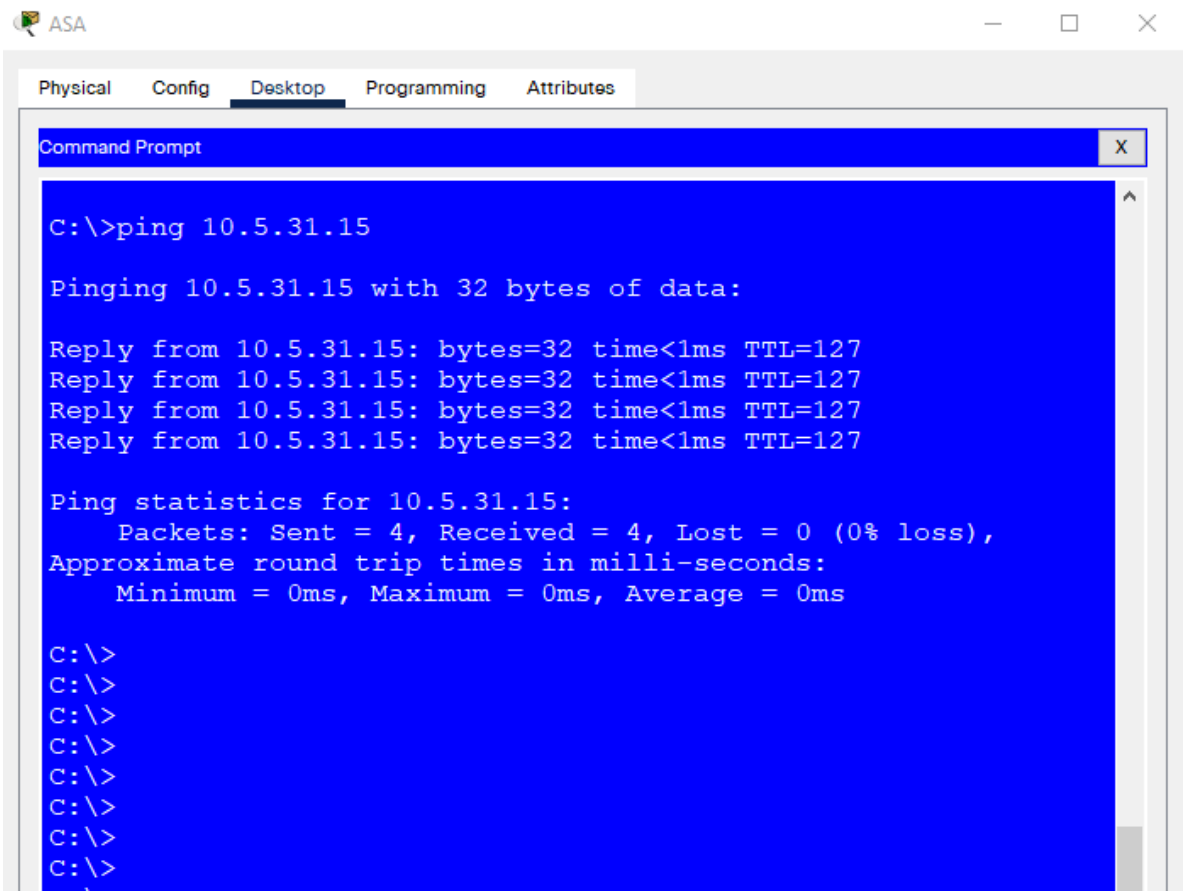

Ilustración 19. Verificación de conectividad IPv4 en ASA.

Como podemos observar en la ilustración anterior se demuestra que el ping realizado desde equipo de escritorio ubicado en el departamento de ASA al equipo ubicado en el laboratorio Leyda Montenegro es exitoso demostrando conectividad entre ambos equipos.

Ahora observaremos la conexión de un equipo ubicado en el laboratorio Leyda Montenegro al departamento de ASA, demostrando nuevamente relación entre dispositivos conectados en segmento de red diferentes.

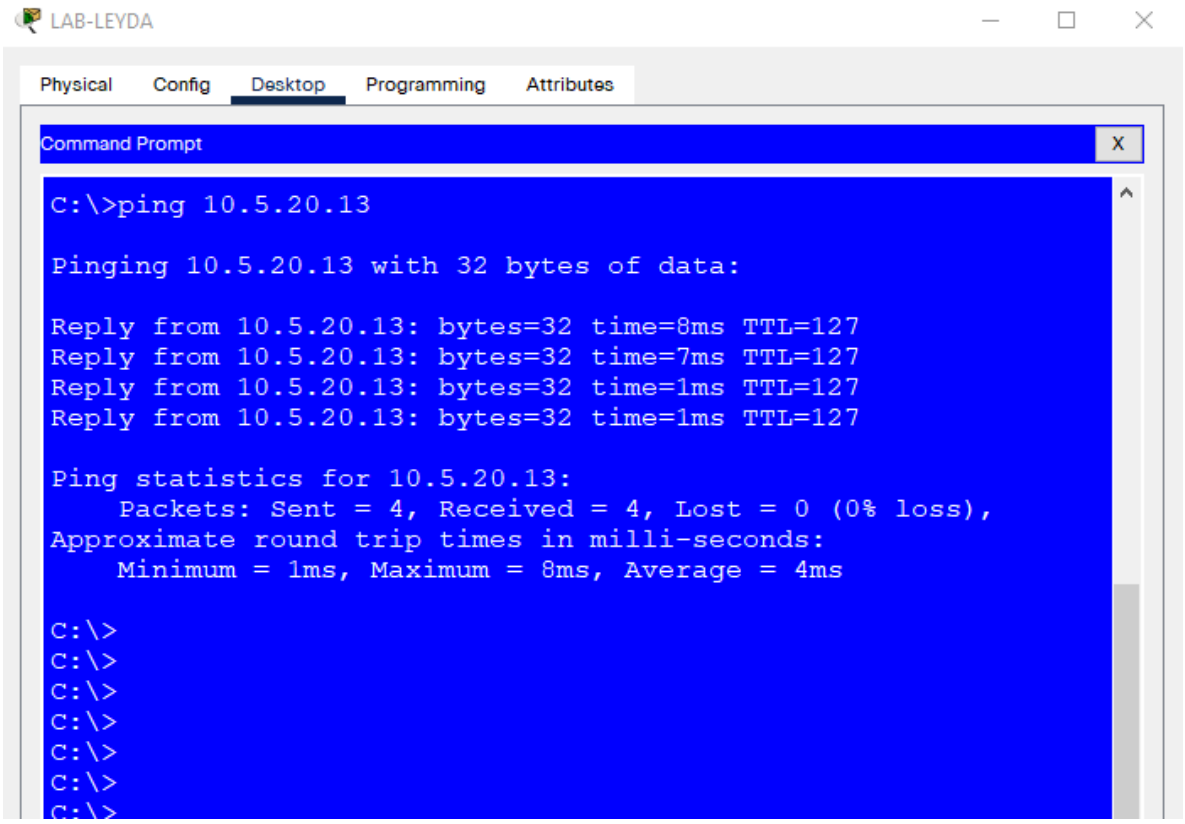

Ilustración 20. Verificación de conectividad IPv4 en LAB-LEYDA.

Como mencionamos anteriormente la conexión se realizó de manera exitosa, procediendo hacer la prueba mediante el protocolo versión 6, donde podremos verificar y demostrar que ambos dispositivos están configurados en doble pila.

5.5.2 Verificación por IPv6.

En esta etapa podremos determinar la coexistencia de ambos protocolos donde haremos ping usando una dirección IP versión 6 dentro del segmento de red 2001:db8:1:1::/64.

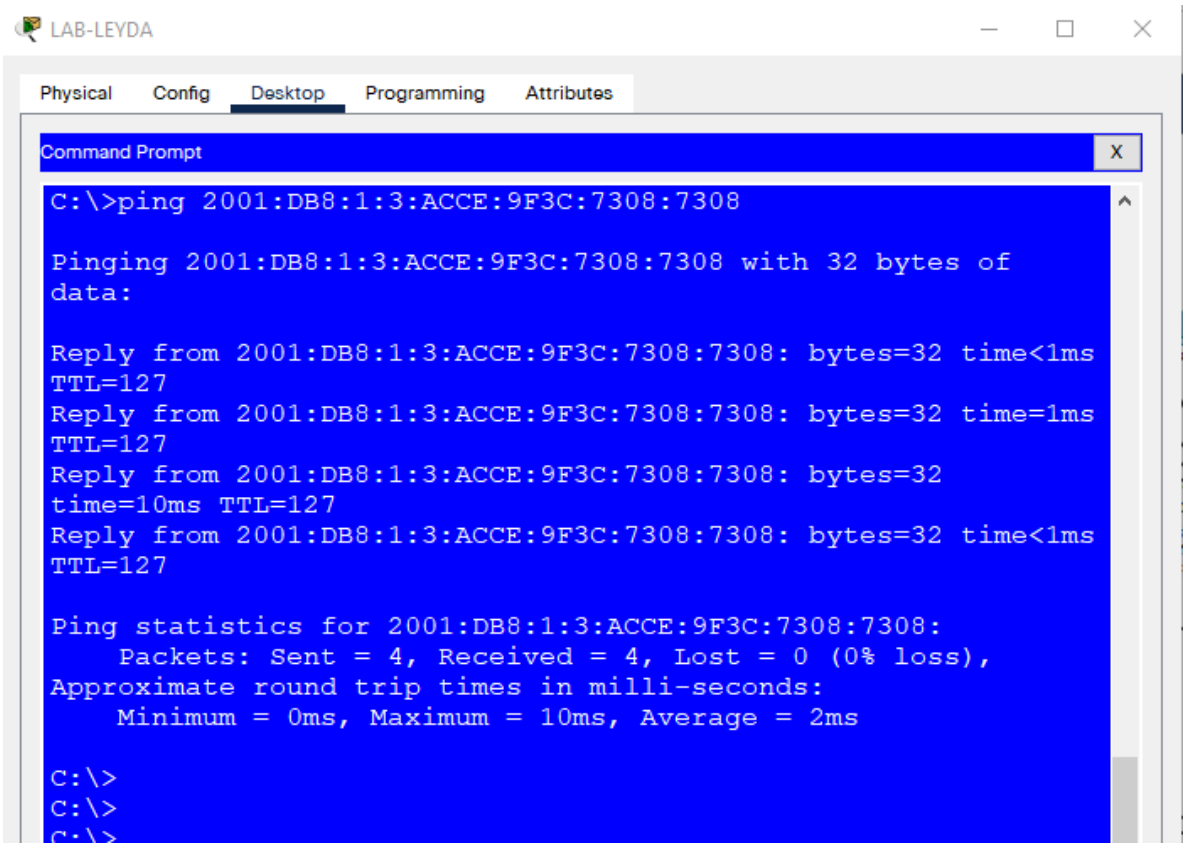

Ilustración 21. Verificación de conectividad IPv6.

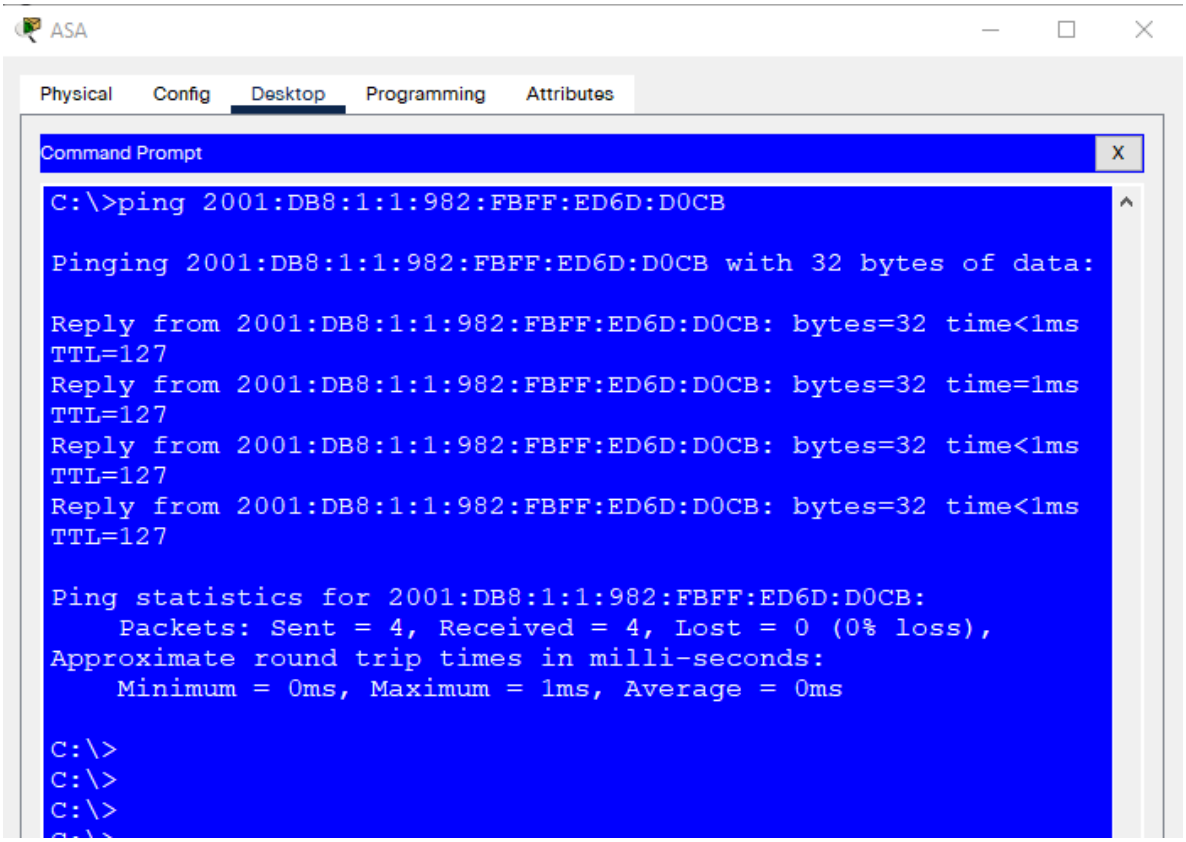

Ilustración 22. Verificación de conectividad IPv6 en Dpto. ASA

Como pudimos ver en las imágenes anteriores se demuestra que la conexión con el protocolo IPv6 se conecta de forma correcta por lo que podemos comprobar que la interfaz está conectada en dual stack.

5.5.3 Verificación al servidor web.

En esta sección de verificaciones lo haremos por medio de direcciones IP para verificar que tenemos conexión tanto IPv4 y IPv6. Se tomará la dirección IP tanto IPv4 como Ipv6 para demostrar que podemos acceder a un sitio web por medio de direcciones IP y así probar que la conexión fue exitosa.

5.5.3.1 Prueba al servidor web por medio de dirección IPv4 asociado.

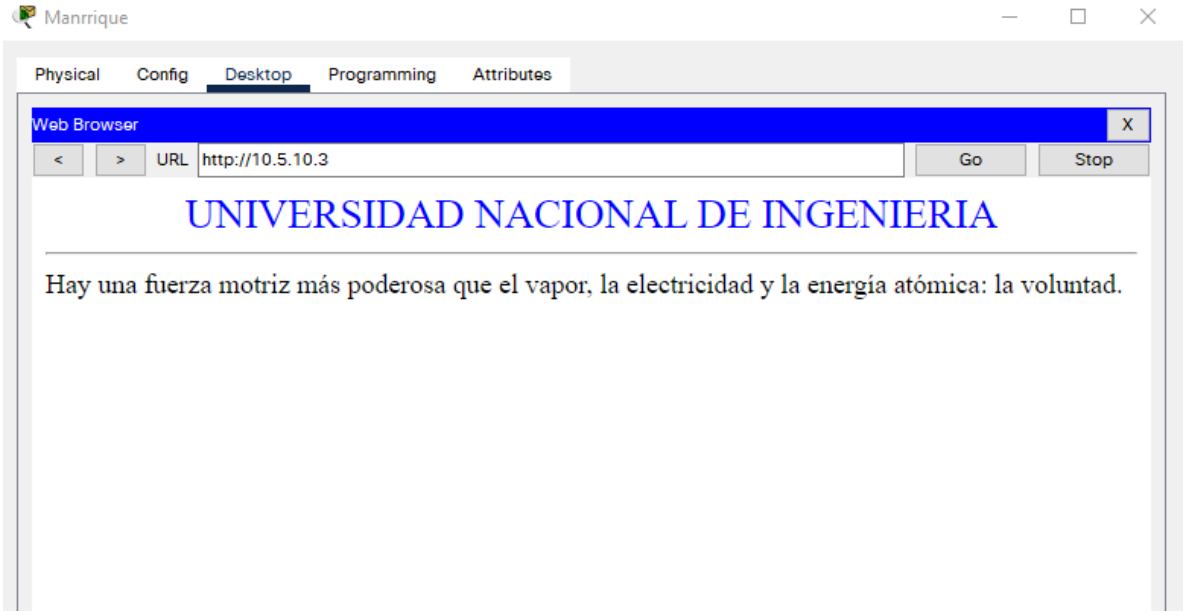

Ilustración 23. Verificación al servidor por medio dirección IPv4.

5.5.3.2 Prueba al servidor web por medio de dirección IPv6 asociado.

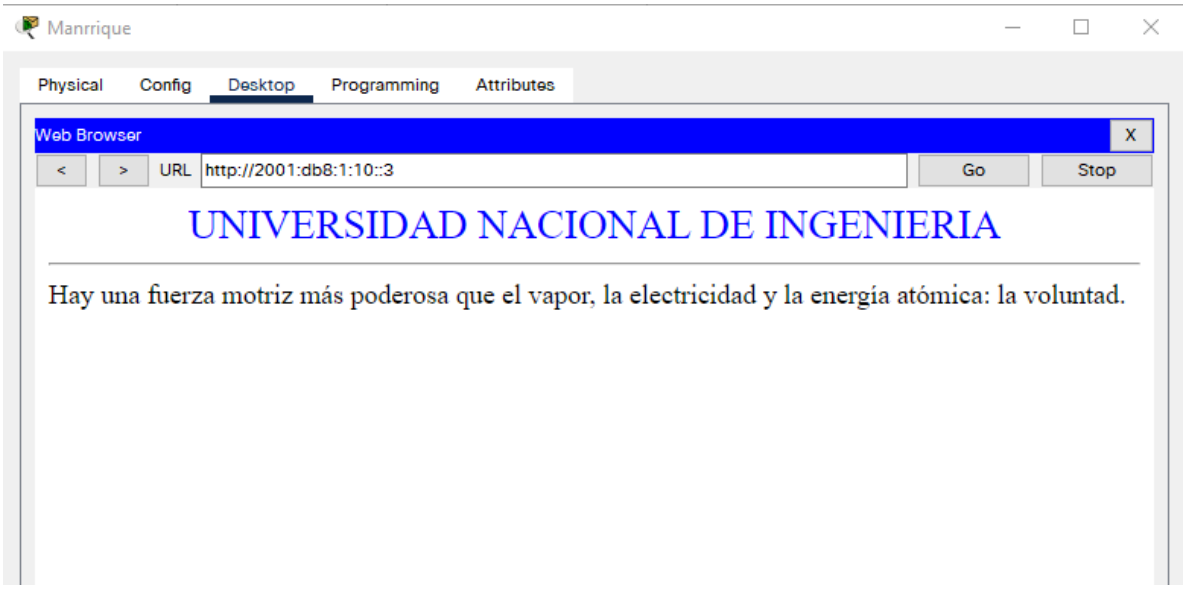

Ilustración 24. Verificación al servidor web por IPv6.

Verificaremos que el servidor web igual se puede acceder por medio del nombre configurado en servidor DNS lo cual completaremos cada una de las pruebas donde un mismo nodo puede configurarse en doble pila para la coexistencia de dichos protocolos.

5.5.3.3 Prueba al servidor web por medio nombre de dominio asociado al servidor DNS.

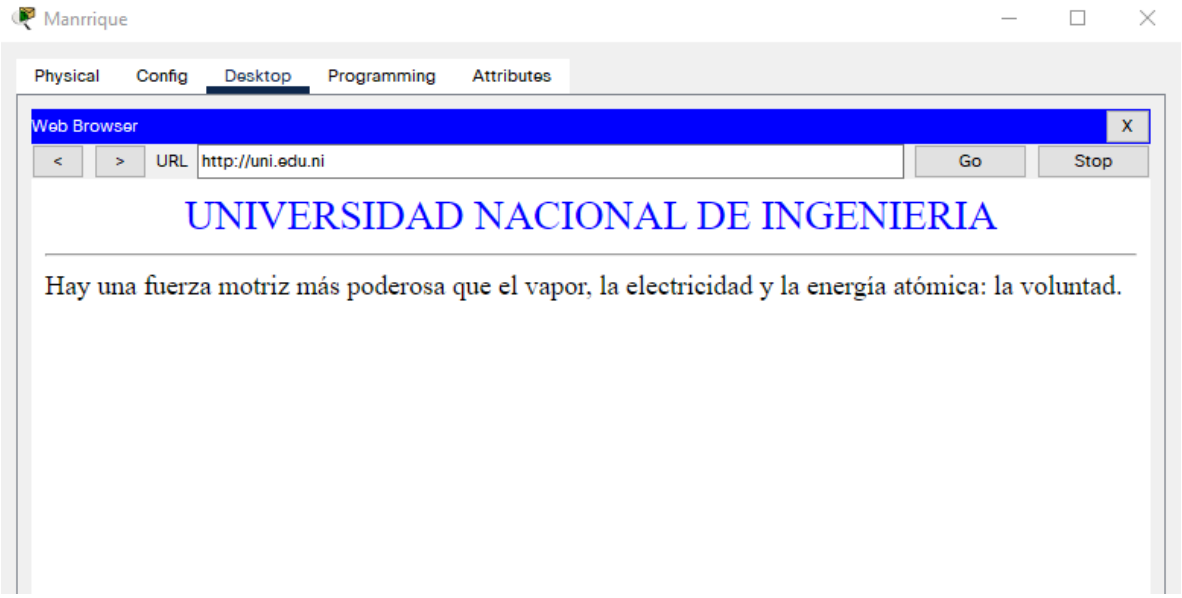

Ilustración 25. Verificación al servidor web por nombre de dominio.

5.6 Fase Act

Con base a los resultados obtenidos en las fases anteriores se demuestra de forma correcta el funcionamiento de la topología en el simulador de Cisco Packet Tracer en la coexistencia de ambos protocolos de internet tanto IPv4 como IPv6 permitiendo el tráfico de datos por ambos protocolos. Sin embargo, se detallarán algunos posibles problemas que podrían presentarse a la hora de implementar este proceso a una red física.

Abordaremos las posibles fallas que se pueden presentar al momento de implementar la red ya sean problemas de forma natural causada por el medio ambiente o problemas que pueden ocurrir causado por el ser humano y definiremos los posibles resultados estandarizados para mejorar y mantener la disponibilidad de la red.

Posibles Fallas	**Resolución de Fallas**
Inundaciones y terremotos.	• Copia de seguridad de las aplicaciones en la nube. • Cambio de equipos afectados. • Configuraciones de equipos afectados.
Vandalismo.	• Copia de seguridad de las aplicaciones en la nube. • Cambio de equipos afectados.
Amenazas externas por piratas informáticos.	• Actualización de programas de protección (firewalls). • Actualización de antivirus.
Amenazas internas por piratas informáticos.	• Políticas de seguridad interna. • Herramientas de ciberseguridad ej. (herramientas de actividad del

	usuario, solución de prevención de pérdidas de datos).
Conflictos de direcciones IP.	• Apagar el equipo del cliente DHCP en conflicto con el dispositivo de red que tiene la dirección IP estática. • En el servidor DHCP, excluir las direcciones IP del ámbito del intervalo de direcciones IP de DHCP. • Reinicie el equipo cliente DHCP.
Fallas en switches o routers.	• Reinicio del switch o router. • Verificar el sistema eléctrico donde se conectan los equipos. • Cambio de equipo.
Conectar equipos desordenadamente.	• Anticiparse al crecimiento de usuarios a nuestra red. • Reorganizar la red.
Tarjetas de red defectuosas.	• Verificación por medio del led integradas a los equipos. • Probar con otro tipo de cable para conectarse a la tarjeta. • Cambio de tarjeta de red.
Red de datos lenta.	• Insuficiente ancho de banda. • Cables en mal estado.
Errores DNS.	• Verificación de los DNS. • Cambio de DNS

Tabla 10. Planes de contingencia.

5.7 Conclusiones.

La propuesta de un marco de referencia para la transición del protocolo IPv4 al protocolo IPv6, nos ayudó a comprender que tan capaz esta la Facultad de Electrotecnia y computación para empezar con este proceso de cambio y saber las fortalezas y debilidades del área en estudio.

Como primer paso dentro de la planeación fue identificar los dispositivos y saber que tan preparados están para soportar las nuevas tecnologías y saber el porcentaje de equipos que están listo para comenzar con la transición, esta etapa nos dio a conocer que es tiempo para empezar a invertir paulatinamente en equipos capaces de soportar ambos protocolos para su funcionamiento.

La elaboración de la propuesta del esquema topológico de red se adecua fundamental en la ubicación de los equipos según el área de trabajo y con la posibilidad de expandirse lo cual lo hace un diseño escalable y confiable para un futuro de cambios en la topología.

Debido a que IPv4 está funcionando en gran porcentaje a nivel global la permanencia de este protocolo debe seguir en funcionamiento bajo este protocolo, por lo cual el mecanismo de transición Dual Stack es el método más práctico para la coexistencia con IPv6, ya que nos encaminamos a hacer uso del protocolo IPv6 de forma nativa y dejar en desuso el antiguo protocolo.

Con los estudios realizados en el presente proyecto se concluye que los equipos propuestos para la transición y el diseño topológico de red de la FEC se ajustan eficientemente al área para lograr en un futuro la implementación de este proyecto.

5.8 Recomendaciones.

1- Planear y preparar la red del área con dispositivos, sistema operativos y aplicaciones que estén realmente listo para adaptarse al nuevo cambio.

2- Impulsar la difusión de la investigación y formación sobre IPv6 en las demás áreas y en las pequeñas empresas, para fortalecer la cultura sobre el uso de este protocolo y poder compartir conocimientos sobre IPv6.

3- El establecimiento de este nuevo protocolo es una necesidad inmediata puesto que la mayoría de equipos y aplicaciones están siendo desarrollados bajo esta tecnología.

4- Emprender el proceso de migración pondría a la Universidad Nacional de Ingeniería en una posición de vanguardia y mostraría su capacidad no solo de adaptarse a la nueva tecnología si no también propiciar el adelanto tecnología en el país.

5- Para facilitar y estandarizar el proceso de transición, se debe realizar pruebas en los segmentos de red con menos equipos y usuarios que aprovechando la similitud de la red, permita afianzar y trasladar la implantación a segmentos de red cada vez más extensos y críticos.

6- La transición a IPv6 debe ir de la mano con la generación o adaptación de aplicaciones a IPv6, ya que no tiene sentido migrar la red si no se va hacer uso de las ventajas del protocolo IPv6.

6 Propuesta metodológica de transición de ipv4 a ipv6.

6.1 El problema

6.1.1 Formulación del problema.

Durante el desarrollo de la presente propuesta hemos mencionado la importancia no solo de estar a la vanguardia utilizando el protocolo IPv6, si no también funcionar con el protocolo IPv4 para evitar incompatibilidad con entidades que aun funcionen bajo este. Véase 5.1.1 Determinar el problema.

Así también detallamos la manera en la que trabajan actualmente las redes de la Universidad Nacional de Ingeniería.

Nótese que todo el caso de estudio está delimitado para la Facultad de Electrotecnia y Computación.

6.1.2 Revisión y análisis bibliográfico y documental.

En nuestra época es poco probable que una persona no se encontrara anteriormente con el mismo problema que deseamos solucionar, debido a esto es de suma importancia antes de comenzar a abordar la problemática realizar una investigación de trabajos relacionados a nuestro tema de interés. Esto lo facilita el común acceso a la información de la era en que vivimos, y nos transfiere experiencia y conocimientos empíricos de otros investigadores.

En este documento se toma como referencia una monografía, que por su contenido similar al propuesto será de gran ayuda en el proceso de transición en este proyecto. “Plan de transición del protocolo de red IPv4 a IPv6 basado en las recomendaciones realizadas por el MIN TIC Colombia”. (Fonseca Castro, 2017)

En este documento se hace mención de una serie de fases para la transición y la coexistencia de ambos protocolos de red bajo las normas impulsada por el Ministerio de Tecnologías de la Información y las comunicaciones de Colombia, en el cual se hace un planteamiento y diagnóstico para cumplir con las normas impuesta por el MIN TIC.

6.1.3 Objetivo de la investigación propuesta.

Generar documentación que sirva como una propuesta metodológica a la Universidad Nacional de Ingeniería para la transición de IPv4 a IPv6 a todas las áreas y recintos de nuestra alma mater.

6.2 Plan de trabajo

6.2.1 Consideraciones generales.

Para la generación de este documento no se requiere un formato específico, pero si es necesario que contenga los incisos de:

- Inventario de equipos finales.
- Inventario de equipos intermedios.
- Propuesta de compra de equipos para reemplazar los que no cumplen los requerimientos.
- Definición de recursos humanos y roles.
- Definición de tareas.
- Cronograma de tareas.
- Mapa topológico de la red en su estado antes de aplicar la migración.
- Mapa topológico de la red luego de la migración.

La información antes mencionada es considerada fundamental para realizar una migración de IPv4 a IPv6. Adicional a esta información, puede agregarse la que se crea pertinente dependiendo de si se desea configurar algo en particular para esta área de la Universidad Nacional de Ingeniería.

6.2.2 Etapas de trabajo, principales actividades de cada etapa.

Transición de infraestructura de servicios informáticos hacia ipv6	
Tareas	**Subtareas**
Recolección de información.	Realizar entrevistas con el personal técnico del nic.ni
	Obtener tabla con los modelos de los switches intermedios.
Inventario de equipos.	Solicitar acceso a las áreas afectadas por el alcance del proyecto.
	Extraer información necesaria por equipo. (Intermedio y final)
Valoración de inventario.	Comprobar si los equipos actuales cumplen con los requisitos necesarios para el proyecto.
Propuesta de equipos para sustituir los que no cumplen los requisitos.	Investigar los equipos que cumplen con los requisitos y realizar una propuesta de compra que satisfaga la relación costo/beneficio.
Realizar mapa topológico de la infraestructura actual.	Obtener previamente la información(ubicación) de los equipos (inventario)
	Realizar análisis de red.
	Creación de vlan en equipos intermedios.
	Administración de vlan mediante protocolo vtp (se centraliza).
	Crear sub interfaces para el transporte de datos de vlan en el enrutador.
	Encapsulamiento de vlan mediante protocolo dot1q.

	Configuración DHCP.
	Configurar servidor WEB.
	Configurar servidor dns.
Realizar mapa topológico de la infraestructura propuesta	Definición de tipo de topología.
	Modelado de nueva topología.
	Ejecución de metodología de migración. (Método Dual Stack).
	Configurar los servicios deseados en la nueva topología.
Realizar pruebas de la nueva topología para asegurar su funcionamiento.	Probar comunicación ipv4 e ipv6.
	Probar conexión DNS.
	Probar conexión hacia la web.

Tabla 11. Definición de tareas.

Véase: 5.2.2 Definición de secuencia de tareas.

En fase vista anteriormente se definen las tareas consideradas indispensables para lograr conseguir una migración de IPv4 a IPv6. Nótese que la persona encargada de aplicar este proceso en otra facultad de la Universidad Nacional de Ingeniería puede agregar tareas para representar una funcionalidad requerida por esta facultad y no es necesaria para la **FEC**.

6.2.3 Cronograma y control.

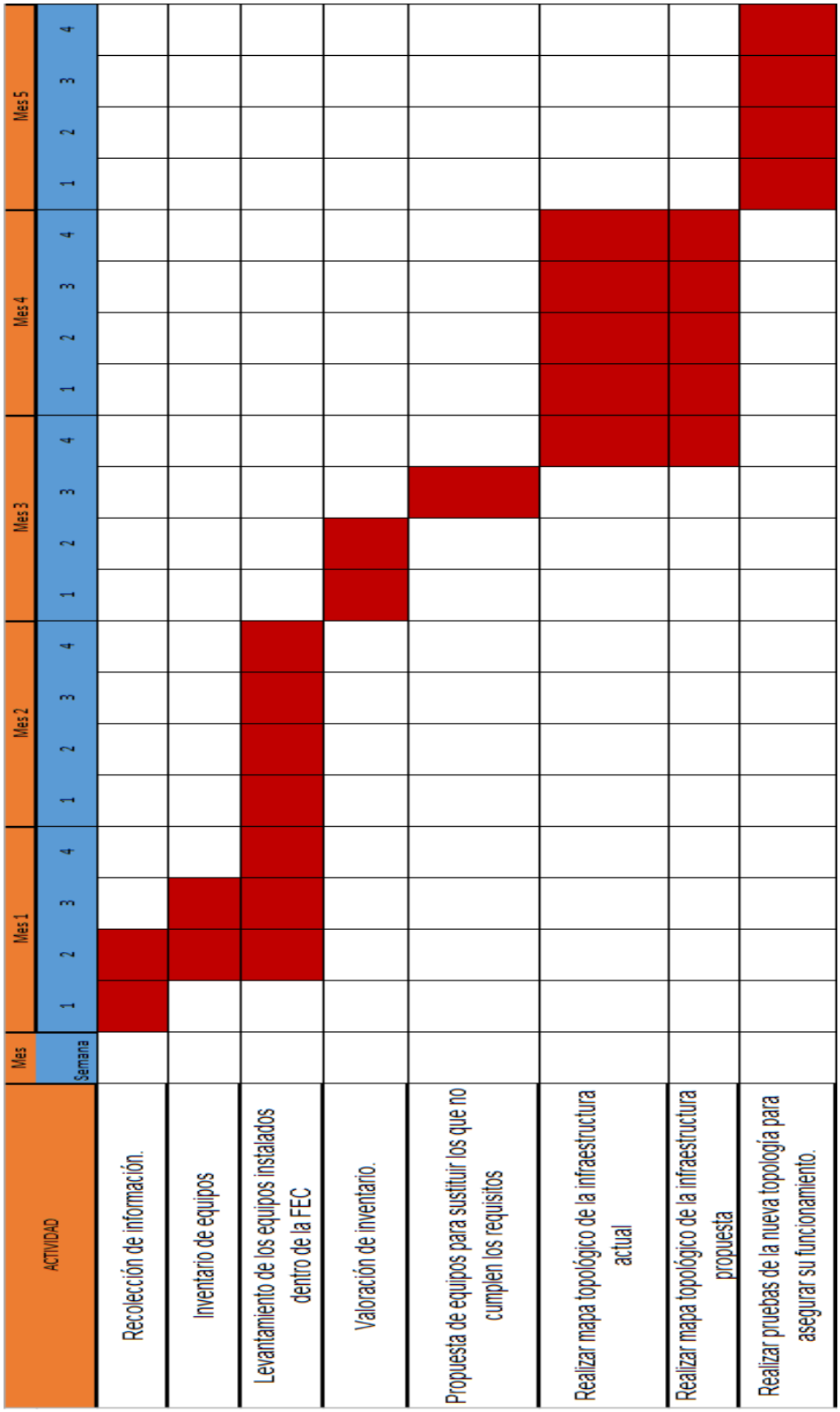

Ilustración 26 Cronograma de actividades.

6.3 Informes de avance e informe final.

6.3.1 Recursos

Para lograr culminar exitosamente la transición de protocolo IPv4 a IPv6 necesitamos definir los medios necesarios. Estos pueden ser materiales o personas que cumplen un rol único, irremplazable y sin el cual no podemos llegar a nuestro objetivo.

6.3.1.1 Humanos

Nombre Completo	Cargo	Función a realizar
Rodrigo Díaz Briseño	Responsable de oficina de servicios técnico Nic.ni	Entrega de información, excluyendo la considerada "información sensible"
Ronald Torres Torres	Decano FEC	Gestor de permisos de acceso.
Carlos Rodríguez	Responsable de infraestructura y soporte técnico Nic.ni	Proporcionar requerimientos técnicos de la red.

6.3.1.2 Locales, instalaciones, equipos y otros recursos

El área con la cual se trabajará en el presente documento es la Facultad de Electrotecnia y Computación (**FEC**) de la Universidad Nacional de Ingeniería. Esta está ubicada en el recinto Simón Bolívar.

En ella se encuentran distribuidos los equipos de interés para el presente trabajo, están ubicados las oficinas que conforman la **FEC** para que cada área, y la **FEC** por ende pueda cumplir con sus funciones. Los equipos de interés son:

Véase: 5.1.2.4 Dispositivos de cómputos finales.

También de relevancia: 5.1.2.3 Dispositivos intermediarios

6.3.1.3 Presupuesto

Véase: 5.1.2.7.1 Sugerencias de equipos para transición a ipv6.

7 BIBLIOGRAFÍA.

Bibliografía

aleashop. (s.f.). Obtenido de https://www.aleashop.es/blog/2019/07/05/direcciones-ip/

aleashop. (s.f.). Obtenido de https://www.aleashop.es/blog/2019/07/05/direcciones-ip/

ecured. (s.f.). Obtenido de https://www.ecured.cu/Redes_de_datos

ecured. (s.f.). Obtenido de https://www.ecured.cu/Cisco_Packet_Tracer

ediciones-eni. (s.f.). Obtenido de https://www.ediciones-eni.com/open/mediabook.aspx?idR=e70d8547ec2bce3ae6047eb1a880dbc9

en.wikipedia.org. (s.f.). en.wikipedia.org. Obtenido de en.wikipedia.org: https://en.wikipedia.org/wiki/IPv6

https://docs.oracle.com/. (s.f.). Obtenido de https://docs.oracle.com/cd/E19957-01/820-2981/ipv6-overview-10/index.html#:~:text=Una%20direcci%C3%B3n%20IPv6%20tiene%20un,las%20equis%20representan%20n%C3%BAmeros%20hexadecimales.

infotecs. (s.f.). Obtenido de https://infotecs.mx/blog/vlan.html

ionos.es. (s.f.). Obtenido de https://www.ionos.es/digitalguide/servidores/know-how/internet-protocol-definicion-y-fundamentos/

lacnic.net. (s.f.). Obtenido de https://www.lacnic.net/545/1/lacnic/2-direcciones-ipv4

nic.cr. (s.f.). Obtenido de https://www.nic.cr/ipv6/transicion

pdcahome. (s.f.). Obtenido de https://www.pdcahome.com/5202/ciclo-pdca/

sites.google. (s.f.). sites.google. Obtenido de sites.google: https://sites.google.com/site/sergioticobachillerato/6-otros-protocolos/a-protocolo-dhcp-definicion-y-funcion

sites.google. (s.f.). sites.google. Obtenido de sites.google: https://sites.google.com/site/redes3isi/unidad-4/4-1-que-es-el-vtp

sites.google.com. (s.f.). Obtenido de https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-

arquitectura-tcp-ip/7-nivel-de-red/8-direccionamiento-ipv6/6-transicion-de-ipv4-a-ipv6

speedcheck. (s.f.). Obtenido de https://www.speedcheck.org/es/wiki/ipv4/

tecnoinformatic. (s.f.). Obtenido de https://tecnoinformatic.com/c-informatica-basica/tipos-de-topologias-de-red-y-sus-caracteristicas/

webempresa. (s.f.). Obtenido de webempresa: https://www.webempresa.com/hosting/que-es-servidor-web.html

wikipedia. (s.f.). Obtenido de https://es.wikipedia.org/wiki/Red_privada

ANEXOS

Configuración cli de los switches en cisco packet tracer.

A continuación, se mostrará la configuración del switch server.

Switch>enable
Switch#
Switch#configure terminal
Switch(config)#
Switch(config)#enable password fec
Switch(config)#line console 0
Switch (config-line)#password 12345
Switch (config-line)#login
Switch (config-line)#exit
Switch(config)#service password-encryption
Switch(config)#hostname SW-SERVER
SAREC-FEC(config)#no ip domain-lookup
SW-SERVER(config)#vtp mode server
SW-SERVER(config)#vtp domain FEC
SW-SERVER(config)#vtp password fec
SW-SERVER(config)#vlan 10
SW-SERVER(config-vlan)#name LEYDA
SW-SERVER(config-vlan)#vlan 20
SW-SERVER(config-vlan)#name REDES
SW-SERVER(config-vlan)#vlan 30
SW-SERVER(config-vlan)#name ASA
SW-SERVER(config)#vlan 40
SW-SERVER(config-vlan)#name SAREC-FEC
SW-SERVER(config-vlan)#vlan 50
SW-SERVER(config-vlan)#name SECRETARIA-FEC
SW-SERVER(config-vlan)#vlan 60
SW-SERVER(config-vlan)#name Dpto-EO

SW-SERVER(config-vlan)#vlan 70
SW-SERVER(config-vlan)#name LAB-ELECTRICA
SW-SERVER(config-vlan)#exit
SW-SERVER(config)#int range fastEthernet 0/1-2
SW-SERVER(config-if-range)#switchport mode trunk
SW-SERVER(config-if-range)#end
SW-SERVER#write

A continuación, se mostrará la configuración de uno de los switches de acceso.

Switch>enable
Switch#configure terminal
Switch(config)#
Switch(config)#enable password fec
Switch(config)#line console 0
Switch (config-line)#password 12345
Switch (config-line)#login
Switch (config-line)#exit
Switch(config)#
Switch(config)#service password-encryption
Switch(config)#Hostname SAREC-FEC
SAREC-FEC(config)#
SAREC-FEC(config)#no ip domain-lookup
SAREC-FEC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SAREC-FEC(config)#vtp domain FEC
Domain name already set to FEC.
SAREC-FEC(config)#vtp password fec
Setting device VLAN database password to fec
SAREC-FEC(config)#interface fastethernet0/24
SAREC-FEC(config-if)#switchport mode trunk
SAREC-FEC(config-if)#exit

SAREC-FEC(config)#
SAREC-FEC(config)#interface range fastethernet0/1-23
SAREC-FEC(config-if-range)#switchport access vlan 40
SAREC-FEC(config-if-range)#end
SAREC-FEC#wr

Configuración del enrutador.

Los siguientes comandos son realizados en la cli del equipo. Se hace referencia solo a la configuración de uno de los equipos que dan acceso a la red tanto en IPv6 como IPv4.

router>enable
router#
router#configure terminal
router(config)#
router(config)#no ip domain-lookup
router(config)#hostname NUCLEO
NUCLEO(config)#enable password fec
NUCLEO(config)#line console 0
NUCLEO(config-line)#password 12345
NUCLEO(config-line)#login
NUCLEO(config-line)#exit
router(config)#
NUCLEO(config)#service password-encryption
NUCLEO(config)#banner motd 'INGRESE LAS CLAVES DE SEGURIDAD DEL ROUTER PARA INGRESAR'
NUCLEO(config)#ipv6 unicast-routing
NUCLEO(config)#ipv6 dhcp pool SAREC-FEC
NUCLEO(config-dhcpv6)#address prefix 2001:db8:1:4::/64
NUCLEO(config-dhcpv6)#address prefix 2001:db8:1:4::/64 lifetime 3600 3600
NUCLEO(config-dhcpv6)#domain-name sarec-fec.com

```
NUCLEO(config-dhcpv6)#dns-server 2001:db8:1:10::2
NUCLEO(config-dhcpv6)#exit
NUCLEO(config)#
NUCLEO(config)#interface fastEthernet 0/0.4
NUCLEO(config-subif)#
NUCLEO(config-subif)#encapsulation dot1Q 40
NUCLEO(config-subif)#ipv6 enable
NUCLEO(config-subif)#ipv6 address 2001:db8:1:4::1/64
NUCLEO(config-subif)#ipv6 dhcp server SAREC-FEC
NUCLEO(config-subif)#ipv6 nd managed-config-flag
NUCLEO(config-subif)#end
NUCLEO#
NUCLEO#write
NUCLEO#configure terminal
NUCLEO(config)#ip dhcp pool 4
NUCLEO(dhcp-config)#network 10.5.25.0 255.255.255.0
NUCLEO(dhcp-config)#default-router 10.5.25.1
NUCLEO(dhcp-config)#dns-server 10.5.10.2
NUCLEO(dhcp-config)#domain-name sarec-fec
NUCLEO(dhcp-config)#exit
NUCLEO(config)#
NUCLEO(config)#interface fastEthernet 0/0.4
NUCLEO(config-subif)#ip address 10.5.25.1 255.255.255.0
NUCLEO(config-subif)#end
NUCLEO(config)#
NUCLEO(config)#write
```

Ilustración 27. Switch de acceso ubicado en el departamento ASA.

Ilustración 28. Switch de acceso ubicado en el laboratorio de REDES.

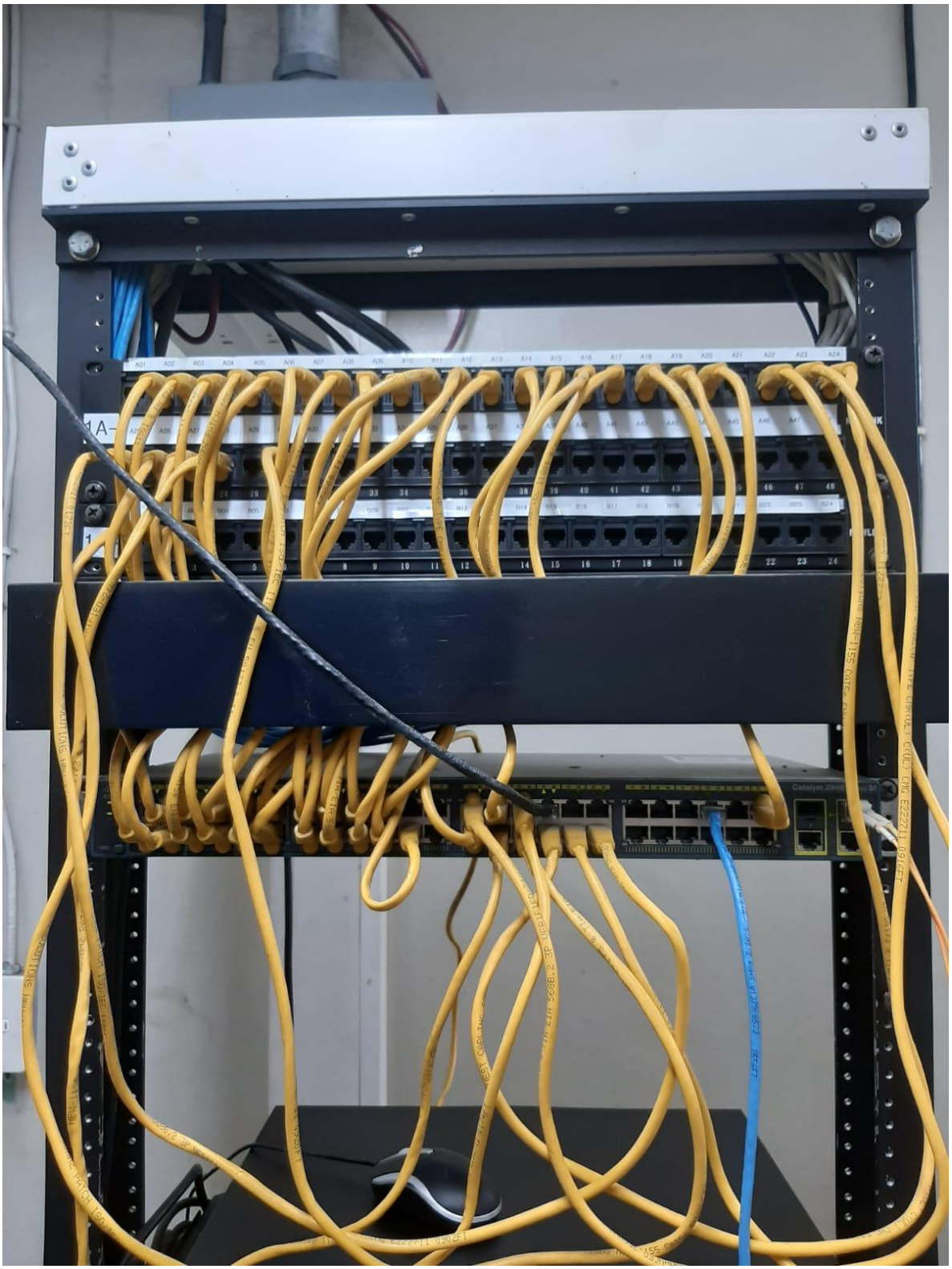

Ilustración 29. Switch de acceso ubicado en el laboratorio Leyda Montenegro.

Managua, 22 de junio del 2021.

Ing. Ronald Torres.
Decano FEC.
Universidad Nacional de Ingeniería.
Su Oficina.

Estimado **Ing. Torres**, de la manera más atenta solicitamos **su autorización para el ingreso de oficinas, departamentos y laboratorios de la Facultad de Electrotecnia y Computación** para hacer un levantamiento de inventario de equipos que permiten la comunicación de Redes de datos. Tal información es de suma importancia para la realización de nuestro tema monográfico que lleva como nombre **"Propuesta de un Marco de Referencia para la Transición del Protocolo IPv4 al Protocolo IPv6 mediante el método Dual Stack caso de estudio Facultad de Electrotecnia y computación (FEC) UNI-RUSB."**

Con el levantamiento solicitado será gran ayuda para generar una Documentación sobre el uso de los equipos y que tan actualizados están para soportar las nuevas tecnologías que diariamente están en constante cambio.

Toda la información generada será de gran referencia para la Universidad Nacional de Ingeniería.

Agradeciendo su atención y colaboración.
Atentamente,

Br. Heymer Manrrique Duarte Lagos.
Carnet: 2011-36558

VoBo

MSc Jorge Prado D.
Tutor

Ilustración 30. Solicitud de ingreso al área en estudio.

Managua, 02 de julio del 2021.

Ing. Rodrigo Díaz.
Responsable Área Técnica.
Dirección Nic.ni
Su Oficina.

Estimado **Ing. Díaz**, de la manera más atenta solicitamos **su autorización para la aprobación de una entrevista con personal técnico capacitado que nos puedan ayudar con información de los siguientes puntos:**

- **Levantamiento de equipos intermediarios de red que posee la FEC y su conexión con el router principal.**
- **Equipos intermediarios que soportan IPv6.**
- **Que equipo intermediario conecta las diferente oficinas y laboratorios de la FEC.**
- **Tipos de cableados utilizados para la conexión.**

Tal información es de suma importancia para la realización de nuestro tema monográfico que lleva como nombre **"Propuesta de un Marco de Referencia para la Transición del Protocolo IPv4 al Protocolo IPv6 mediante el método Dual Stack caso de estudio Facultad de Electrotecnia y computación (FEC) UNI-RUSB."**

Con el levantamiento solicitado será gran ayuda para generar una Documentación sobre el uso de los equipos y que tan actualizados están para soportar las nuevas tecnologías que diariamente están en constante cambio.

Toda la información generada será de gran referencia para la Universidad Nacional de Ingeniería.

Agradeciendo su atención y colaboración.
Atentamente,

Br. Heymer Manrrique Duarte Lagos.
Carnet: 2011-36558

UNIVERSIDAD NACIONAL DE INGENIERÍA
DIRECCIÓN NIC.NI
.ni RECIBIDO
FECHA: 2/07/2021
HORA: 9:57 am.
NOMBRE: JUDITH V.

VoBo

MSc Jorge Prado D.
Tutor

Ilustración 31. Solicitud de información a la nic.ni