Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

IMPLEMENTACIÓN DE LA VERSIÓN 6 DEL PROTOCOLO IP EN LA RED CONVERGENTE DE VOZ Y DATOS DE FUNDACIÓN KINAL

Juan Francisco Herrera
Asesorado por el Ing. Ivan Ernesto Apopa Soto

Guatemala, enero de 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE LA VERSIÓN 6 DEL PROTOCOLO IP EN LA RED CONVERGENTE DE VOZ Y DATOS DE FUNDACIÓN KINAL

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JUAN FRANCISCO HERRERA
ASESORADO POR EL ING. IVAN ERNESTO APOPA SOTO

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO ELECTRÓNICO

GUATEMALA, ENERO DE 2014

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Inga. Elvia Mirian Ruballos Samayoa
VOCAL IV	Br. Walter Rafael Véliz Muñoz
VOCAL V	Br. Sergio Alejandro Donis Soto
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Ivan Ernesto Apopa Soto
EXAMINADOR	Ing. Kenneth Issur Estrada Ruiz
EXAMINADOR	Ing. Byron Odilio Arrivillaga Méndez
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

IMPLEMENTACIÓN DE LA VERSIÓN 6 DEL PROTOCOLO IP EN LA RED CONVERGENTE DE VOZ Y DATOS DE FUNDACIÓN KINAL

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha junio de 2012.

Juan Francisco Herrera

Guatemala 22 de octubre de 2013

Ing. Juan Merk Cos
Unidad de Ejercicio Profesional Supervisado
Facultad de Ingeniería
Su despacho

Por este medio me permito dar aprobación al Trabajo de Graduación titulado: **IMPLEMENTACIÓN DE LA VERSIÓN 6 DEL PROTOCOLO IP EN LA RED CONVERGENTE DE VOZ Y DATOS DE FUNDACIÓN KINAL,** desarrollado por el estudiante **Juan Francisco Herrera** con carné no. **93-12967,** ya que considero que cumple con los requisitos establecidos, por lo que el autor y mi persona somos responsables del contenido y conclusiones del mismo.

Sin otro particular, aprovecho la oportunidad para saludarlo,

Atentamente,

ING. IVAN ERNESTO APOPA
COLEGIADO 6663

Ing. Ivan Ernesto Apopa Soto
ASESOR
iapopa@gmail.com

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Ref. EIME 89. 2013
Guatemala, 28 de OCTUBRE 2013.

Señor Director
Ing. Guillermo Antonio Puente Romero
Escuela de Ingenierìa Mecànica Elèctrica
Facultad de Ingenierìa, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: IMPLEMENTACIÓN DE LA VERSIÓN 6 DEL PROTOCOLO IP EN LA RED CONVERGENTE DE VOZ Y DATOS DE FUNDACIÓN KINAL, del estudiante Juan Francisco Herrera, que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Carlos Eduardo Guzmán Salazar
Coordinador Área Electrónica

sro

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

UNIDAD DE EPS

Guatemala, 21 de noviembre de 2013.
Ref.EPS.DOC.1258.11.13.

Ing. Juan Merck Cos
Director Unidad de EPS
Facultad de Ingeniería
Presente

Estimado Ingeniero Merck Cos.

Por este medio atentamente le informo que como Supervisor de la Práctica del Ejercicio Profesional Supervisado (E.P.S.), del estudiante universitario **Juan Francisco Herrera** de la Carrera de Ingeniería Electrónica, **con carné No. 9312967 ,** procedí a revisar el informe final, cuyo título es **"IMPLEMENTACIÓN DE LA VERSIÓN 6 DEL PROTOCOLO IP EN LA RED CONVERGENTE DE VOZ Y DATOS DE FUNDACIÓN KINAL".**

En tal virtud, **LO DOY POR APROBADO**, solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,

"Id y Enseñad a Todos"

Ing. Kenneth Issur Estrada Ruiz
Supervisor de EPS
Área de Ingeniería Eléctrica

Universidad de San Carlos de Guatemala
ASESOR(A)-SUPERVISOR(A) DE EPS
Unidad de Prácticas de Ingeniería y EPS
Facultad de Ingeniería

c.c. Archivo
KIER/ra

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

UNIDAD DE EPS

Guatemala 21 de noviembre de 2013.
Ref.EPS.D.839.11.13.

Ing. Guillermo Antonio Puente Romero
Director Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería
Presente

Estimado Ingeniero Puente Romero.

Por este medio atentamente le envío el informe final correspondiente a la práctica del Ejercicio Profesional Supervisado, (E.P.S) titulado **"IMPLEMENTACIÓN DE LA VERSIÓN 6 DEL PROTOCOLO IP EN LA RED CONVERGENTE DE VOZ Y DATOS DE FUNDACIÓN KINAL"** que fue desarrollado por el estudiante universitario, **Juan Francisco Herrera,** quien fue debidamente asesorado por el Ing. Iván Ernesto Apopa Soto y supervisado por el Ing. Kenneth Issur Estrada Ruiz.

Por lo que habiendo cumplido con los objetivos y requisitos de ley del referido trabajo y existiendo la aprobación del mismo por parte del Asesor y del Supervisor de EPS, en mi calidad de Directora apruebo su contenido solicitándole darle el trámite respectivo.

Sin otro particular, me es grato suscribirme.

Atentamente,
"Id y Enseñad a Todos"

Ing. Juan Merck Cos
Director Unidad de EPS

Universidad de San Carlos de Guatemala
DIRECCIÓN
Unidad de Prácticas de Ingeniería y EPS
Facultad de Ingeniería

JMC/ra

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 89. 2013.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; JUAN FRANCISCO HERRERA titulado: IMPLEMENTACIÓN DE LA VERSIÓN 6 DEL PROTOCOLO IP EN LA RED CONVERGENTE DE VOZ Y DATOS DE FUNDACIÓN KINAL, procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romero

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 25 DE NOVIEMBRE 2,013.

Universidad de San Carlos
De Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.D.0023-2014

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al trabajo de graduación titulado: **IMPLEMENTACIÓN DE LA VERSIÓN 6 DEL PROTOCOLO IP EN LA RED CONVERGENTE DE VOZ Y DATOS DE FUNDACIÓN KINAL,** presentado por el estudiante universitario: **Juan Francisco Herrera,** autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, enero de 2014

/cc

ACTO QUE DEDICO A:

Dios	Por darme la vida, la fuerza y la perseverancia para poder alcanzar este triunfo.
Mis abuelos	Braulia Telón y Faustino Herrera (q.e.p.d.), porque me hubiera encantado poder compartir este triunfo con ellos.
Mi madre	María Florencia Herrera, por todos los sacrificios económicos que realizó para brindarme la oportunidad de ser un ingeniero.
Mi tía	María Cruz Herrera (q.e.p.d.) por todas sus enseñanzas y cariño.
Mi esposa	Melanea del Carmen Solares, por su apoyo incondicional.
Mis hijos	Rodrigo Alexander, Christian Francisco y Andrea Eunice Herrera Solares, ustedes son mi vida.
Familia	Sandoval Valenzuela, por ser una importante influencia en mi carrera, entre otras cosas.

AGRADECIMIENTOS A:

Dios	Por cuidarme en todo momento y ser fuente de sabiduría.
Mi familia	Por su apoyo incondicional.
Mis tíos y primos	Por su cariño y comprensión.
Ingenieros	Ivan Apopa, Mariano Llarena, Guillermo Puente, Gabriel Tuquer, por la asesoría brindada para la elaboración de este trabajo, su apoyo y amistad.
Señor	Aldo Hernández, por su apoyo incondicional.
Escuela de Ingeniería Mecánica Eléctrica	Por haberme inculcado la educación superior y ayudarme a ser una mejor persona y un buen profesional.
Fundación Kinal	Por abrirme las puertas y darme el apoyo necesario para realizar este trabajo de graduación.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

ARP Address Resolution Protocol (Protocolo de resolución de direcciones).

ARPANET Red de Centros de investigación, antecesor de Internet.

Cabecera Información que suele situarse delante de los datos y que hace referencia a diferentes aspectos de estos.

Capa Cada una de los elementos que conforman una estructura jerárquica.

CIDR Classless Interdomaing Routing (Enrutamiento entre dominios sin clase).

Datagrama Conjunto de estructurado de bytes que forma la unidad básica de comunicación del protocolo IP.

DHCP Dynamic *Host* Configuration Protocol, es un servidor que asigna dinámicamente direcciones a los *host* que se encuentran conectados dentro de una organización.

DNS Domain Named System, es un servidor que

	permite asignar un nombre a una determinada dirección para facilitar el uso para la conectividad, en el caso de IPv6 facilita el poder dar un nombre a una dirección IPv6.
Dual-stack	Método de transición de IPv4 a IPv6, el cual indica que un equipo puede tener ambos direccionamientos.
Encabezado (*Header*)	Información que suele situarse delante de los datos (por ejemplo en una transmisión) y que hace referencia a diferentes aspectos de estos.
Encapsulamiento	Sistema basado en colocar una estructura dentro de otra formando capas.
Firewall	Máquina encargada del filtrado del tráfico de Internet, basado en reglas de comportamiento.
Gateway	Es aquel que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. El propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.
ICMP	Protocolo encargado de la comunicación de mensajes entre nodos conectados a la Internet.
IEEE	Institute of Electrical and Electronics Engineers.

IP	El Internet Protocol; es un protocolo no fiable y sin conexión en el que se basa la comunicación por Internet. La unidad es el datagrama.
IPsec	Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.
ISO	International Organization for Standarization (Organización Internacional para la Normalización).
ISP	Internet Service Provider (Proveedor de servicios de Internet)
IPv4	Es la abreviatura escogida por la IETF con la que se denomina a la versión 4 del protocolo IP.
IPv6	Es la abreviatura escogida por la IETF con la que se denomina a la versión 6 del protocolo IP.
LAN	(Local Área Network): red local. Red que está bajo una misma administración

MAC	Media Access Control (Control de acceso al medio).
MAC *Address*	Dirección única que llevan las tarjetas de red grabadas en una *ROM* para identificarse y diferenciarse de las demás.
MTU	Máximun Transmissión Unit (Unidad máxima de transmisión).
NIC	Network Interface Card (Tarjeta de Interfaz de red).
OSI	Modelo teórico propuesto por IEEE que describe cómo deberían conectarse distintos modelos de ordenadores a diferentes tipos de red para poder comunicarse entre sí.
Overhead	Pérdida de rendimiento o sobrecarga.
Paquetes IP	El paquete lleva los datos en los protocolos que Internet utiliza, que es TCP/IP (Transmission Control Protocol/Internet Protocol). Cada paquete contiene parte del cuerpo del mensaje.
Protocolos	Conjunto de reglas que establece cómo debe realizarse una comunicación.

RFC	(Request For Comments): Documento de especificaciones que se expone públicamente para su discusión.
Router	Dispositivo físico u ordenador que conecta dos o más redes encargado de direccionar los distintos datagramas que le lleguen hacia el destino.
Routing	Procedimiento que consiste en conducir un datagrama hacia el destino a través de Internet.
TCP	(Transmission Control Protocol): Protocolo de nivel superior que permite una conexión fiable y orientada a conexión mediante el protocolo *IP*.
Tunneling	Encapsulado de un protocolo IPv6 dentro de un protocolo IPv4 y viceversa.
UDP	(User Datagram Protocol): Protocolo no fiable y sin conexión basado en el protocolo IP.
VLAN	(Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.
WAN	Red administrada por diferentes organizaciones.
WIN	Microsoft Windows.

RESUMEN

Este trabajo de graduación presenta el desarrollo e implementación de un prototipo de red y un plan piloto para la transición de la red actual de Fundación Kinal basada en protocolo IPv4 a una red IPv6.

En la fase de investigación se da a conocer la trayectoria de Fundación Kinal, con el fin de entender la labor social que la misma realiza.

A través de la fase de servicio técnico profesional se investigó en qué consiste el nuevo protocolo de IPv6, y con base a lo encontrado determinar el método de transición recomendado que debe seguir Fundación Kinal para migrar a IPv6 y además, ver todo lo referente a configuración de equipos de red y equipos de usuario final.

Durante esta segunda fase se utilizó un prototipo de red para probar las configuraciones y un plan piloto que tomó en cuenta la infraestructura de la red actual y los procesos que intervienen sobre ella para demostrar la funcionalidad.

La fase de enseñanza aprendizaje se enfocó en dar a conocer al personal encargado de la red de Kinal cómo se debe configurar este nuevo protocolo en diferentes sistemas operativos.

Los resultados indicaron que la transición no afecta a la plataforma actual de IPv4, gracias al protocolo *dual stack* estas plataformas pueden coexistir sin la necesidad de una migración brusca.

OBJETIVOS

General

Realizar una propuesta de implementación de un plan piloto del protocolo de red IP en la versión 6 de forma paralela a la versión 4 del mismo, de forma que provea un manejo eficiente de las aplicaciones utilizadas en la red de Fundación Kinal.

Específicos

1. Dar a conocer la información general de Fundación Kinal.

2. Presentar los fundamentos del Protocolo de Internet en la versión 6.

3. Analizar la situación actual de la red de voz y datos de Fundación Kinal.

4. Estudiar los distintos escenarios de implementación fundamentados en las estrategias de coexistencia.

5. Presentar una propuesta para el diseño del plan piloto.

INTRODUCCIÓN

El crecimiento de la cantidad de usuarios que ha tenido Internet durante los últimos años no solo en el país, sino que a nivel mundial, el cual se ha desarrollado sobre el protocolo de direcciones de Internet en la versión 4 (IPv4), ha provocado que estas direcciones se estén agotando, cosa que muchos ignoran y otros consideran que pasará mucho tiempo para que se haga necesario migrar a la nueva versión la cual está disponible desde hace varios años y los primeros en implementarlo han sido los países asiáticos.

En el caso de Guatemala la Fundación Kinal quiere preparar la red convergente de voz y datos para esta nueva versión del protocolo IP, es decir IP versión 6.

Para poder lograr este cambio primero se debe entender cómo funciona la red de voz y datos y de Fundación Kinal.

El presente trabajo se enfocará en obtener el diagrama del modelo actual de la red y de ser necesario proponer un modelo como el Empresarial de Cisco que facilita la escalabilidad y el crecimiento futuro de la red, se realizará un estudio de aplicaciones utilizadas así como la cantidad de recursos de red que se necesita. Se propondrá un prototipo de red mediante el cual se realizarán pruebas de laboratorio con las diferentes estrategias disponibles en la actualidad para determinar la que mejor se adapte a Fundación Kinal, para finalmente crear un plan piloto que permita la migración e implementación de las 250 computadoras que componen la red a la versión 6 de IP (IPv6)

.

1. FASE DE INVESTIGACIÓN

1.1. Información general de la institución

Fundación Kinal es una institución sin fines de lucro, la función principal es brindar una educación de calidad a jóvenes y adultos.

1.1.1. Misión de la institución

“Formar a jóvenes y adultos a través de una educación integral, con énfasis en las áreas técnicas y tecnológicas, influyendo positivamente en el trabajo, la familia y la sociedad”.

1.1.1.1. Visión de la institución

“Ser líderes en la formación técnica, tecnológica y humana de la región, brindando una excelente preparación integral a jóvenes y adultos, logrando la superación personal y profesional”.

1.1.2. Reseña histórica

Fundación Kinal se ubicó en varias zonas de la ciudad capital, hasta establecerse de forma definitiva en la sede actual.

1.1.2.1. Ubicación inicial

1961 – 1963

Surgió en 1961 como un Club Cultural y Deportivo. La sede se encontraba ubicada en la cabecera del municipio de Mixco, atendiendo actividades deportivas, de formación humana y espiritual; estas se llevaban a cabo en fin de semana y estaban dirigidas a obreros adultos.

1964 - 1966

En este año se trasladó la sede a la zona 4 de la ciudad capital, próxima a la terminal de autobuses. La localización facilitó que se iniciaran actividades entre semana, aumentando así la participación de personas de otros lugares de la ciudad. A la vez que continuaron las actividades deportivas, de formación humana y espiritual se iniciaron conjuntamente los cursos de carpintería, mecánica automotriz y electricidad.

1967 – 1970

La siguiente sede fue en la calle Martí en zona 6 de la ciudad. Se agregaron nuevos cursos con orientación laboral: albañilería y relaciones humanas.

1971 – 1983

Nuevamente la sede tuvo movimiento, esta vez hacia la zona tres de la ciudad capital. En estos años se desarrollaron actividades en la zona 3 de la ciudad, en un local proporcionado por la Fundación Camhi, próximo al basurero

municipal. Aquí se iniciaron contactos estables con empresas que enviaron al personal a los cursos de capacitación. Se promovió la participación en actividades deportivas y el programa de formación humana y doctrinal abarcó cursos de orientación matrimonial y educación de los hijos. El 70 % de los participantes era proveniente de la capital y el 30 % de los municipios de Guatemala y departamentos.

1984

Desde abril se trasladó a una sede localizada en la 3a. avenida y 10 calle de la zona 1. En el programa de capacitación de obreros se realizaron actividades de formación profesional como pilotos de transporte pesado, electricistas industriales, lubricadores de maquinaria, bodegueros, mensajeros, vendedores, cobradores, etc. Además, se promovieron cursos de desarrollo personal, administrativo, superación personal y familiar, que buscan mejorar las actitudes ante el trabajo, la familia y la comunidad social donde se desenvuelven.

1.1.2.2. Constitución del patronato

1985

Se constituyó un grupo promotor de Kinal para transformarlo en un centro educativo, dando principal atención a la capacitación técnica, iniciando las gestiones para la adquisición de un terreno en donde construir una sede definitiva.

1.1.2.3. onación de terreno para la sede actual

1986

Se recibió en donación un terreno, otorgado por el Ing. Juan Mini Feltrín, localizado en la 6ta avenida 13-54 de la zona 7, colonia Landívar, y se inició la recaudación de fondos para la construcción de la nueva sede.

1987

Se constituyó la Fundación Kinal, aprobada por el Acuerdo Gubernativo 973-87 el 5 de noviembre de 1987.

1988 – 1991

En enero de 1988 se trasladó Kinal a nuevos edificios con un área de 2,000 m^2, con talleres, aulas, biblioteca, auditórium, sala y cafetería, oratorio, oficinas, servicios generales, clínica médica, odontológica e instalaciones deportivas.

1992 – 1993

Se diversifican los programas con la autorización del Ministerio de Educación para impartir clases de bachillerato, las cuales se ofrecen a los alumnos jóvenes junto con una carrera técnica y sé continua impartiendo cursos para obreros y personal que labora en empresas.

1994

Se realiza una ampliación de instalaciones físicas de 3 000 m^2 con talleres, laboratorios, aulas y posteriormente se mejora el pensum de estudios en el cual los alumnos obtienen un perito técnico. Se inicia un trabajo de equipamiento de los talleres y laboratorios de electricidad, electrónica y automatización, mecánica automotriz, refrigeración y soldadura. Además, se consigue dotar una biblioteca técnica y un laboratorio de computación.

1995 – 2000

Con ayuda de organismos internacionales se logra equipar los talleres de electrónica industrial, electricidad industrial e informática.

2001

La Facultad de Ingeniería de la Universidad de San Carlos de Guatemala calificó a Kinal como el centro educativo con el mejor resultado de admisión.

2002

Con el aval de la Universidad del Istmo se incluye en los programas de capacitación, el grado de Técnico Universitario en Electricidad y Electrónica.

Fundación Kinal introduce en los programas del centro educativo y Escuela Técnica Superior capacitación en redes proporcionada por Cisco Systems, convirtiéndose en una academia local de Cisco Networking Academy.

Los cursos están basados en brindar las herramientas y conocimientos necesarios para que los participantes puedan lograr la certificación internacional. CCNA, en los principios y prácticas del diseño, instalación, configuración y mantenimiento de redes de computadoras.

2003 – 2004

Actualmente se atiende personas de los departamentos de Guatemala, Escuintla, Chimaltenango y Sacatepéquez. Dentro del departamento de Guatemala hay beneficiarios de los municipios de Mixco, Villa Nueva, Villa Canales, Santa Catarina Pínula, Chinautla.

Kinal, significa en lengua maya lugar donde nace el fuego y desde el inicio de las actividades, son más de 20 000 las personas que se han beneficiado de las actividades de formación técnico laboral y de formación humana, espiritual, cultural y deportiva. A través de los cursos impartidos a técnicos se han beneficiado varios cientos de empresas.

2005 a la fecha

Se ampliaron las instalaciones llegando a tener 11 000 metros cuadrados de construcción.

Número de empleados: 120

1.1.3. Servicios que presta

Kinal es un centro educativo privado, no lucrativo, dirigido a la formación técnica profesional de jóvenes y adultos. Cuyo valor fundamental es enseñar a realizar el trabajo bien hecho, que sea la base de la superación de los alumnos y el medio para servir a los demás.

Para lograr lo anterior Fundación Kinal cuenta con tres escuelas: centro educativo Técnico Laboral, Escuela Técnica Superior, unidad de capacitación en Tecnología de la Información. Actualmente cuenta con 13 600 m^2, de los cuales se han construido 12 000 m^2, cuenta con 7 edificios con 16 talleres, 30 aulas, 7 laboratorios, 1 biblioteca, 2 auditórium, 2 oratorios, 4 salas de atención personalizada y cafetería. También cuenta con instalaciones deportivas.

La oferta educativa que se ofrece en Kinal se puede dividir en educación formal e informal.

La educación formal cubre las siguientes etapas:

- Educación secundaria
- Educación media
- Técnicos universitarios

En educación informal cubre lo siguiente:

- Carreras técnicas
- Cursos de preparación para certificaciones internacionales

1.1.3.1. Educación secundaria

La etapa de educación secundaria es un programa diseñado especialmente para cubrir las necesidades de formación y desarrollo personal de jóvenes de 12 a 15 años. Se trata de un programa completo y coherente que proporciona un marco de desarrollo académico, de conocimientos destrezas y valores para la vida, apropiados para esta etapa de la adolescencia.

Cuenta con las siguientes áreas:

- Área de Ciencias
- Área Técnica
- Áreas Complementarias

El Área de Ciencias busca dar una amplia base académica y poner los fundamentos necesarios para el futuro desempeño académico.

El Área Técnica facilita una introducción a las áreas técnicas que se imparten a nivel diversificado, con el fin de facilitar la elección de la carrera técnica más apropiada a los alumnos de secundaria.

Las Áreas Complementarias proporcionan una formación en el Área de Informática, además proporciona formación humana y espiritual.

En la actualidad se atiende un promedio de 350 alumnos en esta área.

1.1.3.2. Educación media

El centro educativo Técnico Laboral imparte programas técnicos y educativos a jóvenes de entre 14 y 20 años.

La modalidad de estudio tiene una duración de 3 años en los que un estudiante puede cursar:

- Bachillerato
- Perito Técnico
- Carrera Técnica

Al concluir, el egresado ha concluido una etapa completa de aprendizaje y es apto para trabajar en ese ramo. Con el título de perito técnico o bachillerato, puede ingresar a la universidad.

El centro educativo imparte las siguientes especialidades técnicas:

- Electricidad Industrial
- Electrónica Industrial
- Electrónica de Computación

- Informática
- Dibujo Computarizado de Ingeniería y Arquitectura
- Mecánica Automotriz Diésel
- Mecánica Automotriz Gasolina

1.1.3.3. Técnicos universitarios

La Escuela Técnica Superior Kinal, desarrolla planes de estudio a nivel superior en áreas técnicas específicas. Estos estudios están avalados por la Universidad del Istmo. El fin es optimizar la formación profesional de los participantes, respondiendo a las necesidades actuales y futuras del desarrollo del país.

Programa que está dirigido a todos los que han obtenido un título a nivel medio, para que puedan combinar los estudios superiores con el trabajo, o que logren estudiar dos carreras universitarias de forma simultánea.

Las especiales en este ramo son las siguientes:

- Electricidad Industrial
- Electrónica Industrial
- Mecánica Automotriz
- Informática

- Telecomunicaciones

Actualmente atiende un promedio de 900 alumnos.

1.1.3.4. Carreras técnicas

Están a cargo de la Escuela Técnica Superior Kinal, dirige la capacitación y especialización técnica de jóvenes y adultos. Las principales especialidades son:

- Electricidad y Electrónica Industrial
- Mecánica Industrial
- Mecánica Automotriz
- Administración
- Desarrollo Humano
- Construcción
- Refrigeración
- Calderas de Vapor
- Soldadura Industrial

La Escuela Técnica Superior Universitaria brinda asesoría personalizada a empresas interesadas en la formación de sus trabajadores. Acomoda el horario, contenido técnico y humano a los intereses de cada empresa.

Atiende un promedio de 350 personas en plan fin de semana

1.1.3.5. Certificaciones internacionales

Kinal ofrece cursos de preparación para certificaciones internaciones en el área de Tecnologías de la Información y Comunicación TICs, los cursos preparan para las certificaciones siguientes:

- CompTIA A+
- Cisco Certified Network Associate (CCNA)
- CCNA Security
- Cisco Certified Network Professional (CCNP)
- Sun Certified Java Associate (SCJA)
- Sun Certified Java Programmer (SCJP)
- Visual Studio 2010

Actualmente se atiende un promedio de 300 alumnos.

1.2. El Protocolo de Internet IP

Este proporciona los medios necesarios para la transmisión de bloques de datos llamados paquetes desde el origen al destino, donde origen y destino son *hosts* identificados por direcciones de longitud fija.

1.2.1. Introducción

Internet se ha convertido en la red de computadoras más grande en el mundo, está formada por miles de redes que se encuentran distribuidas en todo el globo terráqueo. Internet tuvo lugar en los años 60, al parecer los inicios fueron con propósitos militares utilizando una red llamada *ARPANET.*

Cuando se desarrollaron las primeras redes sólo era posible realizar una conexión entre computadoras de modelos de una misma marca, llegando al extremo que entre modelos diferentes del mismo fabricante no existía comunicación. Para los años 70 ya era posible la comunicación entre equipos de diferentes modelos. Para lograr lo anterior organismos internacionales como IEEE, ISO se encargan de la regulación de los mecanismos y formas en que se deben realizar las comunicaciones en redes de computadoras. Se definió un modelo teórico denominado modelo OSI, formado por 7 capas que establecen la forma en que se debe comportar cada computadora conectada a la red, logrando con esto la interconexión de diferentes computadoras.

Habiendo logrado la conexión de diferentes computadoras a una misma red, la segunda fase consistió en la comunicación entre los diferentes tipos de redes existentes hasta formar la gran red de redes que actualmente se denomina Internet.

De esta forma se desarrolló una nueva tecnología conocida como packet *switching* (Conmutación de paquetes) la cual utilizaba Transmission Control Protocol e Internet Protocol (TCP/IP).

Los protocolos TCP/IP (entre los que se puede destacar TCP, UDP e IP) son los que utiliza Internet. IP (Internet Protocol) es un protocolo de interconexión de redes heterogéneas cuya función es el transporte de datagramas (Paquetes de datos) a través de la red. UDP (User Datagram Protocol) es un protocolo de comunicación entre computadoras de nivel superior al IP, sin conexión y que no proporciona confiabilidad a la comunicación, es decir no realiza una verificación de las comunicaciones realizadas. TCP (Transmission Control Protocol) es también un protocolo de nivel superior al IP, pero orientado a conexión y confiabilidad.

Actualmente Internet se basa en la versión 4 del protocolo IP, el cual recibe el nombre de IPv4. Gracias a IPv4, Internet ha logrado crecer en la sociedad no solo en el campo tecnológico y económico sino también en aspectos sociales.

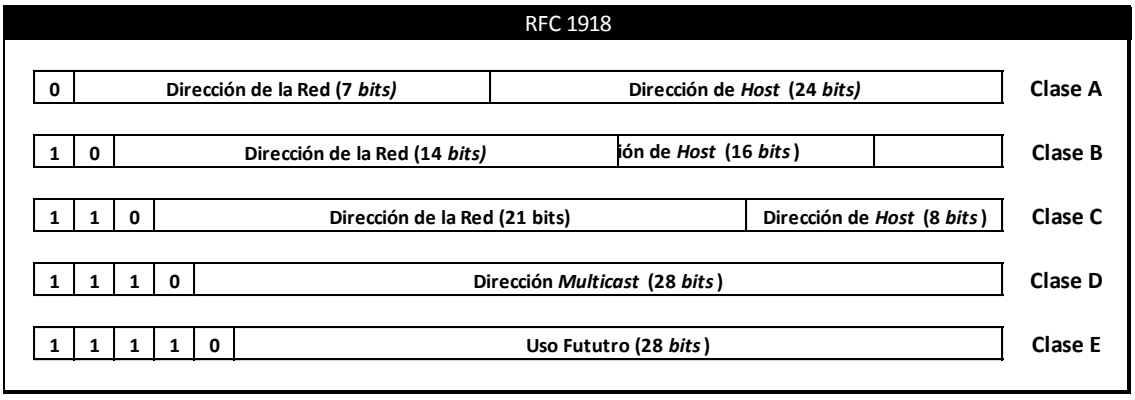
Sin embargo IPv4 no estaba preparado para este crecimiento tan fuerte e inesperado de Internet, el cual está produciendo un agotamiento de la capacidad de proporcionar direcciones a usuarios utilizando este protocolo, esto obligo a que se iniciara el desarrollo de una nueva versión del protocolo IP llamado IPng (IP Next Generation) como sucesor de IPv4. A mediados de los años noventa se anunció que la versión 6 del protocolo IP seria el sucesor de IPv4 y que esta se denominaría IPv6.

1.2.2. Direccionamiento IPv4

En los inicios de la utilización de este protocolo las direcciones IPv4 fueron divididas en grupos llamados clases para la clasificación y asignación. Esto es lo que se conoce como direccionamiento con clase. Con este direccionamiento, cada dirección IP completa tiene un tamaño de 32 bits, estos 32 bits se dividen en la parte de red y la parte de *host*. Un bit o una secuencia de bits al inicio de cada dirección determinan la clase. Las direcciones fueron clasificadas en cinco clases como se muestra en la figura 1. El objetivo de dividir las direcciones IP en clases, fue para facilitar la búsqueda de un equipo en la red. De hecho, con esta notación es posible buscar primero la red a la que se desea tener acceso y luego buscar el equipo dentro de esa red.

Las direcciones de Clase A estaban diseñadas para admitir redes de tamaño extremadamente grande, es decir que contaban con un número bastante grande de *hosts.* Estas direcciones utilizan sólo el primer octeto para indicar la dirección de la red. Los tres octetos restantes son para las direcciones de *host*. En las direcciones de Clase B los dos primeros octetos son para direcciones de red y los dos siguientes para direcciones de *host* y en la Clase C octetos para red y uno para *host*.

Figura 1. **Direcciones IPv4 con clase**



Fuente: elaboración propia.

Cada dirección IP debe tener una máscara que permite distinguir los bits que identifican la red y los que identifican al equipo o *host* de una dirección IP. Por lo tanto una máscara de red se presenta bajo la forma de 32 bits, separados en grupos de 8 *bits,* es decir 4 *bytes* separados por puntos (similar a las direcciones IP) como se muestra en la figura 2.

1.2.2.1. Direcciones IP públicas

Para prolongar la existencia de IPv4 se creó un tipo de dirección llamadas IP públicas, las direcciones IP públicas son únicas. Dos computadoras que tienen acceso a una red pública no pueden tener la misma dirección IP, la razón es porque las direcciones IP públicas son globales y están estandarizadas. Todas las computadoras que se conectan a la Internet acuerdan adaptarse al sistema. Hay que solicitar las direcciones IP públicas de un proveedor de servicios de Internet (ISP), de igual forma los proveedores de servicio de Internet solicitan estas direcciones a organismos internacionales que designando las direcciones de manera jerárquica.

Figura 2. **Direcciones IPv4 con clase con las respectivas máscaras**

Clase A	Red	Host		
Octeto	1	2	3	4
Bits	11111111	00000000	00000000	00000000
Mascara (defecto)	255	0	0	0

Clase B	Red	Host		
Octeto	1	2	3	4
Bits	11111111	11111111	00000000	00000000
Mascara (defecto)	255	255	0	0

Clase C	Red	Host		
Octeto	1	2	3	4
Bits	11111111	11111111	11111111	00000000
Mascara (defecto)	255	255	255	0

Fuente: elaboración propia.

1.2.2.2. Direcciones IP privadas

A diferencia de las direcciones IP públicas, las direcciones IP privadas si se pueden repetir, la razón es porque estas nunca serán visibles desde Internet.

Las direcciones IP privadas no tienen que ser asignadas por un proveedor de servicios, estas están disponibles para el uso sin la necesidad de un registro previo.

Tabla I. **Direcciones IPv4 privadas**

Clase	Rango de direcciones privadas RFC 1918
A	10.0.0.0 1 a 10.255.255.255
B	172.16.0.0 a 172.31.255.255
C	192.168.0.0 a 192.168.255.255

Fuente: elaboración propia.

1.2.2.3. Escases de direcciones

El protocolo IPv4 con el crecimiento de Internet dejo de ser capaz de sostener las necesidades de la Internet, esto ocurrió debido a que el esquema de direccionamiento original produjo una asignación poco eficiente de las direcciones. Uno de los principales factores de escases de direcciones se debe a que inicialmente no se consideró el enorme crecimiento que iba a tener Internet; se asignaron bloques de direcciones grandes (de 16 271 millones de direcciones) a países, e incluso a empresas.

Otro motivo de desperdicio es que en la mayoría de redes, exceptuando las más pequeñas resulta conveniente dividir las redes en subredes. Esta fue una solución a corto plazo, en la cual una subred consiste en reducir el campo del identificador de *host*, pero esto implica que para poder identificar entra varias subredes se utilizó una máscara de dirección de subred, la cual es utilizada para el *router* o dispositivo de capa 3 del modelo OSI para realizar una decisión de *ruteo*. Otra cosa a tener en cuenta es que a pesar que en cada subred, la primera y la última dirección no son utilizables; de todos modos no siempre se utilizan todas las direcciones restantes.

Con la llegada de IPv6 se solucionará las limitaciones de IPv4 en las redes, permitiendo tener más direcciones IP, una buena calidad de servicio, movilidad y velocidad de datos.

1.2.2.4. NAT (Network Address Translation)

Con la escasez de direcciones IPv4, una de las primeras soluciones fue el traductor NAT, para asignar múltiples direcciones privadas a una única dirección IP pública además este mecanismo permite que un dispositivo que trabaje en la capa 3 de modelo OSI, como por ejemplo un *router*, sea capaz de actuar como traductor de direcciones.

El funcionamiento de NAT es de la siguiente manera:

Como sabe una dirección IP pública debe ser única, y las mismas son escasas, y la idea es que una IP pública le provea acceso a Internet a una red que fue diseñada con direcciones IP privadas, entonces varias direcciones privadas son asociadas a una dirección a un rango de direcciones IP públicas.

Mediante la utilización de NAT los *host* que poseen direcciones privadas podrán acceder a Internet haciendo uso de un mínimo de una dirección pública. No obstante, este mecanismo no puede utilizarse en los terminales móviles y, además, muchas aplicaciones son incapaces de ser utilizadas mediante este tipo de direcciones, especialmente las relacionadas con la autenticación y la seguridad de las comunicaciones.

1.2.2.5. Limitaciones en el enrutamiento

Aún si existieran más direcciones con clase, muchas direcciones de red provocaran que los *routers* trabajen demasiado lento debido a la carga del enorme tamaño de las tablas de enrutamiento, necesarias para guardar las rutas de acceso a cada una de las redes.

Esto requeriría una capacidad mayor de la Internet para sostener tablas de enrutamiento exageradamente grandes.

1.2.2.6. Limitaciones en configuración

Existen dos formas de configurar una dirección de IPv4, se puede realizar una configuración manual o mediante un protocolo de configuración de direcciones como lo es el Protocolo de configuración dinámica de *host* DHCP (Dynamic Host Configuration Protocol).

Al utilizar DHCP un *host* obtiene una dirección de forma dinámica sin que el administrador de red tenga que configurar cada uno de los *host* de la red. A medida que cada *host* es conectado a la red, es decir cuando se arranca un *host* configurado con DHCP, este se comunica con el servidor DHCP y solicita una dirección. Pero en la actualidad con la existencia de más equipos y dispositivos que utilizan IP, surge la necesidad de una configuración más sencilla y automática así como otras opciones de configuración que no dependan de la administración de una infraestructura DCHP.

1.2.3. Análisis del protocolo IP versión 6 (IPv6)

Desde hace varios años se ha planteado el problema del agotamiento de direcciones de IP en la versión 4 (IPv4), por lo tanto la IETF inicio un proceso para diseñar una nueva versión del protocolo del cual fue presentada la primera versión en el año 1990. Esta versión de IP de nueva generación se desarrolló hace varios años. Pero la implementación se va retrasando con la utilización de mecanismos para rescatar el espacio de direcciones en IPv4. En cualquier caso el futuro de IP ya está definido.

Algunos informáticos se pregunta ¿por qué no IPv5?, estas direcciones fueron extensiones experimentales y terminaron de formalizarse como una nueva versión del protocolo, y con el fin de evitar posibles conflictos de numeración y/o confusión, se optó por elegir el número de versión 6.

En líneas generales, el protocolo IPv6 es considerado una evolución más que una revolución respecto al protocolo IPv4. Se han mantenido los conceptos principales del protocolo, removiendo aquellas características de IPv4 que son poco utilizadas en la práctica. Se han añadido nuevas características que buscan solucionar los problemas existentes en el protocolo IPv4 y tal y como se describe en la RFC 2460, IPv6 es el sustituto de IPv4. Cada dirección de este nuevo protocolo paso de tener un tamaño de 32 bits a 128 bits, lo que da un total de 340 282 366 920 938 463 463 374 607 431 768 211 456 direcciones, mientras que en la versión cuatro se tienen 4 294 967 296 direcciones.

Este aumento en el espacio de direcciones no sólo proporciona la capacidad de poder asignar direcciones a un mayor número de *host*, sino una jerarquía de direcciones mayor. Según Christian Huitima (vocero de la IETF)

estima que habrá 1 500 direcciones IPv6 por cada metro cuadrado de la superficie terrestre.

1.2.4. Principales diferencias entre IPv4 e IPv6

- Mayor espacio de direcciones: el tamaño de las direcciones para IPv6 cambia de 32 bits a 128 bits, esto con el fin de soportar más niveles de jerarquías de direccionamiento.

- Un encabezado más simple: algunos campos del encabezado de IPv4 fueron removidos o se convirtieron en opcionales.

- Paquetes IPv6 eficientes y extensibles: los *routers* no fragmentan los paquetes, y con una cabecera de longitud fija, más simple, que agiliza el procesamiento por medio del *router*.

- Posibilidad de paquetes con carga útil (datos): IPv6 tiene la capacidad de enviar paquetes de hasta 65 355 bytes.

- Seguridad en el núcleo del protocolo (IPsec*):* IPsec viene integrado pudiendo lograr la capacidad de autenticación y privacidad, pero es necesario configurarlo.

- Capacidad de etiquetas de flujo: puede ser utilizada por un *host* para etiquetar paquetes pertenecientes a un flujo (*flow)* de tráfico particular, que requieren manejo especial por los *routers*, tal como la calidad de servicio o el servicio en tiempo real como la video conferencia.

- Autoconfiguración: la autoconfiguración de direcciones es más simple. Especialmente en direcciones Globales Unicast, los 64 bits superiores son asignados por un mensaje desde el *router* y los 64 bits más bajos se obtienen de la dirección MAC.
- Renumeración: facilitando el cambio del proveedor de servicios

- Características de movilidad: es la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de la movilidad.

- Calidad de servicio (*QoS)* y clase de servicio (CoS)

1.2.5. Características generales de IPv6

A continuación se van a ver de forma básica algunas características generales del protocolo IPv6.

1.2.5.1. Nuevo formato de encabezado

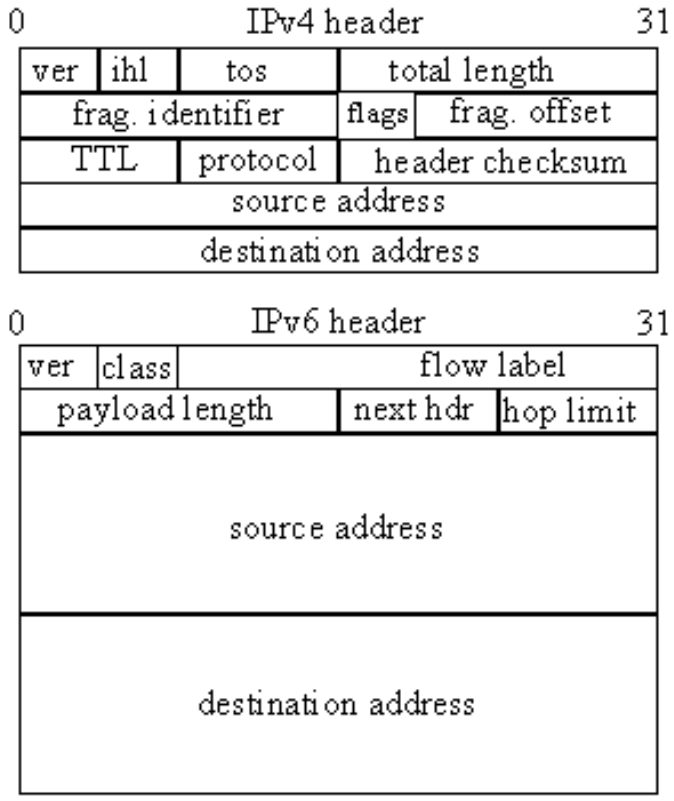
El encabezado IPv6 tiene nuevo formato que está diseñado para reducir al mínimo la sobrecarga del encabezado. Esto se consigue al mover los campos que no son esenciales y los campos de opciones a encabezados de extensión que se colocan a continuación del encabezado IPv6. La simplificación del encabezado IPv6 permite un procesamiento más eficaz en los enrutadores intermedios.

El nuevo encabezado de IPv6 sólo tiene el doble de tamaño del encabezado IPv4, a pesar de que las direcciones IPv6 son cuatro veces mayores que las direcciones IPv4.

En la figura 3 se observa que el encabezado de IPv6 es más simple, también se observan los campos que fueron omitidos al darse la transición.

La cabecera de un paquete IPv6 es más sencilla y la funcionalidad es mayor que la del paquete IPv4.

Figura 3. **Comparación de encabezados IPv4 vs IPv6**

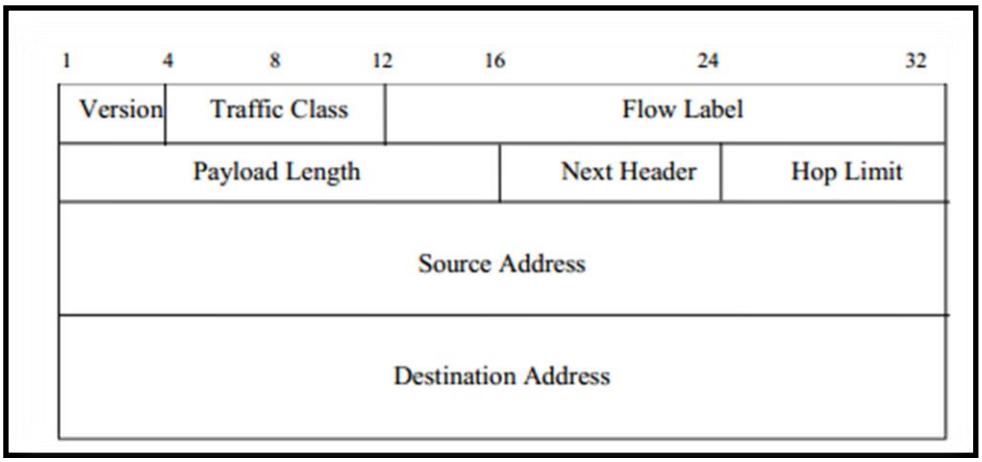


Fuente: http://techashram.wordpress.com/tag/ipv6-header/. Consulta: marzo de 2013.

1.2.5.2. La cabecera IPv6

La cabecera de un paquete IPv4 es variable, por lo que necesita un campo de tamaño o *lenght.* Sin embargo, para simplificar la vida de los *routers,* IPv6 utiliza un tamaño de cabecera fijo de 40 bytes, que componen un total de ocho campos:

Figura 4. **Encabezado de IPv6**



Fuente: http://docs.oracle.com/cd/E19683-01/817-0573/chapter1-fig-8/index.html. Consulta: marzo de 2013.

Se han suprimido seis campos (tamaño de cabecera, tipo de servicio, número de identificación del datagrama, banderas, número de byte del datagrama fragmentado y el *checksum*) respecto a la versión del protocolo IP. Además se ha redefinido los campos de longitud del datagrama, tiempo de vida y de tipo del protocolo.

- Campo versión (4 bits): se sigue manteniendo como el primer campo del datagrama. Esto es así para mantener la compatibilidad con formatos anteriores y porque permite de una forma sencilla y rápida discriminar

que versión del datagrama se recibe, facilitando a los *routers* el proceso de discriminar entre la versión 4 y la versión 6.

- Campo clase (*class):* es un número de 8 bits que hace referencia a la prioridad del datagrama. Este campo es una de las nuevas aportaciones para conseguir que algunos tipos de aplicaciones (videoconferencia, telefonía, etc.) puedan realizarse en tiempo real.

- Campo tipo de flujo (*Flow Label*): se compone de 16 bits, que permiten especificar que una serie de datagramas deben recibir el mismo trato. Esto es aplicable por ejemplo a una serie de datagramas que van del mismo origen al mismo destino y con las mismas opciones. Junto con el campo de clase permiten aplicaciones en tiempo real.

- Campo tamaño de los datos (*Payload Length):* al igual que en la versión 4 es un número de 16 bits, lo que permite un tamaño máximo en principio de 2^{16} = 65536 bytes (64K). No obstante, a diferencia de la versión 4, este número hace referencia sólo al tamaño de los datos que transporta, sin incluir la cabecera.

- Campo siguiente cabecera (*Next Header)*: es un valor de 8 bits que indica al *router* si tras el datagrama viene algún tipo de extensión u opción. Este campo sustituye al campo de banderas (*flags)* de la versión 4. De esta manera, en lugar de complicar la cabecera IP con la interpretación de los diferentes bits de opciones, se sitúan fuera del datagrama básico.

- Campo alcance del datagrama (*Hop Limit)*: este campo es necesario para evitar que los datagramas circulen infinitamente por la red,

eliminándose al llegar a 0 (el valor máximo es de $2^8 = 256$). Este campo está formado por 8 bits que indica el número máximo de *routers* que puede atravesar un datagrama hasta llegar al destino y es el equivalente al tiempo de vida (TTL) de la versión 4. Cuando un datagrama llega a un *router* y es encaminado hacia otro computador el valor de este campo es disminuye en una unidad.

- Campo dirección origen y destino (*Source Address y Destination Address*): son las direcciones de los nodos de IPv6 que realizan la comunicación, tienen un tamaño de 128 bits cada una.

1.2.5.3. Formato de direcciones en IPv6

La representación de una dirección IPv6 tiene el siguiente formato:

X : X : X : X : X : X : X : X

Donde X es número hexadecimal de 16 bits. También es común agregar el prefijo:

Dirección_IPv6 / longitud_del_prefijo

Donde la dirección es expresada de la forma indicada anteriormente y la longitud del prefijo es un valor decimal que especifica el número de bits más a la izquierda que se tomaran de la dirección en la forma expandida.

Un ejemplo una dirección IPv6 es el siguiente:

2001:0000:1234:0000:0000:C1C0:ABCD:0876/64

Con el fin de simplificar la escritura y memorización de direcciones, se pueden aplicar las siguientes reglas a las direcciones de IPv6.

- No se hace distinción entre mayúsculas y minúsculas. ABC9 es equivalente a abc9.

- Los ceros al inicio de un campo son opcionales. 00c1 es equivalente a c1.

- Una sucesión de campos con ceros puede ser remplazados por **::** 1234:0000:0000:abc9 es igual a 123::abc9 pero la regla solo puede ser utilizada una vez en una dirección IPv6.

Si tiene la siguiente dirección y queremos aplicar las reglas anteriores obtendrá:

2001:0000:1234:0000:0000:C1C0:ABCD:0876

Mediante la regla a), se puede escribir como:

2001:0000:1234:0000:0000:c1c0:abcd:0876

La dirección se puede escribir de forma resumida utilizando la regla b):

2001:0:1234:0:0:c1c0:abcd:876

Aplicando la regla c) se puede resumir aún más a:

2001:0:1234::c1c0:abcd:876

Tal como es el caso de IPv4 para poder identificar la parte de red y la parte que identifica al *host*, se utiliza el formato CIDR en la forma <dirección>/<prefijo>. Por ejemplo, una dirección en la forma 3ffe:b00:c18:1::1/64 indica que los primeros 64 bits identifican a la red (3ffe:b00:c18:1) y los restantes 64 bits identifican al *host* de dicha red (::1).

Tradicionalmente el uso del símbolo **:** en las direcciones IPv4 señala un puerto en un determinado nodo, por ejemplo 192.168.1.1:80 señala al puerto 80 (WWW) del nodo 192.168.1.1. Esto representa un problema de incompatibilidad al utilizar direcciones IPv6, por lo que se ha establecido que para señalar un puerto en una determinada dirección de IPv6, esta debe estar encerrada por corchetes en la forma [dirección] : puerto.

1.2.6. Direccionamiento en IPv6

En IPv6 se ha definido 3 tipos de direcciones:

- Unicast: identifican a un nodo único en particular. Un paquete enviado a una dirección *unicast* es entregado sólo a la interfaz identificada con dicha dirección.

- Multicast: identifican a un grupo de nodos. El tráfico enviado a una dirección *multicast* es reenviado a todos los nodos pertenecientes al grupo.

- Anycast: identifican a un conjunto de interfaces *y* es utilizada para enviar tráfico a la interfaz más cercana del grupo.

En el IPv6 no existen direcciones *broadcast,* la funcionalidad ha sido mejorada por las direcciones *multicast.*

1.2.7. Nomenclatura de las direcciones IPv6

A continuación se describe los diferentes tipos de direcciones que las direcciones IPv6 poseen.

1.2.7.1. Direcciones *unicast*

Es un identificador asignado a una sola interfaz. Así un paquete enviado a una dirección *unicast*, sólo será enviado a esa interfaz. Existen varias formas de asignación de direcciones *unicast*, algunas con estructuras más complejas que proporcionan asignación de direcciones jerárquicas.

Algunas direcciones *unicast* de propósito especial que han sido definidas hasta el momento de la escritura de este documento son las siguientes:

1.2.7.2. Dirección *loopback*

No debe ser asignada a una interfaz física y todos los paquetes con esta dirección deben permanecer dentro del *host* creador del paquete. Aún más, los *routers* no transmiten paquetes con direcciones *loopback* la representación es (::1).

1.2.7.3. Dirección no especificada

Esta dirección no puede ser asignada a una interfaz y no debe ser utilizada como una dirección destino en los paquetes. Esta dirección indica la

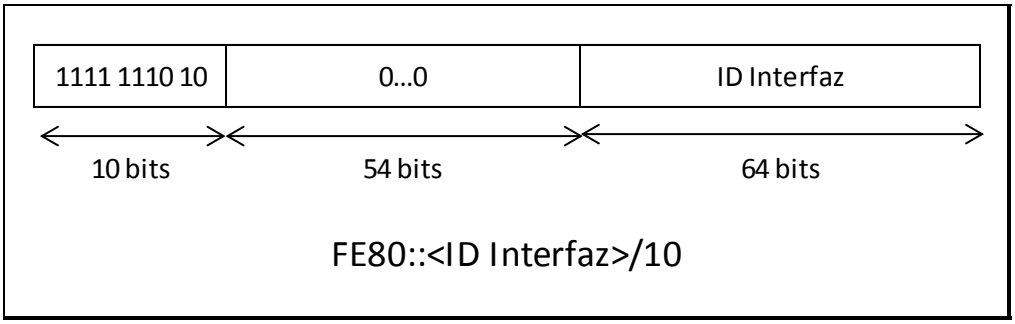
ausencia de una dirección IPv6, por ejemplo a inicializar un *host* en una red IPv6, se puede utilizar este tipo de direcciones como dirección fuente en los paquetes hasta que se reciba la dirección IPv6 del *host* mientras se realiza la configuración automática. La representación es (::).

1.2.7.4. Direcciones de enlace local

Este tipo de direcciones pueden ser automáticamente configuradas en una interfaz utilizando el prefijo FE80::/10. También son utilizadas en el proceso de configuración automática sin estados y en el protocolo de descubrimiento de vecinos *MLD* (*Multicast Listener Discovery).* Aún más, los *routers* no transmiten paquetes con direcciones de enlace local a otros sitios, estas son locales a una subred.

En la figura 5 se muestra el formato de este tipo de direcciones:

Figura 5. **Formato de direcciones *unicast* de enlace local**

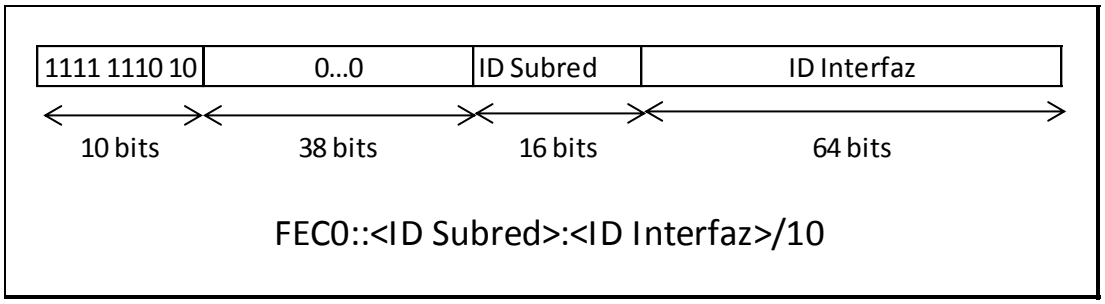


Fuente: elaboración propia.

1.2.7.5. Direcciones de enlace de sitio

Utilizan el prefijo FEC0::/10 como se observa en la figura 6 se concatenan el identificador de subred con el identificador de interfaz. Estas direcciones pueden ser utilizadas para ser asignadas a un sitio completo sin tener que utilizar una dirección de prefijo único global. Son similares a las direcciones privadas de IPv4 y los *routers* no transmiten paquetes con direcciones fuente o destino de este tipo, estas son locales a una organización.

Figura 6. **Formato de direcciones de enlace de sitio**



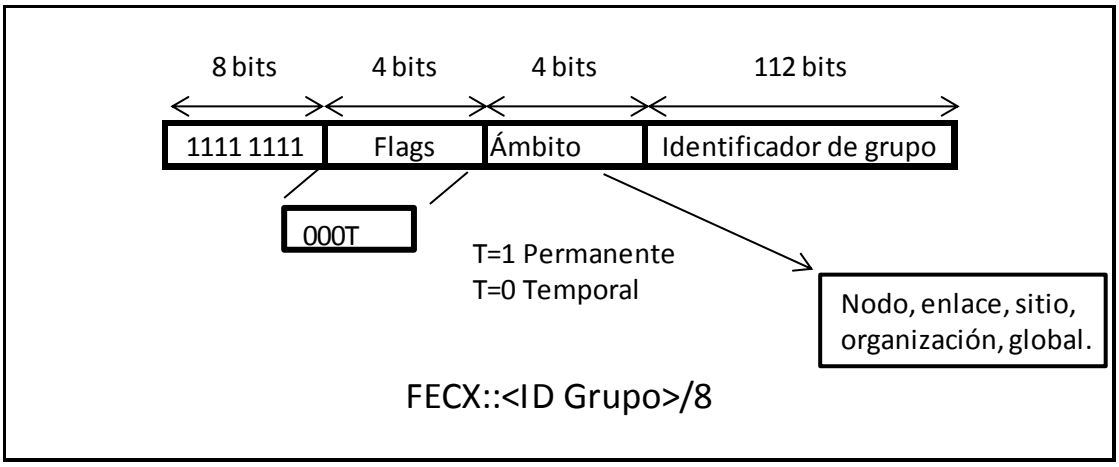
Fuente: elaboración propia.

1.2.7.6. Direcciones *multicast*

Una dirección *multicast* identifica a un grupo de nodos y cada uno de estos nodos puede pertenecer a cualquier número de grupos *multicast*. El formato de una dirección *multicast* se presenta en la figura 7.

Los primeros 8 bits (todos unos) de la dirección de IPv6 identifican una dirección *multicast*. El campo flags es de cuatro bits, y los tres primeros bits de más alto orden están reservados para uso futuro y deben ser inicializados a cero. El cuarto bit (el de menos orden) indica el tipo de dirección *multicast*, con T = 0 se trata de dirección permanente y con T = 1 es una dirección *multicast* temporal.

Figura 7. **Formato de la dirección *multicast***



Fuente: elaboración propia.

El campo ámbito de cuatro bits es utilizado para limitar el alcance del grupo *multicast*.

El campo Group ID identifica el grupo *multicast*, ya sea permanente o temporal con el alcance dado en el campo *scope.*

Las direcciones *multicast* no deben ser utilizadas como una dirección fuente en el paquete IPv6 o aparecer en cualquier encabezado de ruteo.

Existen direcciones *multicast* reservadas:

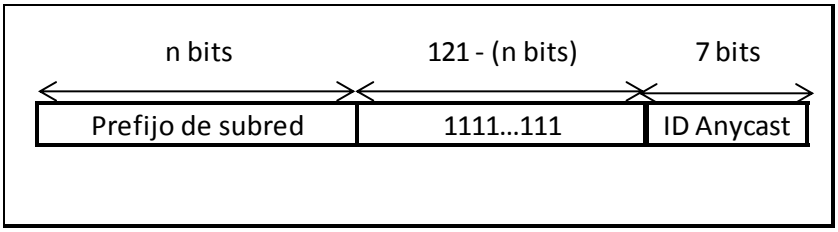
- FF01::1 todos los nodos
- FF02::1 todas las interfaces
- FF02::2 Todos los *routers* locales

- FF05::2 Todos los *routers* del sitio

1.2.7.7. Direcciones *anycast*

Es una dirección que es asignada a más de una interfaz, típicamente perteneciendo a distintos nodos, con la propiedad de que un paquete enviado a una dirección *anycast* es ruteado a la interfaz más cercana que tenga esa dirección, de acuerdo a la métrica de distancia del protocolo de ruteo. Las direcciones *anycast* tienen el formato que se muestra en la figura 8.

Figura 8. **Direcciones *anycast***



Fuente: elaboración propia.

Las direcciones *anycast* son localizadas en el espacio de direcciones *unicast*, utilizando cualquiera de los formatos de direcciones *unicast* definidos. Por lo tanto, una dirección *unicast* es asignada a más de una interfaz, entonces se convierte en una dirección *anycast*. Los *host* a los cuales la dirección es asignada deberán ser explícitamente configurados para saber que esta es una dirección *anycast*.

Algunos usos del esquema de direcciones *anycast* son los siguientes:

- Identificación de un conjunto de *routers* pertenecientes a un proveedor de servicios de Internet.

- Identificación de un conjunto de *routers* conectados a una subred particular.

- Identificación de un conjunto de *routers* que proveen una entrada a un dominio particular de ruteo.

Algunas restricciones impuestas en el uso de direcciones *anycast* son:

- Estas no deben ser utilizadas como dirección fuente para un paquete en particular.

- Una dirección *anycast* sólo debe ser asignada a un *router* no a un *host*

- Todos los *routers* en una subred deben soportar las direcciones *anycast*

- Las direcciones *anycast* deberán ser utilizadas para aplicaciones donde un nodo necesita comunicación con un grupo de *routers* en una subred remota.

1.2.8. Configuración de Direcciones IPv6 con y sin estado

Actualmente IPv6 puede ser configurado en la mayoría de los sistemas operativos como Linux y Windows a partir de la versión de Windows XP y en varios dispositivos de interconexión de red.

Los sistemas operativos de las MacOS X tienen un soporte transparente del usuario y tiene una interfaz para realizar la configuración automática o manual.

Sin embargo muchos dispositivos con infraestructura de redes no tiene el soporte adecuado para las configuraciones IPv6, tales como:

- *Firewalls*
- VPN *server*
- AP (Puntos de Acceso Inalámbricos)
- *Switches*

1.2.8.1. Configuración estática (*static*)

La configuración estática consiste en ingresar manualmente la dirección IPV6 de un nodo en un archivo de configuración o mediante el uso de herramientas propias del sistema operativo. La información que se debe incluir como mínimo es la dirección IPv6 y el tamaño del prefijo de red.

1.2.8.2. Configuración *stateless*

Otra forma es utilizar *stateless* o procedimiento de autoconfiguración sin estados, el cuál no requiere de ninguna configuración manual en el *host*, es una configuración mínima la que se realiza en los *routers,* y no requiere de servidores adicionales. Permite que un *host* sea capaz de generar su propia dirección mediante una combinación de información local y de información

anunciada por los *routers.* Utiliza el protocolo de descubrimiento de vecinos *NDP* para reconocer a los *routers* presentes en el enlace y generar una dirección IPv6 a partir del prefijo que estos anuncian. Los pasos que realiza un nodo para obtener una dirección son los siguientes:

- Descubrir un prefijo utilizado en el enlace: el nodo escucha los anuncios que envían los *routers* periódicamente al enlace (mensajes RA) o puede solicitar un anuncio, enviando un mensaje de solicitud de *router* (RS). A partir de los mensajes RA, obtiene la información del prefijo de red.

- Generar un identificador de interfaz: para generar el resto de la dirección IPv6, el nodo genera un identificador de interfaz. Puede generarla a partir de la dirección MAC (como en las direcciones locales a enlace, no funciona en sistemas operativos Windows) o de forma aleatoria.

- Verificar que la dirección no esté duplicada: la dirección IPv6 generada debe ser única, por lo que el nodo inicia el procedimiento de detección de direcciones duplicadas (*DAD*). Si la dirección es única, el nodo comienza a utilizarla.

1.2.8.3. Autoconfiguración *stateful*

En esta autoconfiguración, el *host* obtiene la dirección de la interfaz y la información de parámetros de configuración desde un servidor. Los servidores mantienen una base de datos con las direcciones que han sido asignadas a cada *host* mediante DHCPv6.

Las autoconfiguraciones (*stateless* y *stateful*), se complementan.

Un *host* puede usar la autoconfiguración *stateless*, para generar su propia dirección, y obtener el resto de parámetros mediante la autoconfiguración predeterminada (*stateful*).

El mecanismo de autoconfiguración sin intervención se emplea sólo para asegurarse de que la dirección es única y enrutable sin importar que dirección ha sido asignada al *host.*

Al contrario, el mecanismo de configuración estática, asegura que cada *host* tiene asignada una determinada dirección, la cual es asignada manualmente.

1.2.8.4. Algoritmos de enrutamiento

El uso de IPv6 no implica cambios significativos en la forma en que operan los protocolos de enrutamiento en las redes IP. Sin embargo, para aprovechar las nuevas características de IPv6, se han desarrollado nuevas versiones o complementos a los protocolos de enrutamiento más utilizados. En la tabla II se presentan las nuevas versiones desarrolladas para IPv6.

Tabla II. **Protocolos de enrutamiento en IPv6**

Protocolo de enrutamiento	Versiones para IPv6
RIP	RIPng
EIGRP	EIGRP para IPv6
OSPF	OSPFv3
IS-IS	Integrated IS-IS
BGP	BGP-MP

Fuente: elaboración propia.

1.2.8.5. ICMPv6

El protocolo de mensajes de control de Internet (ICMP) es utilizado para enviar información de configuración y reportes de error entre los nodos de una red. Para IPv6, se ha desarrollado una nueva versión del protocolo, denominada ICMPv6.

A diferencia de ICMP para IPv4, el cual no es esencial para las comunicaciones en redes IPv4, ICMPv6 posee características imprescindibles para la configuración y comunicación en redes IPv6. El protocolo ICMPv6 comprende una serie de mensajes. Cada uno identificado con un código. Dichos mensajes permiten llevar a cabo diversos procesos en IPv6 tales como: descubrimiento del máximo valor MTU en un camino, manejo de grupos *multicast*, detección de destinos inalcanzables y el protocolo de descubrimiento de vecinos.

1.2.8.6. Protocolo de descubrimiento de vecinos

El protocolo de descubrimiento de vecinos NDP (Neighbor Discovery Protocol) es un protocolo necesario para el correcto funcionamiento de las redes IPv6. Es el encargado de descubrir otros *host* en el enlace, realiza la resolución de direcciones IPv6 y direcciones MAC, encuentra los *routers* disponibles y mantiene información actualizada sobre el estado de las rutas hacia otros nodos.

Este protocolo realiza funciones para IPv6 similares a las realizadas por ARP en IPv4.

1.2.8.7. DHCP para IPv6

Utiliza un protocolo UDP cliente/servidor, diseñado para reducir el costo de gestión de nodos para IPv6 en entornos donde los administradores precisan un control sobre la asignación de los recursos de red, superior a los facilitados por el mecanismo de configuración *stateless.*

Además, DHCP ha sido diseñado para ser fácilmente extensible con nuevos parámetros de configuración, a través de extensiones que incorporan esta nueva información.

Los cambios fundamentales entre IPv4 con DHCP e IPv6, basados el formato de direccionamiento y autoconfiguración de IPv6, son:

- La dirección de enlace local permite a un nodo tener una dirección tan pronto como arranca, lo que significa que todos los clientes tienen una dirección IP fuente para localizar un servidor o relé en el mismo enlace.

- Los indicadores de compatibilidad *BOOTP* y *broadcast* han desaparecido

- El *multicast* y los ámbitos de direccionamiento permiten el diseño de paquetes de descubrimiento, que definen por sí mismo el rango por la dirección *multicast*, para la función requerida.

- Se soportan múltiples direcciones por cada interfaz

Algunas opciones DHCP ya no son precisas, debido a que los parámetros de configuración se obtienen a través de ND o del protocolo de localización de servicios. De esta forma, se soportan las siguientes funciones nuevas:

- Configuración de actualizaciones dinámicas de DNS
- Desaprobación de direcciones, para reasignación dinámica
- Relés pre configurados con direcciones de servidores, o mediante *multicast*.
- Autentificación
- Los clientes pueden pedir múltiples direcciones IP
- Las direcciones pueden ser reclamadas mediante el mensaje de iniciar-reconfiguración.
- Integración entre autoconfiguración de direcciones *stateless* (detección automática) y *statefull* (configuración manual).
- Permitir relés para localizar servidores fuera del enlace

1.2.8.8. DNS (Domain Name Server)

Al referirnos a direcciones IP se refiere a la localización de un *host* mediante la utilización de una URL. Para que este mecanismo funcione, existe un protocolo denominado Domain Name System (sistema de nombres de Dominio).

Este mecanismo, fue definido inicialmente para IPv4, el mismo que después fue actualizado, el cual incluía un nuevo tipo de riesgo para almacenar

las direcciones IPv6, y definiciones actualizadas las que devuelven direcciones de Internet como parte de procesos de secciones adicionales.

El problema del sistema DNS existente es comprensible. Ya que al hacer una consulta, las aplicaciones asumen que se les devolverá una dirección de 32 *bits* pero para resolverlo hay que definir algunas extensiones:

- Un nuevo tipo de registro para mapear un nombre de dominio con una dirección IPv6: es el registro AAAA (con un valor decimal de 28).

- Un nuevo dominio para IPv6 es *IP6.INT.* La representación se realiza en orden inverso de la dirección, separado por puntos los valores (hexadecimal), seguidos del dominio *IP6.INT.*

- Redefinición de las consultas existentes, que localizan direcciones IPv4, para que puedan también direcciones IPv6.

1.2.9. Mecanismos de transición a IPv6

Con la creación de un nuevo protocolo para resolver el problema de direccionamiento que presentan actualmente las redes de comunicaciones, es necesario que se piense en un método que permita la migración de IPv4 a IPv6. Debe conocer estos métodos que se denominan mecanismos de transición. Existen tres bloques básicos definidos por la *IETF: dual stack,* Traducción y Tunneling.

1.2.9.1. Mecanismo de transición *dual stack*

Al inicio de la migración, la gran mayoría de los sistemas continuarán utilizando IPv4. Un sistema dual da la facilidad de que puedan utilizar IPv6

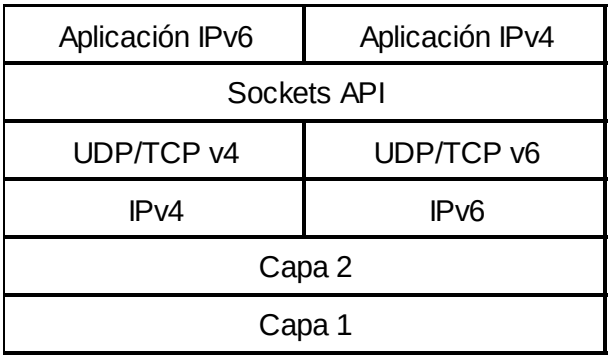
para comunicarse con sistemas iguales, y al mismo tiempo puedan retroceder para comunicarse con sistemas viejos que manejen IPv4.

Este mecanismo, como su nombre lo sugiere, se refiere al uso de dos pilas, de diferente protocolo, que trabajan paralelamente y permiten al dispositivo trabajar con uno u otro protocolo.

Los dispositivos configurados con *dual stack* procesan las aplicaciones IPv4 utilizando la pila IPv4, mientras que para las aplicaciones IPv6 utilizan la pila IPv6. Hay que tener en cuenta que este mecanismo solo es útil para nodos similares; es decir, IPv6 – IPv6 e IPv4 – IPv4 como se ve en la figura 9. Ambos protocolos conviven por tal razón pueden operar en uno de tres modos.

- Pila IPv4 habilitada y pila IPv6 deshabilitada
- Pila IPv6 habilitada y pila IPv4 deshabilitada
- Con ambas pilas habilitadas

Figura 9. **Esquema *dual stack***



Fuente: elaboración propia.

Nodos *dual stack* con la pila IPv6 deshabilitada trabajan como un nodo de IPv4. Similarmente para los que trabajan con la pila IPv4 deshabilitada, el comportamiento será como el de un nodo de IPv6.

Actualmente muchos sistemas comerciales ya cuentan con un protocolo IP de *dual stack*. En consecuencia, esto lo hace el mecanismo más utilizado en la solución de transición. Esta técnica tiene la ventaja de asegurar la conectividad de los nodos de la red, cuando no sea posible utilizar IPv6 se puede utilizar IPv4. Las desventajas son una disminución del desempeño de los equipos de red, que deben mantener tablas de direcciones y rutas independientes para cada protocolo.

1.2.9.2. Mecanismo de transición traducción

Este mecanismo de transición es similar al realizado por el proceso NAT, donde se modifican las cabeceras de los paquetes. La traducción es necesaria cuando un nodo solo IPv4 se quiere comunicar con un nodo de IPv6. Este mecanismo no es recomendable.

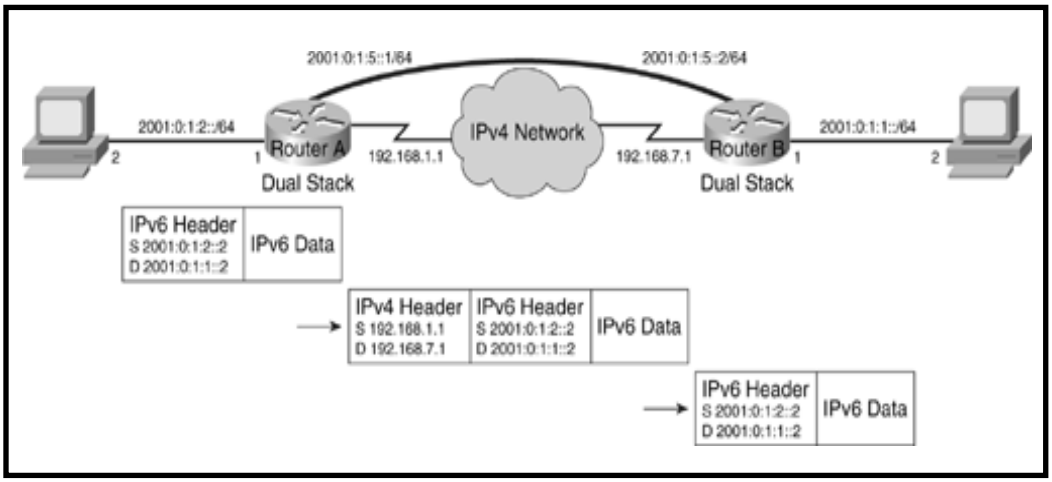
1.2.9.3. Mecanismo de transición *tunneling*

El *tunneling* es un proceso donde la información de un protocolo es encapsulada dentro de la trama o paquete de otra arquitectura, habilitando que los datos originales sean llevados sobre un protocolo diferente. Los escenarios de *tunneling* para IPv4 hacia IPv6 son diseñados para habilitar a una infraestructura IPv4 existente a llevar paquetes IPv6 mediante el encapsulamiento de la información mediante datagramas IPv4.

También se puede describir al *tunneling* IPv6 como una técnica para encapsular paquetes IPv6 dentro de paquetes IPv4 para que estos puedan ser transmitidos a través de redes IPv4. El uso de túneles requiere que exista un equipo en cada extremo que realice el proceso de encapsulación y extracción de los paquetes IPv6. Los túneles permiten otorgar conectividad IPv6 cuando no es posible implementar IPv6 en todos los dispositivos de una determinada red.

En la figura 10. Se puede observar que los paquetes que originalmente son encapsulados en IPv6 nuevamente serán encapsulados dentro de un paquete IPv4. El proceso inverso se realiza en el otro extremo del túnel.

Figura 10. **Modelo general del esquema *tunneling***



Fuente: http://www.fengnet.com/book/CCNP.BSCI.642-901.Official.Exam.Certification.Guide.4th.Ed/final/ch21lev1sec2.html. Consulta: abril de 2013.

Túneles 6to4: permiten la comunicación de redes IPv6 a través de redes IPv4 a través de redes IPv4, estos túneles son configurados de forma

automática con IP pública y para realizar pruebas no se necesita de un proveedor de servicios.

Túneles 6over4: permite la configuración de túneles de tipo *host-to-host*, *host-to-router*, *router-to-host*; el descubrimiento de vecinos se realiza por medio de IPv4 utilizando *multicast*.

2. FASE DE SERVICIO TÉCNICO PROFESIONAL

2.1. Situación actual de la red de voz y datos de Fundación Kinal

Fundación Kinal posee 3 enlaces a Internet mediante IPv4, otorgados por los ISP Columbus Network que provee dos enlaces y Claro que provee un enlace como se observa en la tabla III.

Tabla III. **Servicio de Internet Fundación Kinal**

Proveedor	Velocidad	Tipo de enlace
Columbus Network	8Mbps	Enlace Simétrico Fibra Óptica
Columbus Network	6Mbps	Enlace Simétrico Fibra Óptica
Claro	2Mbps	Enlace ADSL

Fuente: Departamento de IT Fundación Kinal.

Debido a que Fundación Kinal es pionera en la implementación de IPv6, encontró el obstáculo de que, ninguno de los dos proveedores pudo proporcionar un direccionamiento en IPv6, por lo que para tener acceso a Internet, hará uso del servicio que presta Hurricane Electric Internet Services, permitiendo realizar un túnel de forma gratuita y obtener un direccionamiento IPv6 gratuito, es decir que para obtener la direcciones IPv6 utilizar el método de *tunneling*, mientras que para la configuración de los usuarios en la LAN utilizar el método de *dual stack.*

Pese a que el objetivo final sea la total sustitución del protocolo IP en la versión 4, los expertos sugieren que a corto-mediano plazo el escenario más común para facilitar la transición es aquel en el que los dos protocolos coexistan, siendo *dual stack* el método de transición que proporciona estas características, logrando la implementación de un red hibrida, y este será el enfoque de migración adoptado en las instalaciones de Fundación Kinal, ya que permite que el usuario final no se vea perturbado en la actividad cotidiana pudiendo utilizar los servicios tradicionales sobre IPV4.

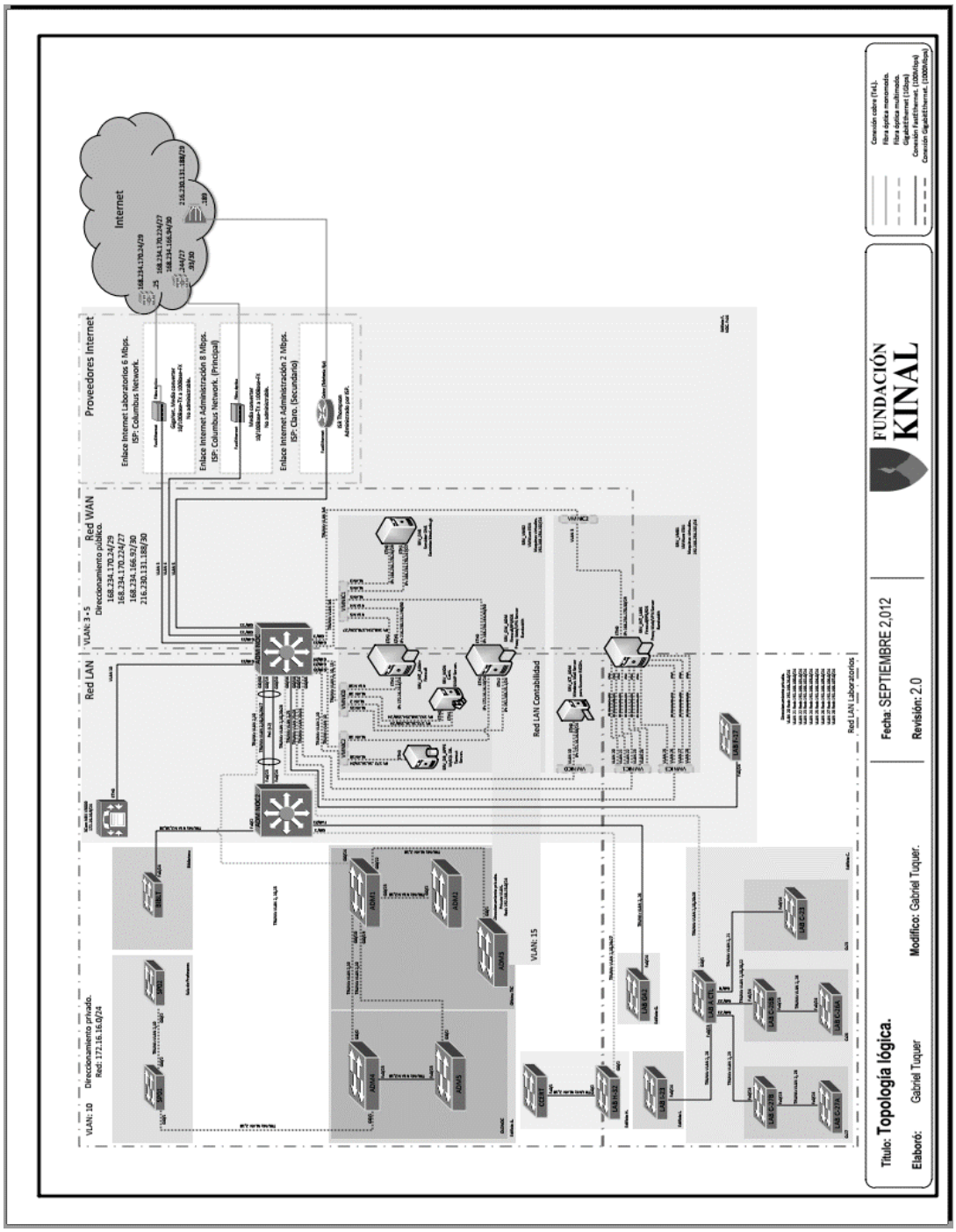
El servicio de voz sobre IP no se verá afectado, dado que el mismo quedara configurado en una VLAN que permita aprovechar al máximo este servicio.

Para la implementación de la red IPv6, sobre la red de Fundación Kinal, que funciona sobre IPv4, es factible utilizar la técnica de *dual stack,* que permita mantener funcionando el actual protocolo simultáneamente con la nueva tecnología, de manera que se garantice la conectividad de nodos de la red y cuando no sea posible utilizar IPv6, se pueda utilizar IPv4.

Se debe tener en cuenta que se tendrá la desventaja del desempeño de los equipos de red, que deben mantener tablas de direcciones y rutas independientes para cada protocolo.

Para poder hacer uso de direcciones IPv6 se debe seguir los pasos proporcionados en la página de Hurricane Electric Internet Services http://www.tunnelbroker.net/ para poder realizar las pruebas con direcciones reales de IPv6.

Figura 11. **Diagrama de red Fundación Kinal**



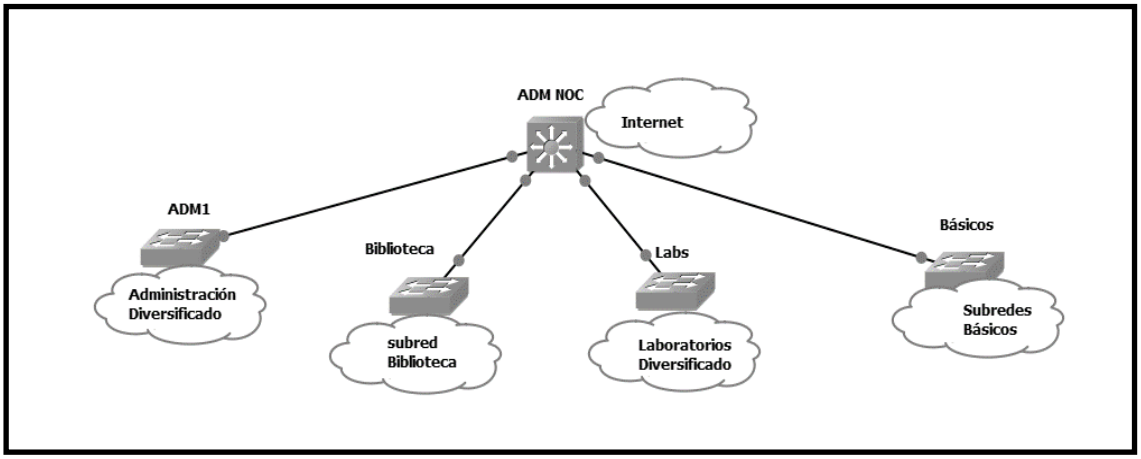
Fuente: Mecanismo de implementación de la red IPv6.

Esta empresa proporcionara una dirección de red para ser utilizada por Fundación Kinal con prefijo /48, esto mientras un proveedor de servicios local pueda ofrecer este servicio.

2.1.1. Topología lógica

La Topología lógica actual de Fundación Kinal es la representada en la figura 11. Funciona como una estrella extendida como se muestra en la figura 12.

Figura 12. **Topología lógica Fundación Kinal**



Fuente: Departamento IT Fundación Kinal.

Los equipos de la red de Fundación Kinal, tienen instalados los siguientes sistemas operativos que se detallan en la tabla IV.

Tabla IV. **Sistemas operativos Fundación Kinal**

Equipos	Sistema Operativo	Soporte para IPv6
Servidores	Windows server 2008	Si
Servidor Proxy	ClearOS	Si
Clientes	Windows XP	hay que instalarlo
Clientes	Windows Vista	Si
Clientes	Windows 7	Si
Clientes	Windows 8	Si
Teléfonos IP	Basado en Linux	Si

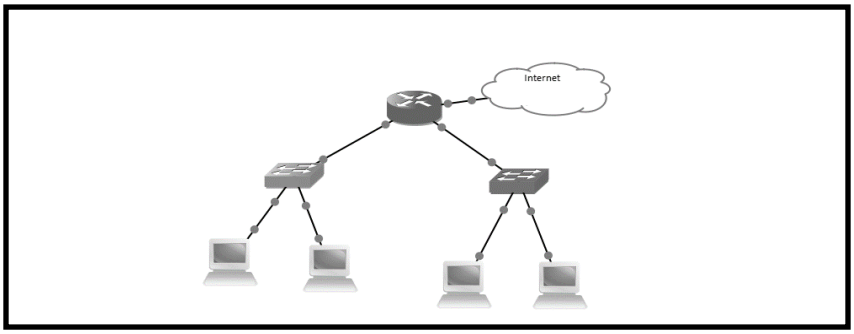
Fuente: Departamento de IT Fundación Kinal.

En el sistema operativo Windows XP, hay que instalar el protocolo IPv6, para que exista la debida comunicación entre el cliente y todos los servicios IPv6 del servidor.

2.1.2. Topología física

En la figura 11 se observa la topología física de la red de Fundación Kinal, ahora bien para el prototipo de red utilizará la siguiente topología:

Figura 13. **Diagrama de prototipo de red**



Fuente: elaboración propia.

2.2. Implementación de prototipo de red

Una red prototipo consta sólo de la porción de red necesaria para probar una función o capacidad especifica. La red prototipo debe estar completamente separada de la red existente y para la misma se utilizará el equipo existen en Kinal.

2.2.1. Descripción del escenario

El prototipo de red consta de dos redes de computadoras, se utilizaran equipos con sistema operativo Windows XP e IPv6 instalado y equipos con sistema operativo Windows 7 instalado, utilizar un *router* modelo 2811 y *switches* modelo 2950, todo marca Cisco. El *router* servirá para que las direcciones IPv6 se puedan comunicar con las direcciones IPv4, además en el mismo se configurara un túnel para que Fundación Kinal pueda tener acceso a direcciones IPv6.

La infraestructura del prototipo de red de pruebas se puede ver en la figura 13, en la que se cuenta con los siguientes servicios:

- Una computadora con sistema operativo Windows XP, denominada *host*1*,* la cual estará configurada tanto con IPv4 como con IPv6.

- Una computadora con sistema operativo Windows 7, también configurada
  tanto con IPv4 como con IPv6 y que se denomina *host*2.

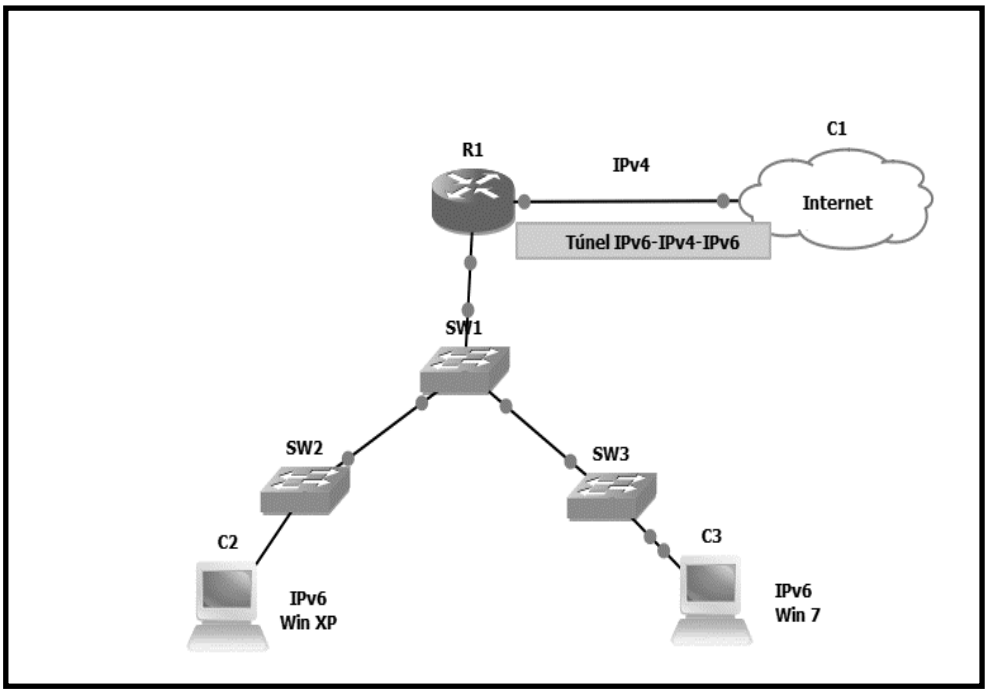
- Un *router* 2811 marca Cisco con *IOS* (Sistema Operativo) 15

- Tres *switch* modelo 2950 marca Cisco con *IOS 12.4*

El objetivo del implementar el prototipo es comprobar que se puede implementar IPv6 en la red de Fundación Kinal sin perder las funcionalidades existentes que corren sobre IPv4.

Aunque se inició con un prototipo bastante sencillo, de ser necesario se pueden agregar más equipos al mismo.

Figura 14. **Prototipo de red para IPv6**

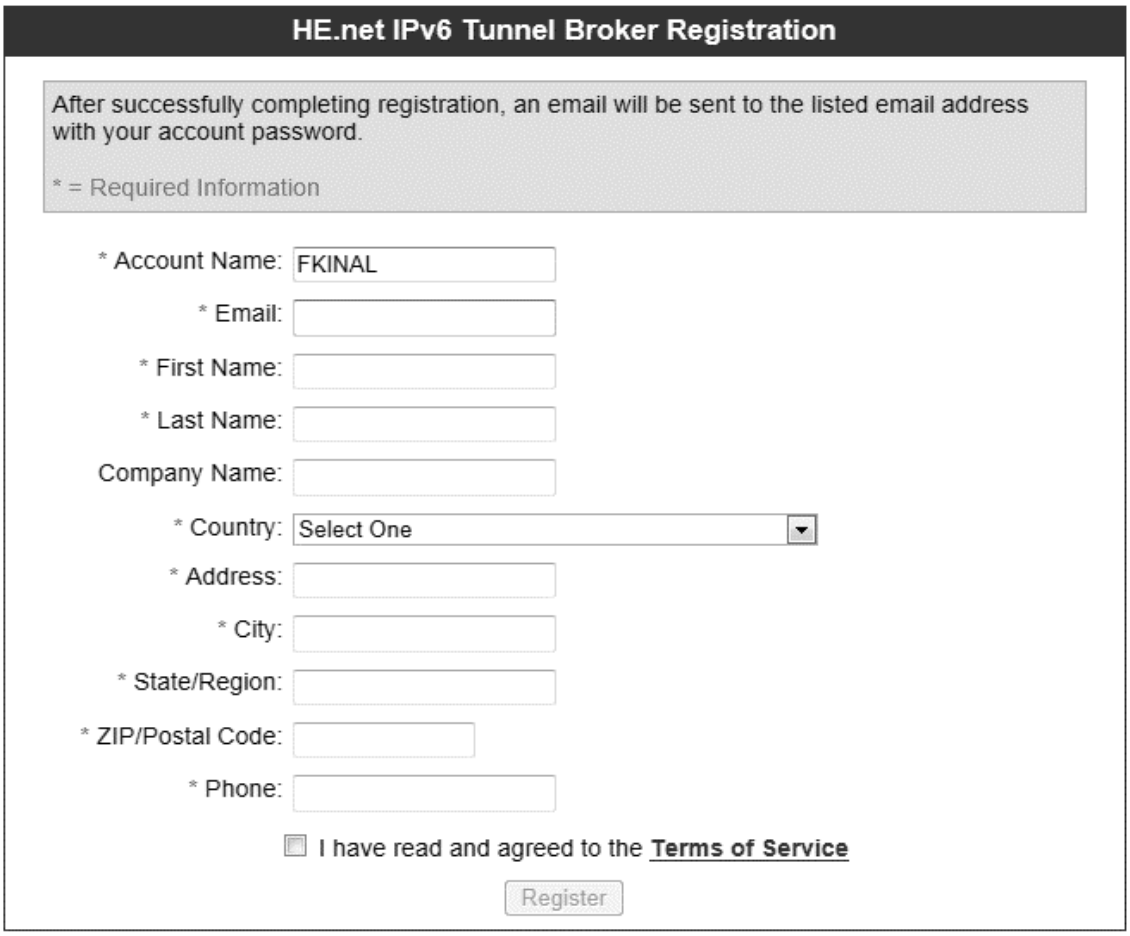


Fuente: elaboración propia.

2.2.1.1. Obteniendo el direccionamiento IPv6

Para poder obtener una red de IPv6 debe registrarse en la siguiente dirección: http://www.tunnelbroker.net/ y completando el formulario de la figura 14. El cual solicita datos básicos de la empresa, y que no es complicado de completar, para luego a vuelta de correo le proporcionan un usuario y un *password* para iniciar a hacer uso de este servicio.

Figura 15. **Formulario de registro para direcciones IPv6**



Fuente: http://tunnelbroker.net/register.php. Consulta: junio de 2013.

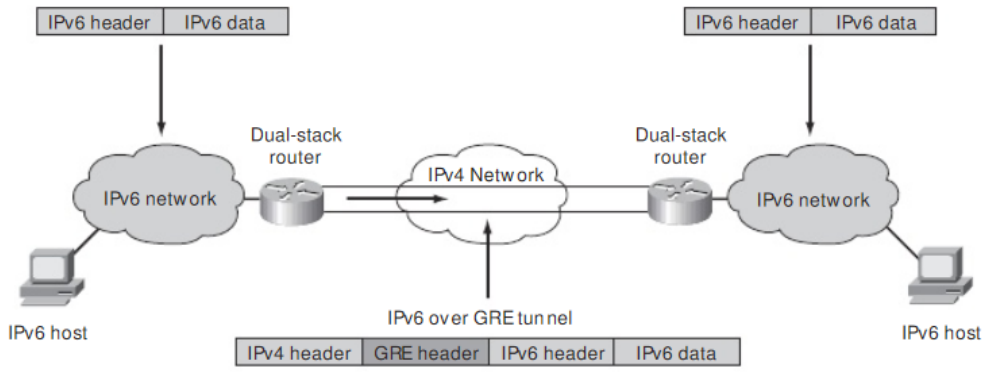
Luego de haber realizado el registro y haber sido aprobado el mismo, se procedió a utilizar una de las direcciones públicas Kinal para solicitar la aprobación de realizar un túnel hacia Miami, por medio de esta empresa.

Al haber sido aceptada la solicitud, se obtuvo la siguiente dirección de red IPv6 para ser utilizada por Fundación Kinal: 2001:470:5:A55::/48.

2.2.1.2. Configuración del *router*

Para poder manejar tráfico con IPv6 en redes separadas por enrutadores IPv4, como es este caso, es decir que la red tendrá IPv6 pero el proveedor de servicios continua dando servicios solo para IPv4, por tal razón debe recurrir a los llamados Túneles. A través de ellos se envían los paquetes IPv6 encapsulados en paquetes IPv4 hacia otra red que maneje también el protocolo. Con esto se logra unir nubes de IPv6, pero encapsulado en redes IPv4.

Figura 16. **Modelo general del esquema de túnel**



Fuente: http://www.scielo.org.co/scielo.php?pid=S0123-921X2010000200006&script=sci_arttext. Consulta: junio de 2013.

Antes de la creación de los túneles fueron necesarios varios datos:

Tabla V. **Parámetros para la configuración del túnel**

Datos para la Configuración del Túnel	
Dirección IPv4 Local	168.234.170.245
Dirección IPv4 remota	209.51.161.58
Dirección IPv6 Local	2001:470:4:A55::2/64
Dirección IPv6 remota	2001:470:4:A55::1/64

Fuente: elaboración propia.

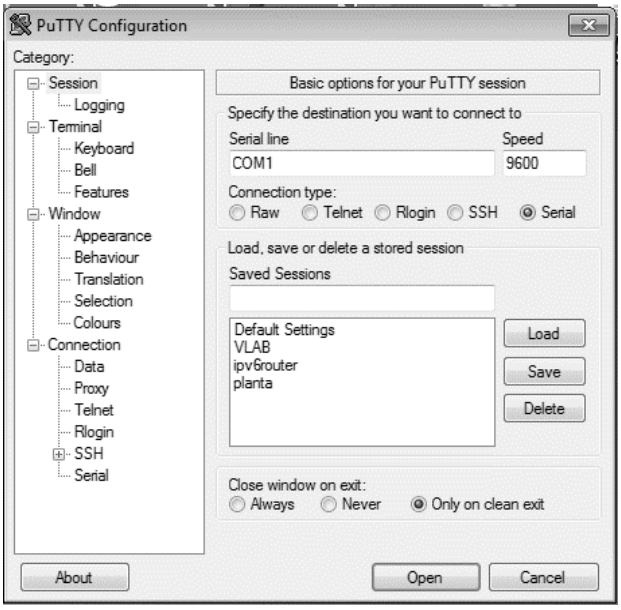
Se procede a explicar la configuración del *router:*

- Conecte el cable de consola al puerto serial o a un convertido de USB a DB-9.

- Utilizar el programa Putty para configurar el *router* utilizando el puerto COM 1 manteniendo la siguientes propiedades:

    - Bits por segundo: 9600
    - Bits de datos: 8
    - Paridad: None
    - Bits de Parada: 1
    - Control de flujo: None

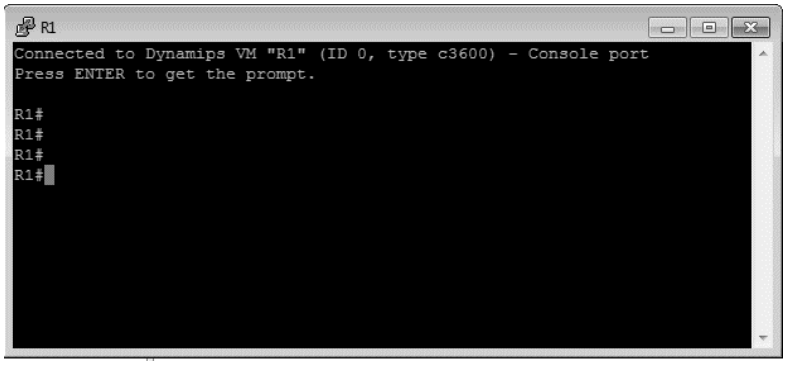
Figura 17. **Cliente para conexión remota Putty**



Fuente: imagen tomada de escritorio de Windows 7.

- Cuando se habrá la ventana de sesión de Putty, presione la tecla Intro hasta recibir respuesta del *router.*

Figura 18. **Conexión por consola al *router***



Fuente: imagen de consola de Putty tomada de escritorio de Windows 7.

- Si el *router* no tiene ninguna configuración, seguro estará en el modo de configuración, salga ingresando NO.

- Para ver lo que se configuró y cómo se configuro el *router,* se despliega la configuración del mismo.

- Si el símbolo dentro de Putty es de esta forma: *router>* indica que esta en el modo de usuario y debe pasar al modo de usuario privilegiado ingresando el comando siguiente: router>enable.

- Para realizar las configuraciones dentro del *router* debe ingresar al mode de configuración global ingresando el siguiente comando: configure terminal, para salir de este modo puede escribir la palabra end.

- Inicie colocando un nombre al *router* utilizando el siguiente comando desde modo de configuración global: *hostname* PrototipoIPv6.

  router(config)# *hostname* PrototipoIPV6
  (Es necesario configurar el nombre del *router* sino no dejar configurar SSH).

  PrototipoIPV6 (config)# ip domain-name Kinal.edu.gt
  (Cisco se basa en estas 2 variables para generar las claves RSA. El nombre y el Dominio para generarlas).

  PrototipoIPV6 (config)#crypto key generate rsa 1024
  (Genera las claves RSA con un tamaño de 1024 bits).

  PrototipoIPV6 (config)#ip ssh time-out 30

(Configura el tiempo de espera esto es en segundos).
PrototipoIPV6 (config)#ip ssh authentication-retries 3
(Configura un máximo de logins fallidos).

PrototipoIPV6 (config)#ip ssh version 2
(Habilitar de SSH versión 2).

PrototipoIPV6(config)#username Kinal privilege 15 password 4dcbl0g5p0t
(Configura los Usuario que tendrán acceso vía SSH y los privilegios).

PrototipoIPV6 (config)#line vty 0 4
(Línea donde se aplicara el SSH).

PrototipoIPV6 (config-line)# transport input ssh
(Activa el SSH en la línea VTY).

PrototipoIPV6 (config-line)# login local
(Para que se haga uso del usuario).

Todo lo que aparece entre paréntesis solo es descripción de los comandos utilizados.

Las siguientes tablas muestran la configuración realizada para IPv6:

Tabla VI. **Configuración básica de un *router***

Configuración Basica del Router	
Descripción	**Comandos**
habilitar IPv6	R1(config)# IPv6 unicast-routing
Crear una ruta por defecto para IPv4	R1(config)# ip route 0.0.0.0 0.0.0.0 168.234.170.244
Crear una ruta por defecto para IPv6	R1(config)#ipv6 route ::/0 Tunnel0
Dar permiso a una red para navegar por IPv4	R1(config)#ip access-list standard HOST permit 172.16.0.0 deny any
Configurar NAT para que naveguen los usuarios por IPv4	R1(config)#ip nat inside source list HOST interface FastEthernet0/0 overload

Fuente: elaboración propia.

La tabla VI muestra como habilitar IPv6, así como la manera de permitir a los usuarios que puedan seguir navegando por IPv4.

Tabla VII. **Configuración de las interfaces de un *router***

Configuracion de la interfaces	
Descripción	**Comandos**
Ingresar a modo de Configuración	R1#Configure Terminal
En modo de configuración ingresar los siguientes comandos	interface FastEthernet0/0 description */Esta interfaz conecta con el proveedor de servicios /* ip address 168.234.170.245 255.255.255.224 ip nat outside no shutdown exit interface FastEthernet1/0 Description */interfaz con configuración dual stack /* ip address 172.16.16.254 255.255.255.0 duplex auto speed auto ipv6 address 2001:470:4:A55::1/64 ipv6 enable no shutdown exit

Fuente: elaboración propia.

La tabla VII muestra la configuración de *dual stack* en la interfaz FastEthernet 1/0.

Tabla VIII. **Configuración de *tunneling***

Configuración del Tunel	
Descripción	**Comandos**
Ingresar a modo de Configuración	R1#Configure Terminal
En modo de configuración ingrese los siguientes comandos	interface Tunnel0 description Hurricane Electric IPv6 Tunnel Broker no ip address ipv6 address 2001:470:4:A55::2/64 ipv6 enable tunnel source 168.234.170.245 tunnel destination 209.51.161.58 tunnel mode ipv6ip

Fuente: elaboración propia.

La tabla VIII muestra la configuración que se realizó para que los datos de IPv6 puedan pasar por el proveedor de servicios sin problema a pesar de que él aun no proporciona el servicio de IPv6.

Tabla IX. **Configurar servidor de DHCP para IPv6**

Configuración de DHCP	
Descripción	**Comandos**
Ingresar a modo de Configuración	R1#Configure Terminal
En modo de configuración ingrese los siguientes comandos	ipv6 dhcp pool ADM address prefix 2001:470:4:A55::/64 lifetime infinite infinite dns-server 2001:4860:4860::8888 domain-name kinal.edu.gt
Aplicando el Pool de DHCP	interface FastEthernet0/1 ipv6 address 2001:470:5:A55::1/64 ipv6 enable ipv6 nd other-config-flag ipv6 dhcp server ADM end

Fuente: elaboración propia.

Como se puede ver en la configuración, se utilizó DHCP para IPv6, esto con el fin de seguir el lineamiento utilizado por Fundación Kinal para la asignación de direcciones IP.

2.2.1.3. Configuración de los *host*

Todas las versiones de XP, incluyen IPv6 preinstalado, pero es preciso habilitarlo, para ello se debe seguir los siguientes pasos:

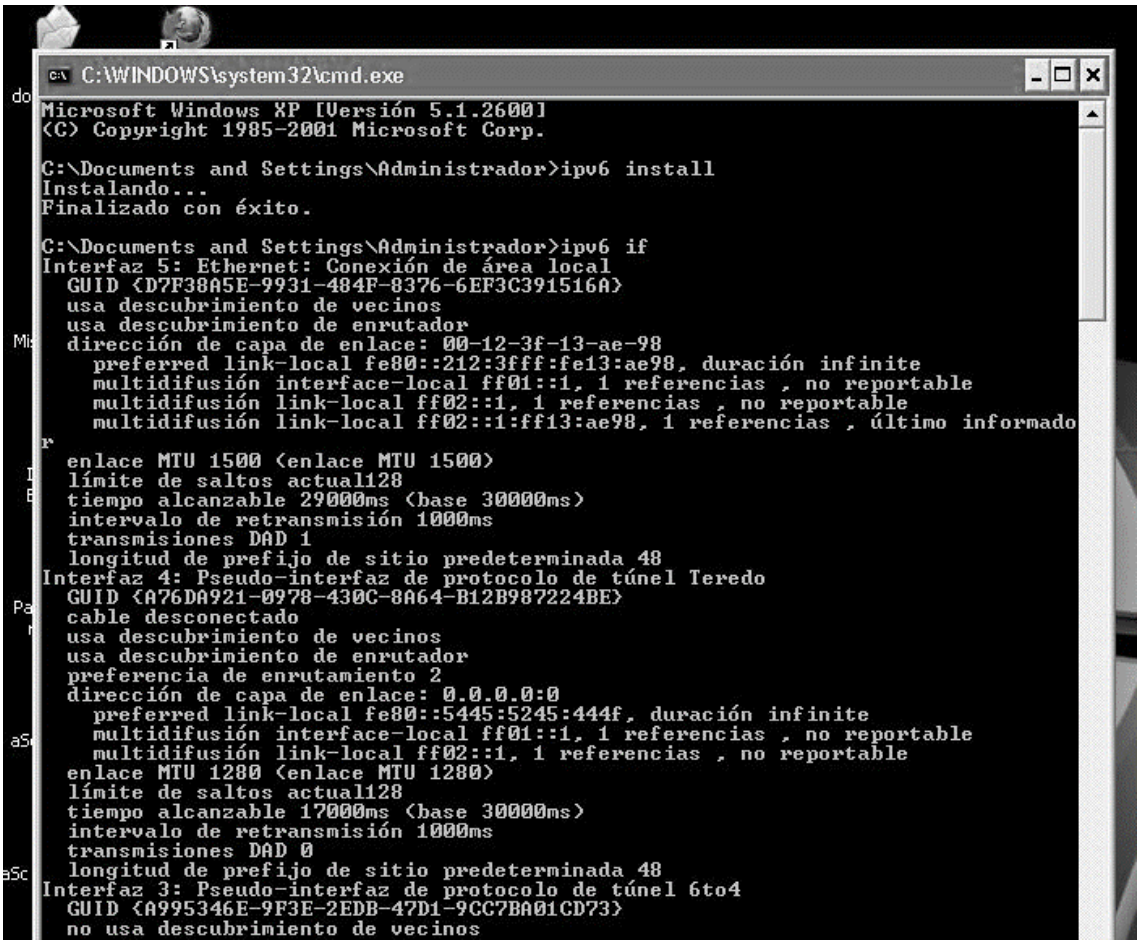
Paso 1. Ingresar al modo consola mediante el comando cmd.

Paso 2. Una vez con privilegio de administrador, se ejecuta el *comando ipv6 install.*

Aparecerá un mensaje indicando que se ha configurado exitosamente.

Para comprobar que la instalación se ha culminado con éxito se usa *ipv6 if* y se despliega el resultado mostrado en la figura 19:

Figura 19. **Configuración de IPv6 en Windows XP**

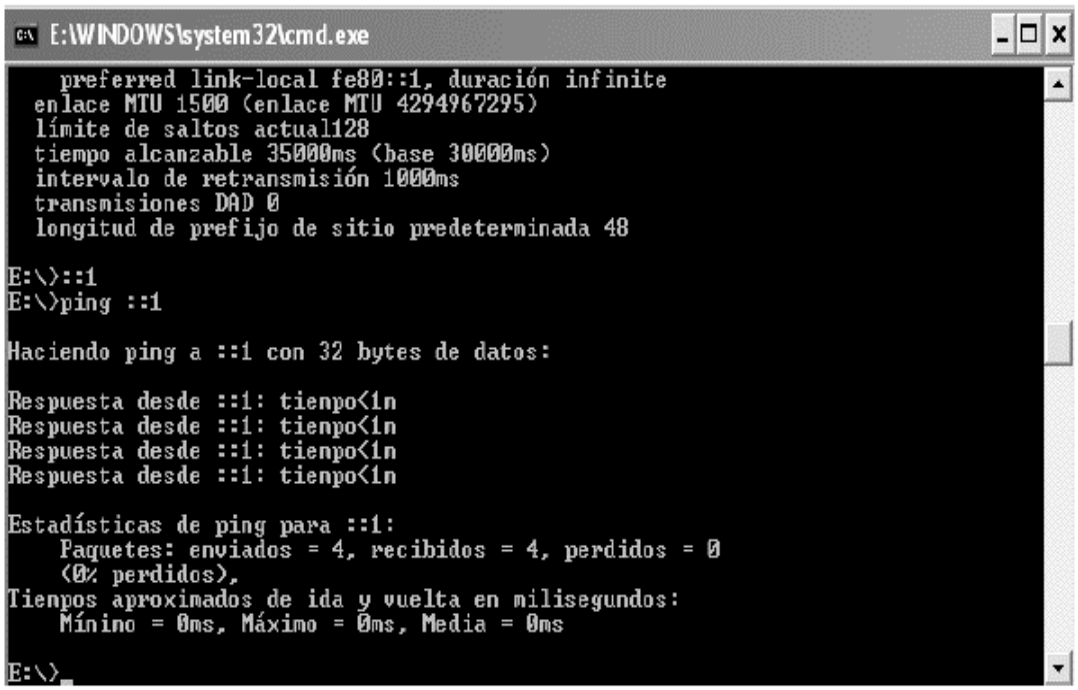


Fuente: imagen de interface de línea de comandos en escritorio de Windows XP.

La figura 19 muestra la configuración y las direcciones IPv6 adquiridas para cada interfaz.

Se puede comprobar el correcto funcionamiento de IPv6 con el comando Ping ::1

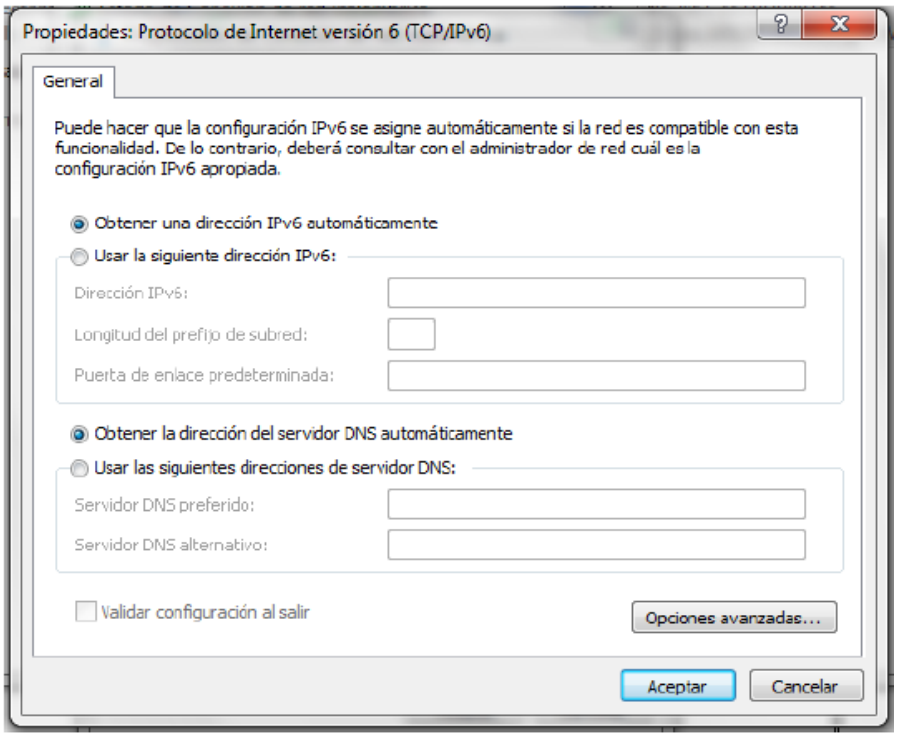
Figura 20. **Prueba de IPv6 en Windows XP**



Fuente: imagen de interfaz de línea de comandos de Windows XP.

Los sistemas operativos Windows Vista, Windows 7 y Windows 8, cuentan con la última implementación IPv6 desarrollada por Microsoft, la cual incorpora todas las características definidas por el protocolo como se muestra en la figura 21.

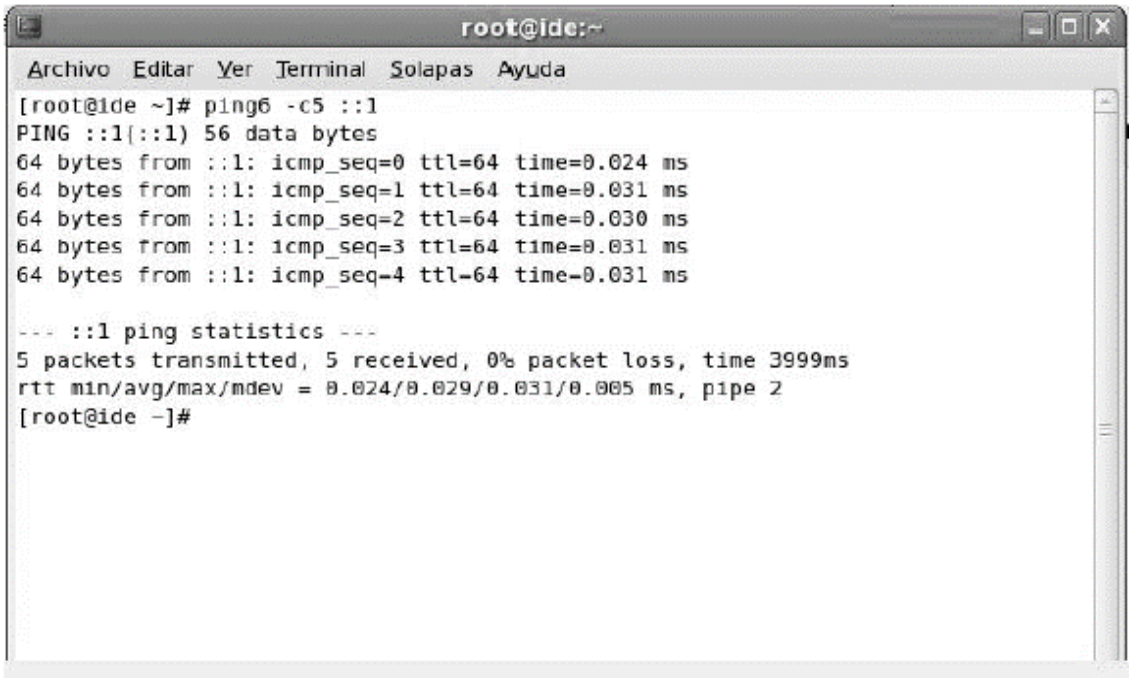
Figura 21. **Interfaz gráfica para IPv6**



Fuente: Imagen de la propiedades de interfaz tomada de Windows 8.

En cuanto a los sistemas operativos basados en Linux, a pesar que Fundación Kinal no tiene computadoras con sistemas operativos basados en Linux se realizaran pruebas en Centos. Este sistema operativo cuenta soporte IPv6 oficialmente instalado desde la versión 2.2 pero se recomienda tener una versión más reciente. Para comprobar el funcionamiento se utiliza el comando ping –c5 ::1 como se muestra en la figura 22.

Figura 22. **IPv6 en Linux**



Fuente: imagen de interfaz de línea de comandos de Linux.

Como se puede observar el ping fue exitoso, el sistema está preparado para IPv6.

2.2.2. Pruebas sobre la simulación

En la actualidad no se está migrando a IPv6, el término correcto es Transición es así que se desarrollan diferentes aplicaciones duales tanto para IPv6 como para IPv4, este sin número de aplicaciones tienen algún tipo de soporte para IPv6, como se muestra en la tabla X.

Tabla X. **Aplicaciones de uso común**

Aplicaciones	Paginas Web	IPv6	Notas
Explorer		X	Versiones superiores a la 7.0
Firefox		X	Versiones superiores a la 6.0
Safari		X	
Thunderbird		X	
	Facebook	X	IPv6
	Google	X	IPv6
	Yahoo	X	IPv6

Fuente: elaboración propia.

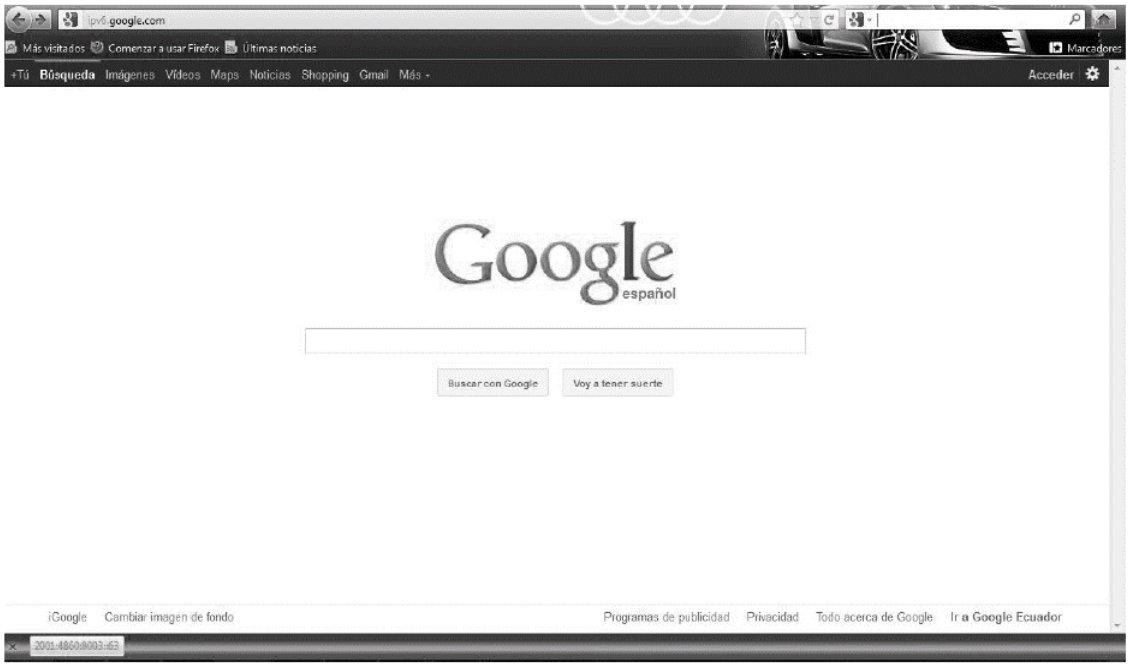
Como se muestra en la figura 23 una de las principales redes sociales posee una plataforma en IPv6, como lo es Facebook.

Figura 23. **Página IPv6 para Facebook**

Fuente: http://www.v6.facebook.com. Consulta: septiembre de 2013.

Al igual uno de los buscadores más utilizados posee una plataforma IPv6, como lo es Google.

Figura 24. **Buscador google para la versión de IPv6**



Fuente: http://ipv6.google.com. Consulta: septiembre de 2013.

Una vez obtenida la dirección de IPv6 por medio de DHCP se procedió a realizar pruebas obteniendo los siguientes resultados:

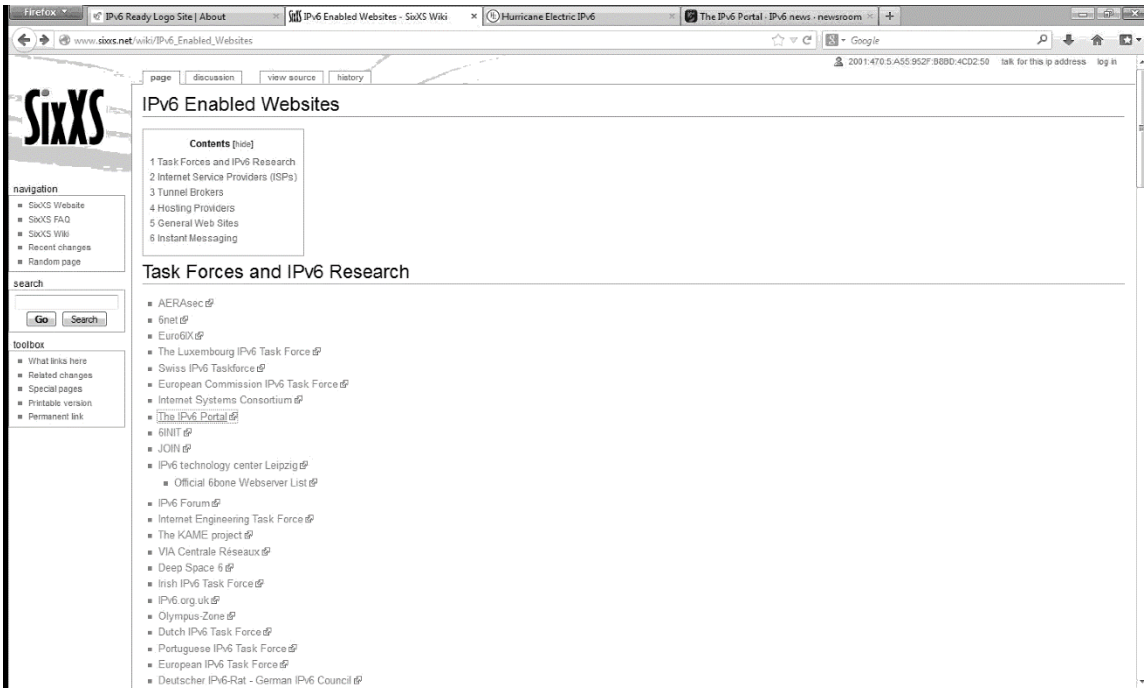
Figura 25. **Navegar en IPv6**

Fuente: http://www.ipv6tf.org/index.php. Consulta septiembre de 2013.

Para algunos navegadores como Firefox Mozilla es recomendable descargar un *plugin*, para este caso debe descargarlo desde: https://addons.mozilla.org/en-US/firefox/addon/showip/.

Esto permite visualizar en Firefox la dirección IPv6 o IPv4 al iniciar la navegación a la página web que se esté accediendo.

Figura 26. **Comprobando el funcionamiento de IPv6**



Fuente: http://www.sixxs.net/wiki/IPv6_enabled_websites. Consulta: septiembre de 2013.

2.2.3. Limitaciones del prototipo de red

Se logró simular la mayoría de ambientes de trabajo que posee Fundación Kinal sin mayores inconvenientes, las únicas limitaciones que ha presentado este prototipo de red han sido la cantidad de equipos que se han podido conectar simultáneamente al mismo.

2.3. Diseño plan piloto

Habiendo realizado las pruebas necesarias en la red prototipo se procedió a integrar el protocolo *dual stack* a la red de Fundación Kinal, pero se

implementó únicamente con una VLAN que en este caso ha dado acceso a la VLAN 11.

2.3.1. Descripción de tareas a realizar

La planificación de IPv6 puede ser estructurada por los siguientes aspectos:

- Direccionamiento
- Ruteo
- Seguridad
- Servicios

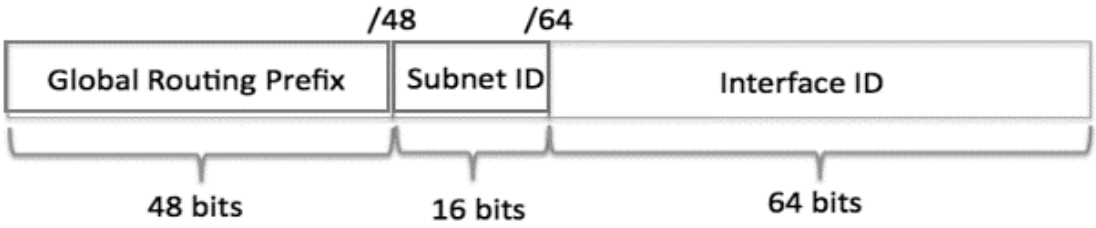
2.3.1.1. Plan de direccionamiento

En la nueva versión del protocolo IP se cuenta con un espacio de direcciones mucho más amplio, lo que hace innecesarias técnicas como NAT, esto significa que se debe rediseñar el plan de direcciones con el fin de implementar IPv6.

Siguiendo las recomendaciones del documento RFC 3177, se debe de asignar un prefijo /48 a cada sitio, para este caso este será el prefijo para Fundación Kinal.

La forma de crear subredes será utilizando el siguiente esquema:

Figura 27. **Esquema para crear subredes**



Fuente: elaboración propia.

Para este caso la división que se realizó fue acorde a lo siguiente: dado que la red de Kinal está dividida en VLANs, o sea LAN virtuales, las cuales estan configuradas en cada uno de los *switch*, se mantuvo esta estructura dado que es una excelente manera de segmentar las redes y se distribuyeron las redes de la forma siguiente:

- Administración 100 computadoras
- 9 laboratorios con un promedio de 30 computadoras por laboratorio
- Direcciones para 3 servidores.
- Direcciones para administrar cada dispositivo de red 23 direcciones

Para lo anterior utilizar la dirección de IPv6 siguiente: 2001:470:4:A55::/48. Con la siguiente distribución:

Figura 28. **Distribución de subredes IPv6**

VLAN	Descripción	Sub red de IPv6
VLAN 11	Plan Piloto	2001:470:4:A55:D3B3::/64
VLAN 20	Laboratorio C23, C26	2001:470:4:A55:1AB1::/64
VLAN 30	Laboratorio C27, C28, C29	2001:470:4:A55:1AB2::/64
VLAN 40	Laboratorio F17, H32, H22 y G42	2001:470:4:A55:1AB3::/64
VLAN 50	Administración Diversificado	2001:470:4:A55:ADD1::/64
VLAN 60	Administración Básicos	2001:470:4:A55:ADBA::/64
VLAN 70	Red Inalámbrica	2001:470:4:A55:CAFE::/64

Fuente: elaboración propia.

Para este caso se implementó la VLAN 11, con las mismas configuraciones realizadas prototipo de red, las otras VLAN tienen una configuración similar.

2.3.1.2. Plan de ruteo

El plan de ruteo pretende mantener un esquema similar al ocupado actualmente por IPv4, para evitar tener dos redes de topología distintas, y dado que en este caso se utiliza un túnel, la única implementación necesaria es la del túnel en el *router* que conecta al proveedor de servicios, sin embargo en el apéndice B se mostrara como implementar un protocolo de enrutamiento pensando en el crecimiento de la red.

2.3.1.3. Plan de seguridad

Dado que como mejora de la red se implementó un *firewall* con Fortinet, se debe tener en cuenta al momento de realizar configuraciones en el mismo que se deben mantener activos los registros de eventos.

Los mensajes ICMPv6 son necesarios debido a que por medio de los mismos si en los extremos se realizó fragmentación esta es la forma de darlos a conocer.

Se debe tener cuidado de que los nodos no se unan a grupos de *multicast* innecesarios y los *firewall* deben evitar la salida de este tipo de información.

En general debe recordar que aunque las políticas son similares a las aplicadas en IPv4, debe recordar que IPv4 e IPv6 trabajan de forma independiente.

2.3.1.4. Plan de servicios

- Servicios web: si bien la mayoría de servidores web ya proveen soporte para IPv6, el soporte puede haber sido desactivado por los administradores de sistemas. Por lo tanto la transición hacia IPv6 puede requerir cambios de configuración. En el caso de navegadores web es similar. Existe un amplio soporte de IPv6 por parte de los navegadores, pero se requiere revisar que no esté deshabilitado.

- Los servidores de correo por el momento seguirán funcionando en IPv4 dado que estan en la nube y no en las instalaciones de Fundación Kinal.

- El servicio DNS a utilizar será el que provee Google para IPv6

2.3.2. Guía detallada para la implementación

Dado que la configuración para IP versión cuatro se mantiene integra, esto gracias al método de migración seleccionado, los pasos a seguir son los siguientes:

2.3.2.1. Configuración del *router* de núcleo

Para cada una de las VLAN debe configurar un grupo (*pool*) de direcciones, por ejemplo para la VLAN 11 la configuración es la siguiente:

Tabla XI. **Configuración de DHCP**

Configuración de DHCP	
Descripción	**Comandos**
Ingresar a modo de Configuración	R1#Configure Terminal
En modo de configuración ingrese los siguientes comandos	ipv6 dhcp pool ADM address prefix 2001:470:4:A55:D3B3::/64 lifetime infinite infinite dns-server 2001:4860:4860::8888 domain-name kinal.edu.gt
Aplicando el Pool de DHCP	interface FastEthernet0/1.11 encapsulation dot1Q 11 ipv6 address 2001:470:5:A55:D3B3::1/64 ipv6 enable ipv6 mtu 1452 ipv6 nd other-config-flag ipv6 dhcp server ADM end

Fuente: elaboración propia.

Esto se debe repetir por cada VLAN que se tenga.

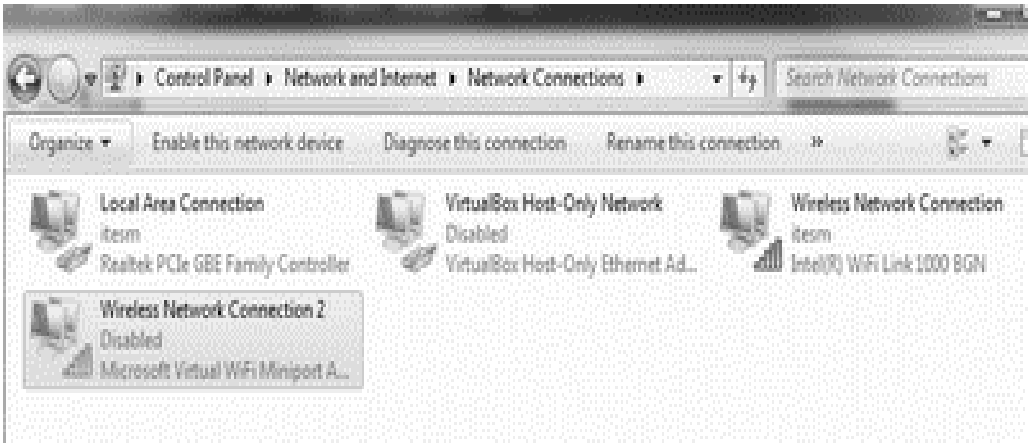
Con respecto a los clientes hay que seguir los siguientes pasos:

Activa IPv6: IPv6 ya viene instalado en los sistemas operativos más actuales, por lo que técnicamente se activa y no se instala. Para instalar IPv6 en Windows XP/2003, acude a Inicio/ejecutar/cmd y abre una ventana de comandos. Escribe ipv6 install y un mensaje de confirmación indicará el éxito de la operación. Si experimentas problemas, prueba de manera alternativa netsh interface ipv6 install. También puedes buscar en panel de control/conexiones de red e Internet/conexiones de red cualquiera de los iconos conexión de área local o Conexiones de red inalámbricas y acceder a Propiedades/General. Allí, busca Microsoft TCP/IP versión 6 (1) y dale a Instalar/Protocolo (2). En cuanto a Windows Vista, 7 u 8, el soporte para IPv6 ya viene instalado y habilitado por defecto. No obstante, en caso de desactivación involuntaria, se pueden utilizar los procedimientos indicados para XP/2003: la ejecución de netsh en ventana DOS o el acceso mediante el Panel de Control.

Los Sistemas Operativos Windows 7 y 8 tienen integrado por defecto los protocolos de IPv6 e IPv4 y en general ofrecen un buen servicio aunque el *stack* es algo primitivo, ya que solo es una modificación del *stack* liberado por Microsoft en agosto del 2004 para su Sistema Operativo Windows XP SP2 y por lo mismo está hecho con los RFC que definían a IPv6 en aquel entonces.

Para acceder a la ventana de configuración de IPv6 de alguna interfaz de red es necesario llegar primero al *Network and Sharing Center* el cual puede ser accedido desde el panel de control o desde el icono de red que aparece en la parte derecha de la barra de tarea. Desde ahí se selecciona *Change adapter settings* (Centro de redes y recursos compartidos).

Figura 29. **Interfaces de redes Windows Vista, 7 y 8**

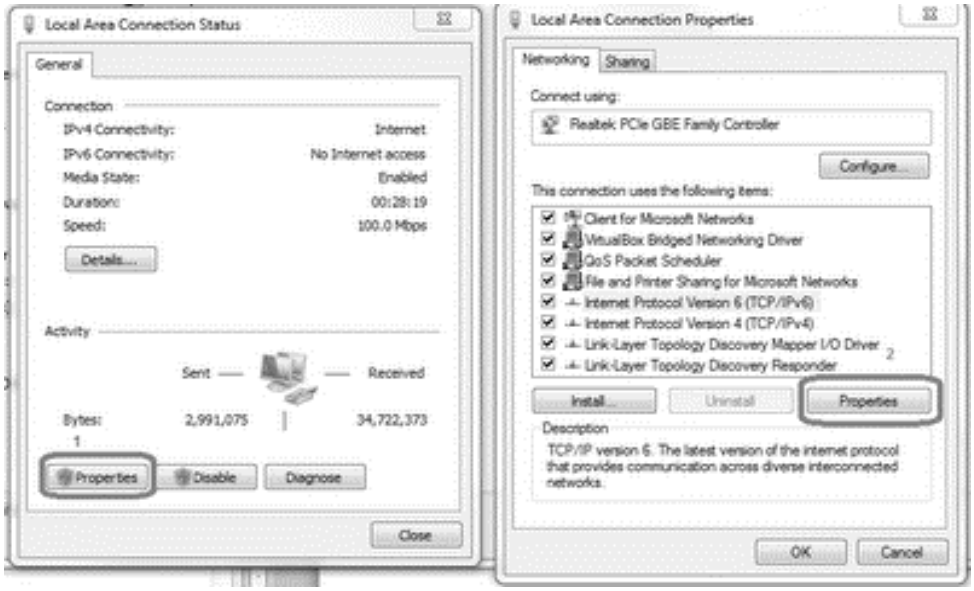


Fuente: imagen de interfaces de red en Windows 8.

Se debe de seleccionar la interfaz que se desea configurar y aquí es importante entender que al estar habilitados IPv4 e IPv6 es muy probable que Windows tenga interfaces lógicas para los túneles Teredo.

Una vez seleccionada la interfaz, se hace clic derecho sobre ella y en la ventana emergente se escoge Propiedades (en la imagen de abajo es el botón marcado con el número 1). Para este paso el usuario debe poseer privilegios de redes o bien ser un usuario administrativo.

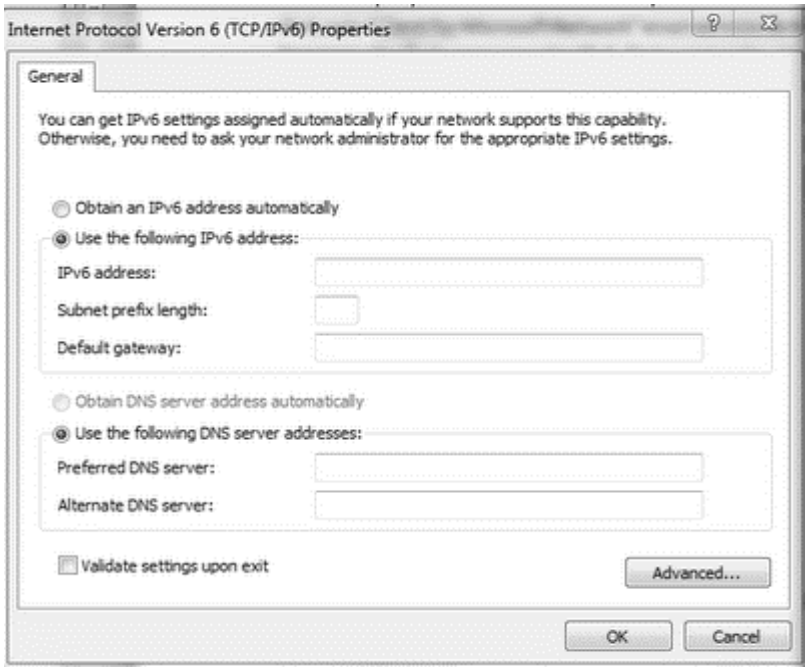
Figura 30. **Configurando IPv6**



Fuente: imágenes de configuración de redes tomadas de Windows 8.

De las opciones ahí presentes tome el protocolo *Internet Protocol Version* 6 (TCP/IPv6) una vez seleccionado se hace clic en el botón 2 (Propiedades) Para que se abra una nueva ventana de propiedades del protocolo como la que se muestra a continuación:

Figura 31. **Configurar la forma en que se obtendrá la dirección IPv6**



Fuente: imagen de configuración de TCP/IP versión 6 tomada de Windows 8.

Debe seleccionar la configuración automática, dado que está utilizando DHCP.

2.3.3. Restitución (*rollback*) en caso de falla

Lo primero que se realiza antes de proceder a configurar los dispositivos de red, *router* o *swith*, es guardar una copia de la configuración de los mismos, la cual se obtiene por medio del comando *show running-config y se copia* en un block de notas. En caso de falla debe aplicar esta configuración a los dispositivos de red, copiándola y pegándola en modo de configuración global del *router* o *switch.*

Con respecto a los equipos de los clientes, no deben experimentar problemas, dado que *dual stack* les permite utilizar simultáneamente IPv4 o IPv6.

2.3.4. Tiempo necesario estimado para la implementación

Dado que el proveedor de servicios no ha dado una fecha en la cual de soporte a IPv6, la implementación final se realizara cuando ellos estén listos, sin embargo todas las VLAN estarán configuradas para IPv6 a partir del segundo semestre de 2014.

3. FASE DE ENSEÑANZA-APRENDIZAJE

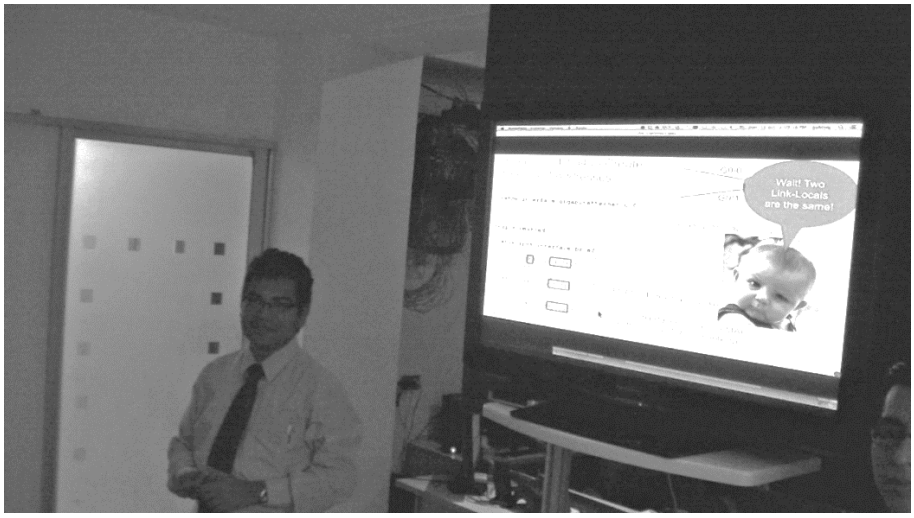
3.1. Capacitación al Departamento de IT

Se impartieron dos cursos al Departamento de IT, el primero para que conozcan el protocolo de red IPv6 y el segundo para aprender a implementarlo en los que se trataron los siguientes temas:

- Fundamentos de IPv6

Se realizaron dos cursos durante los cuales se explicó a detalle al Departamento de IT tanto la parte teórica como práctica del protocolo IP en la versión 6.

Figura 32. **Curso de IPv6**



Fuente: Sala de Capacitación, tema IPv6.

- Métodos de migración

Se realizaron demostraciones de configuraciones y pruebas con equipos reales de las ventajas y desventajas de los diferentes métodos de migración.

- Configuración de equipos

El prototipo de red dio la confianza necesaria para que el Departamento de IT configurara equipos sin la preocupación de que los resultados obtenidos afectaran los procesos diarios de Fundación Kinal.

Figura 33. **Configuración de IPv6 en un *router***

Fuente: Laboratorio H-32.

3.1.1. Resultados de la presentación

Luego de la presentación se obtuvieron los siguientes resultados:

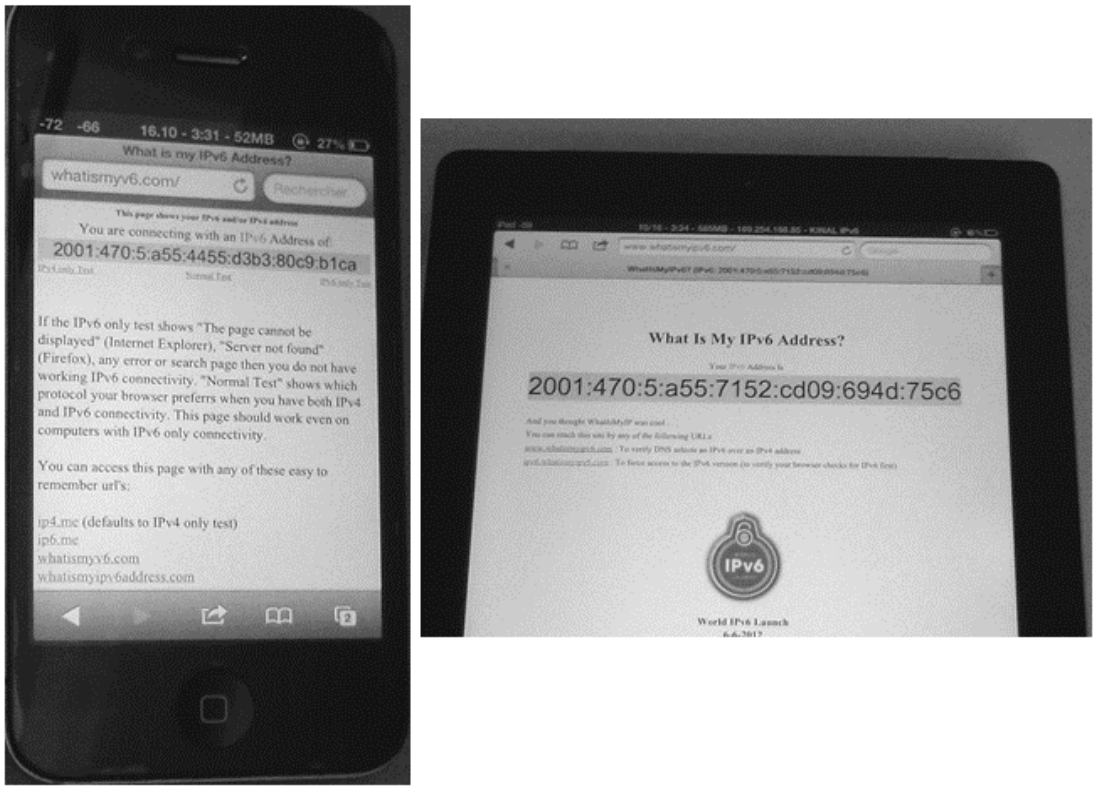
- Los participantes comprendieron las ventajas de migrar a IPv6 en una etapa temprana, pues esto le da una ventaja competitiva porque conocen el protocolo y pueden participar en otras implementaciones del mismo.

- Los participantes indicaron que el protocolo es mucho más sencillo de lo que ellos pensaban, dado que hay tantas direcciones consideraban que sería muy complicado utilizarlo, pero se encontraron con que no es así.

- Se logró disminuir la resistencia al cambio, luego de haber realizado pruebas en el prototipo de red, al momento de participar en el plan piloto realizaron las configuraciones con toda confianza sabiendo que tanto las aplicaciones de IPv4 como las de IPv6 pueden convivir.

- Luego de la implementación del plan piloto se demostró que los dispositivos móviles con IOS se unen sin mayor problema a IPv6 no así los dispositivos con Android.

Figura 34. **Dispositivos móviles conectados a IPv6**

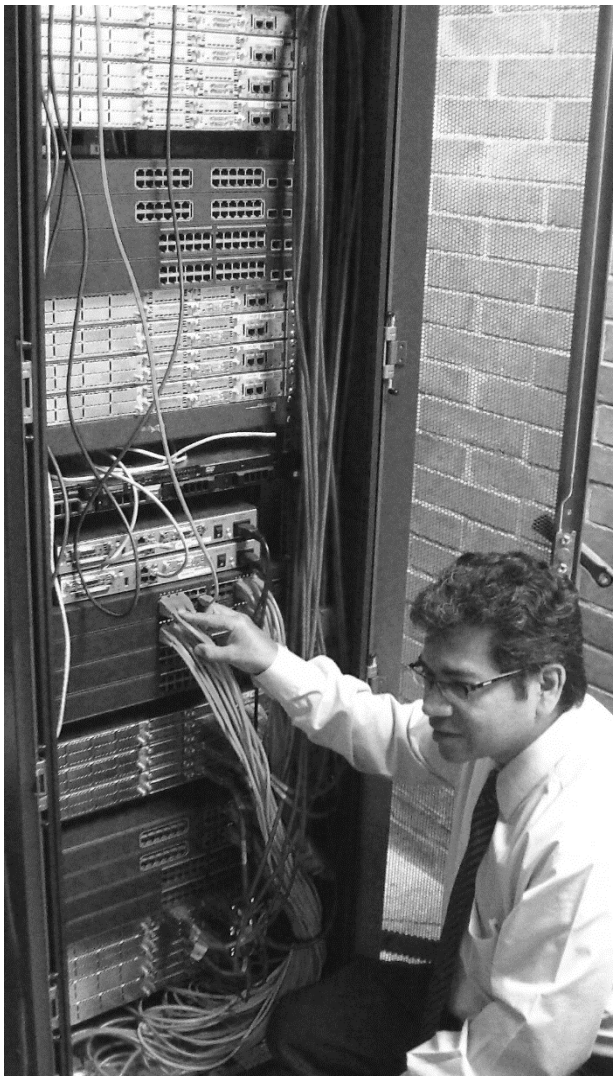


Fuente: pruebas realizadas en dispositivos móviles MAC.

3.1.2. Implementación de mejoras

- Se remplazaron varios de los *switch* de Cisco Catalyst 2960 por *switch* Cisco 3560.

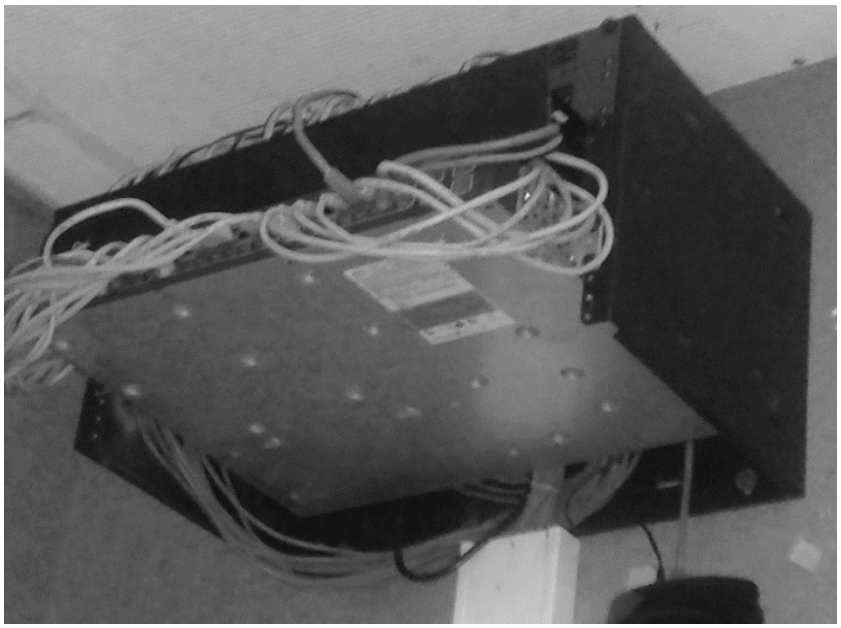
Figura 35. **Revisión de equipos Cisco instalados**



Fuente: equipos principales de la red de Fundación Kinal.

- En las áreas donde existe telefonía IP se aprovechó la característica de *power over Ethernet* para dar alimentación a los teléfonos por medio del cableado de red UTP categoría 5.

Figura 36. **Nuevos equipos instalados**



Fuente: equipos en sala de profesores.

- Se dejó Implementado *dual stack* en la VLAN 11 de la red de Fundación Kinal, la cual fue implementado por el personal de Kinal, lo que indica que pueden migrar el resto de la red sin ningún problema.

Figura 37. **Página en *dual stack***

Fuente: http://www.cedia.org.ec. Consulta: septiembre de 2013.

CONCLUSIONES

1. Se ha podido implementar un plan piloto para la transición de IPv4 a IPv6, utilizando el Protocolo *dual stack* en Fundación Kinal, logrando que cada estudiante o docente que desee navegar en IPv6 dentro del campus lo pueda hacer a través de un dispositivo portátil, siempre y cuando tenga instalado IPv6 o en su defecto siguiendo los pasos antes mencionados, dependiendo del sistema operativo que tenga el dispositivo final.

2. No existen mayores diferencias en cuanto a la configuración entre las plataformas IPv4 e IPv6, ya que los comandos a emplearse son muy similares a los de IPv4, con mínimas diferencias en cuanto a la escritura y muchas semejanzas en cuanto a la estructura y funcionamiento de cada protocolo.

3. Una de las ventajas más importantes de IPv6 respecto a IPv4 es la disponibilidad de direcciones que ofrece IPv6. Mientras IPv4 tiene 2^{32} direcciones disponibles algo que en el inicio parecía interminable, IPv6 dispone de 2^{128} direcciones, es decir, cerca de 1000 sixtillones de direcciones disponibles.

4. La técnica *dual stack* ejecuta las dos pilas de protocolos IPv4 e IPv6 de manera simultánea en los nodos de la red, pudiendo navegar de manera adecuada en las diferentes páginas web con soporte tanto para IPv6 como para IPv4, en un corto tiempo de respuesta.

RECOMENDACIONES

1. Antes de dar inicio a un proyecto de transición debe verificar si los dispositivos intermedios son compatibles con IPv6, mediante el análisis de la versión de IOS que se usa en cada equipo.

2. Para actualizar el sistema operativo de los equipos de red es necesario actualizar el IOS de manera inmediata, buscando un software licenciado para el correcto funcionamiento.

3. Debe tener claro la manera en la que se encuentra estructurada la Red IPv4, para aprovechar esta distribución y a partir de la misma realizar el direccionamiento y planificación IPv6.

4. Utilizar RFC 3177, para la planificación de direcciones, debido a que es el estándar más usado y desarrollado en la actualidad.

5. Continuar con el proceso de transición de IPv4 a IPv6 con las VLANs que aún no se encuentra configuradas.

BIBLIOGRAFÍA

1. ARIGANELLO, Ernesto. *REDES CISCO: Guía de estudio para la certificación CCNP*. 2a ed. España: Alfaomega, Ra-Ma, 2011. 734 p.

2. FORD, Mat. *More operators, more Ipv6 – 2013 a flying start* [en línea]. http://www.worldipv6launch.org/blog/ [Consulta: marzo de 2013].

3. GRAZIANI, Rick. *IPv6 Fundamentals: A straighforward Aproach to Understanding IPv6.* USA: Cisco Press, 2013. 407 p.

4. HEBERT Scott. *RFC 3177 (IPv6 address assignment to end sites) has been obsoleted* [en línea]: http://slaptijack.com/networking/rfc-3177-ipv6-address-assignment-to-end-sites-has-been-obsoleted/ [Consulta: abril de 2013].

5. LACNIC. *Tutorial práctico de IPv6* [en línea]. https://lacnic.net/sp/eventos/lacnicix/tutorial_ipv6.html. Marzo 2013 [Consulta: agosto 2013].

6. MCQUERY, Steve. *Interconnenting Cisco Network Devices, part 2 (ICND2).* 3a ed. Cisco Press 2008. 383 p.

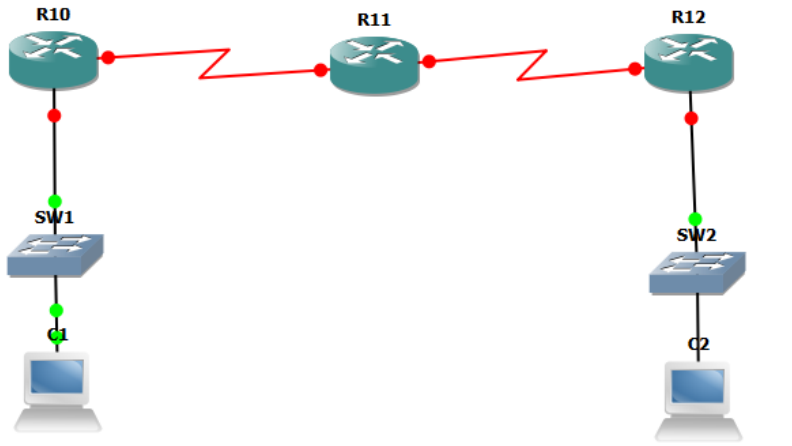
7. TEARE, Diane. *Implenting Cisco IP Routing (ROUTE) Foundation Learning Guide.* USA: Cisco Press, 2011. 929 p.

APÉNDICES

Apéndice A: Configuración de RIP con IPv6 (RIPng)

Se utilizará el siguiente diagrama para este ejemplo:

Figura A.1



Paso 1. Tabla de direccionamiento

La tabla de direccionamiento es la siguiente:

Tabla A.1

Disp.	Interfaz	Direccion IP	Prefijo	Puerta de Enlace
R10	Fa0/0	2001:470:5:A55:1ad1::1	64	
	S0/0/0	2001:470:5:A55:1ad2::1	64	
R11	S0/0/0	2001:470:5:A55:1ad2::2	64	
	S0/0/1	2001:470:5:A55:1ad3::2	64	
R12	S0/0/1	2001:470:5:A55:1ad3::1	64	
	FAa0/0	2001:470:5:A55:1ad4::1	64	
c1		2001:470:5:A55:1ad1::2	64	2001:470:5:A55:1ad1::1
c2		2001:470:5:A55:1ad4::2	64	2001:470:5:A55:1ad4::1

Tarea 1: Configuración base

Realice el cableado de acuerdo a la topología mostrada tanto de los dispositivos intermedio como de los dispositivos finales.

Aquellos dispositivos finales que ocupen una dirección estática deben ser configurados en este punto.

Tarea 2: Cargue la configuración

En esta ocasión, se utilizara una configuración pre-establecida en los enrutadores, estas instrucciones se les denomina scripts, y se pueden pasar utilizando un servicio de TFTP o por medio de una consola de terminal. Para esta práctica, se utilizará una sesión de terminal para tal propósito; la forma de pasar el script dependerá específicamente del software que esté utilizando como termina. Por lo general existen 3 aplicaciones comunes en el laboratorio de redes:

a) Hyperterminal -Encontrado por defecto en computadoras con Windows XP. Para el envío de un script vaya a opciones y seleccione enviar archivo de texto.

b) Terra-term – No instalado por defecto en computadoras con Windows 7. Extremadamente amigable para inserción de scripts, basta con seleccionar la opción de pegar.

c) GtkTerm – No instalado por defecto pero hallado en el repositorio de la mayoría distribuciones de Linux. Tiene una función similar a Hyperterminal de enviar archivos “raw” (de texto).

d) Putty se puede descargar desde Internet y es muy liviano

Sin importar que software de terminal se esté utilizando, los scripts son comandos válidos para el IOS, por lo tanto, el comando debe ser introducido en el nivel correcto, es decir, el comando “*Hostname*” solo es un comando valido en el nivel de configuración global del enrutador, no en el nivel privilegiado, interfaz global y mucho menos en el nivel de acceso público.

Para cargar los scripts se recomienda crear un archivo de texto para cada uno y en ellos colocar el texto que se muestra a continuación. Debe tener cuidado de que no aparezca texto que no corresponda a los comandos.

Paso 1: Cargue el siguiente script a R1 desde configuración global.

```
!
hostname R1
ipv6 unicast-routing
!
interface FastEthernet0/0
ipv6 address 2001:470:5:A55:1ad1::1/64
duplex auto
speed auto
no shutdown
!
interface Serial0/0/0
ipv6 address 2001:470:5:A55:1ad2::1/64
clock rate 64000
no shutdown
exit
!
banner motd ^C Solo personal autorizado! ^C
!
line con 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login
!
end
!
```

Paso 2: Cargue el siguiente script a R2

```
!
hostname R1
ipv6 unicast-routing
!
!
interface S0/0/0
ipv6 enable
ipv6 address 2001:470:5:A55:1ad2::2/64
duplex auto
speed auto
no shutdown
!
interface Serial0/0/1
ipv6 enable
ipv6 address 2001:470:5:A55:1ad3::2/64
clock rate 64000
no shutdown
exit
!
!
banner motd ^C Solo personal autorizado! ^C
!
line con 0
password cisco
login
line aux 0
line vty 0 4
password cisco
```

login

!

end

!

Paso 3: Cargue el siguiente script a R3

!

hostname R1

ipv6 unicast-routing

!

!

interface S0/0/1

ipv6 enable

ipv6 address 2001:470:5:A55:1ad1::2/64

duplex auto

speed auto

no shutdown

!

interface fa0/0

ipv6 enable

ipv6 address 2001:470:5:A55:1ad4::1/64

no shutdown

exit

!

!

banner motd ^C Solo personal autorizado! ^C

!

line con 0

password cisco

login
line aux 0
line vty 0 4
password cisco
login
!
end

Tarea 3: Examine el funcionamiento de la red

Verifique que las interfaces estén levantadas, puede utilizar los comandos **show ipv6 interface** o el comando **show ipv6 interface brief.**

Tarea 4: Configure RIP

Una vez el enrutador tenga la configuración completa se empezara a configurar el protocolo de enrutamiento RIP, el cual es extremadamente sencillo. **Estos pasos se deben de seguir en orden para la correcta contestación de la práctica.**

RIP para IPv6 funciona de forma muy parecida que RIP para IPv4, de hecho, los cambios sustanciales es que reconozca los grupos *multicast* de IPv6 (FF02::9) y las direcciones IPv6, tal como están indicados en el documento RFC2080 (Cisco, 2011). **El protocolo RIP para IPv6 es denominado RIPng** y a lo largo de esta práctica use de forma indistinta estos términos.

Paso 1: Configure la depuración para RIP en R1

Lo que se desea realizar con este paso es verificar cómo se comporta la tabla de ruteo conforme aparezcan los mensajes de RIP. Prepare el despliegue de información relacionado a RIPng con el siguiente comando:

R1#debug ipv6 rip
RIP Routing Protocol debugging is on

Paso 2: Configure RIP en R1

La configuración de cualquier protocolo de enrutamiento para IPv6 difiere de la forma tradicional en IPv4. Mientras que en IPv4 el comando era, desde configuración global, router rip en IPv6 el comando es:

(config)#Ipv6 router rip <name>

El primer campo, Name permite identificar el proceso del protocolo RIPng que está configurando a partir de un nombre, permitiendo anexar varias líneas a un mismo proceso o bien tener múltiples procesos de RIP corriendo simultáneamente en el enrutador (Algo que no se puede realizar en IPv4).

Ejecute el comando:

R1(config)#ipv6 router rip AS1

Habrá notado que ahora está en un nuevo nivel de configuración

R1(config)#ipv6 router rip AS1
R1(config-rtr)#

Por lo anterior, al introducir el comando "***ipv6 router RIP AS1***" lo único que ha hecho es crearlo, pero no tiene ninguna interfaz añadida y para hacerlo debe salir de dicho nivel.

Las siguientes líneas muestran las opciones que se tiene para RIP AS1 en una interfaz:

R1(config-rtr)#exit
R1(config)#int serial 0/0/0
R1(config-if)#ipv6 rip AS1 ?
default-information Configure handling of default route
enable Enable/disable RIP routing
metric-offset Adjust default metric increment
summary-address Configure address summarization

De las opciones que se tienen, el comando: "ipv6 rip *AS1* enable" hará que en la interfaz serial 0/0/0 participe en el proceso AS1 (que opera como un protocolo de enrutamiento RIP) con lo cual dicho proceso compartirá y aprenderá rutas con cualquier otro enrutador que mande algún mensaje de RIP.

Introduzca el comando en esa interfaz. Como se tiene la depuración habilitada debe de aparecer algo similar a lo desplegado a continuación: al habilitar el RIP en esa interfaz.

R1(config-if)#ipv6 rip AS1 enable
R1(config-rtr)#exit

R1(config-if)#exit
R1(config)#interface fa0/0
R1(config-if)#ipv6 rip AS1 enable

R1(config-if)#exit

Paso 3: Configure RIP en R2

Se recomienda para este paso, tener en una terminal para R10 y otra para R12. Recuerde, que es necesario realizar los pasos de esa tarea en orden.

Ejecute el comando que habilita el enrutamiento para IPv6 y a continuación habilite la depuración para RIPng. Una vez realizado esos comandos ejecute los siguientes:

R2(config)#ipv6 router rip AS2
*R1(**config-rtr**)#exit*
R2(config)#int serial 0/0/1
R2(config-if)#ipv6 rip AS2 enable
R2(config)#int serial 0/0/0
R2(config-if)#ipv6 rip AS2 enable

Espere unos segundos y observe los mensajes de depuración en R1 y R2

Paso 4: Configure RIP en R3

Recuerde que para realizar este paso es necesario primero completar en orden los pasos anteriores.

Configure la depuración de RIP en R3 y verifique que desde R2 se estén enviando mensajes de RIP por la interfaz serial.

R3(config)#ipv6 router rip AS3

R3(config)#int serial 0/0/1

R3(config-if)#ipv6 rip AS3 enable

R3(config)#int fa0/0

R3(config-if)#ipv6 rip AS3 enable

Estos son los pasos para configurar RIPng en un router, para comprobar la configuración se puede utilizar el comando:

R1#show ip route

Fuente: elaboración propia.

Apéndice B: Ejemplo de Configuración de las VLAN en los switch

Paso 1: Utilizar las siguientes direcciones para el ejemplo.
Dirección de red: 2800:68:16:1300::/64
Gateway: 2800:68:16:1300::1/64
Rango IPv6: 2800:68:16:1300::1/64 – 2800:68:16:1300:ffff:ffff:ffff:ffff

Paso 2: proceder a crear una VLAN este es un proceso repetitivo, solo es de ingresar al modo de configuración global e ingresar el comando: switch(config)#VLAN 20 y listo ha creado la VLAN 20.

Paso 3: Con este direccionamiento, se procede a la configuración de los equipos intermedios y finales.

Paso 4: En modo de configuración Global ingrese los comando que aparecen en la figura:

Figura B.1

```
#interface vlan19
#ipv6 address 2800:68:16:1300::1/64
#ipv6 enable
#ipv6 nd prefix 2800:68:16:1300::/64
```

Con el comando IPv6 nd prefix, los usuarios finales obtendrán direcciones IPv6 dinámicamente.

Fuente: elaboración propia.