UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

METODOLOGÍA DE TRANSICIÓN DEL PROTOCOLO DE INTERNET VERSIÓN 6 PARA LA UNIVERSIDAD TÉCNICA DEL NORTE

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO EN INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

AUTORA: SAYRA BELÉN ESPINOSA ESPINOSA

DIRECTOR DE TRABAJO DE GRADO: ING. EDGAR MAYA

IBARRA - ECUADOR

JULIO 2013

CERTIFICACIÓN

Certifico, que el presente trabajo de grado “METODOLOGÍA DE TRANSICIÓN DEL PROTOCOLO DE INTERNET VERSIÓN 6 PARA LA UNIVERSIDAD TÉCNICA DEL NORTE” fue desarrollado en su totalidad por la egresada de la Carrera de Ingeniería en Electrónica y Redes de Comunicación Srta. Sayra Belén Espinosa Espinosa, bajo mi supervisión.

Ing. Edgar Maya
DIRECTOR DE PROYECTO

UNIVERSIDAD TÉCNICA DEL NORTE

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, SAYRA BELÉN ESPINOSA ESPINOSA, con cédula de identidad Nro. 100297469-7, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autora de la obra o trabajo de grado denominado: **"METODOLOGÍA DE TRANSICIÓN DEL PROTOCOLO DE INTERNET VERSIÓN 6 PARA LA UNIVERSIDAD TÉCNICA DEL NORTE"**, que ha sido desarrollado para optar por el título de Ingeniera en Electrónica y Redes de Comunicación, en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En mi condición de autora me reservo los derechos morales de la obra antes citada. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Técnica del Norte.

Ibarra, a los 12 días del mes de julio de 2013

Nombre: Sayra Belén Espinosa Espinosa
Cédula: 10029749-7

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital Institucional determina la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información.

DATOS DEL CONTACTO	
Cédula de Identidad	1002974697
Apellidos y Nombres	Espinosa Espinosa Sayra Belén
Dirección	Sánchez y Cifuentes 22-38 y Tobías Mena
Email	s_belen19@yahoo.es
Teléfono Fijo	
Teléfono Móvil	0988094159
DATOS DE LA OBRA	
Título	METODOLOGÍA DE TRANSICIÓN DEL PROTOCOLO DE INTERNET VERSIÓN 6 PARA LA UNIVERSIDAD TÉCNICA DEL NORTE
Autora	Espinosa Espinosa Sayra Belén
Fecha	12 Julio 2013
Programa	Pregrado
Título por el que se aspira	Ingeniera en Electrónica y Redes de Comunicación
Director	Ing. Edgar Maya

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, SAYRA BELÉN ESPINOSA ESPINOSA, con cédula de identidad Nro. 1002974697, en calidad de autora y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 144.

_____

Firma

Nombre: Sayra Belén Espinosa Espinosa

Cédula: 1002974697

Ibarra a los 12 días del mes de julio de 2013

3. CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló sin violar derechos de autor de terceros, por lo tanto la obra es original y que es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Firma

Nombre: Sayra Belén Espinosa Espinosa

Cédula: 1002974697

Ibarra a los 12 días del mes de julio de 2013

DECLARACIÓN

Yo, Sayra Belén Espinosa Espinosa, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que éste no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las Leyes de Propiedad Intelectual, Reglamentos y Normatividad vigente de la Universidad Técnica del Norte.

Sayra B. Espinosa E.

DEDICATORIA

Dedico este proyecto a mis padres Luis Eduardo y Nilda Beatriz, que fueron mi apoyo, mi sustento diario para seguir adelante, ahora que ya no pueden compartir conmigo este gran logro sé que están orgullosos de mí porque he alcanzado mi meta, no me queda más que agradecerles por los valores y principios impartidos desde pequeña.

Sayra B. Espinosa E.

AGRADECIMIENTOS

Agradezco al Departamento de Informática de la Universidad Técnica del Norte por permitirme realizar este proyecto y a todo su personal quienes me guiaron de la mejor manera.

Agradezco a mi tutor Ing. Edgar Maya por su desinteresada colaboración, por su gentileza de guiarme a todo momento cuando mas he necesitado y sobre todo a mis padres y hermanos que cada apoyo fue un sustento para seguir adelante y ver el resultado en este proyecto.

Sayra B. Espinosa E.

CONTENIDO

Índice de Figuras

Índice de Tablas

Resumen

El trabajo presentado a continuación consiste en el estudio del protocolo de Internet versión 6 (IPv6) para la Universidad Técnica del Norte, dentro de los avances tecnológicos que tiene la institución es trabajar en su red de datos con IPv6 brindando beneficios para futuras aplicaciones.

Para llegar a esta meta en la UTN, el proyecto inicia en conocer a la organización que tiene asignado IPv6 para el Ecuador (Red CLARA), seguidamente la organización en nuestro país que impulsa a que las instituciones trabajen en sus redes de datos con IPv6 (CEDIA), de esta manera se establece el proveedor de servicios de Internet que trabaja con el protocolo de Internet versión 6 en la Universidad (TELCONET).

IPv6 es la nueva versión del protocolo de Internet versión 4 que actualmente utilizamos, se crea esta nueva versión por decrecimiento masivo de direcciones IPv4 disponibles ya que IPv4 para su direccionamiento posee 32 bits mientras que IPv6 posee 128 bits llevando una considerable diferencia. En el desarrollo del proyecto se realiza un estudio de ambos protocolos de Internet.

Al ser la versión que sigue a IPv4 se basa en principios similares dando lugar a que se hable de una transición, es decir un mecanismo que permita que los dos protocolos funcionen correctamente. Existen tres formas para que ambos protocolos puedan trabajar conjuntamente, el desarrollo consiste en analizar cada forma y determinar que mecanismo de transición es el adecuado para la Universidad Técnica del Norte.

Para activar IPv6 en la red de datos de la UTN se verifica que los equipos de red soporten la nueva versión del protocolo de Internet, para lo cual consiste

dentro del desarrollo verificar los equipos de red si pueden o no trabajar con IPv6.

Finalmente con todos los datos anteriores se inicia con la configuración de IPv6 en equipos de red del entorno externo que posee la institución (router, switch) como fase inicial, además de una aplicación en la configuración de servidor web.

Abstract

The work presented here consist of the study of Internet Protocol version 6 (IPv6) for the Universidad Técnica del Norte, within the technological advances that the institutions its work on your data network to provide benefits to the future IPv6 applications.

To reach this goal in the UTN, the project start in know the organization that has assigned IPv6 for Ecuador (Red CLARA), then the organization in our country that encourages institutions to work on their networks with IPv6 (CEDIA), like this establish the Internet service provided that works with the Internet Protocol version 6 at the University (TELCONET).

IPv6 is the new version of the Internet Protocol version 4 that we actually use, this new version is created by massive die of available IPv4 address as IPv4 for routing has 32 bits while IPv6 has 128 bits carrying a considerable difference. In the development of the project we make a study of both Internet protocols.

As the following IPv4 is based principles that are leading to talk of transition, as a result of mechanism which allows the two protocols function properly. There are three ways for the both protocols can work together, the develop consist in analyze every shape and determine which transition mechanism is right for the Universidad Técnica del Norte.

To enable IPv6 on the network data verifies that the UTN network equipment can support the new version of the Internet Protocol, for which is within the development verify network new version may or may not work with IPv6.

Finally with all previous data starts with the configuration of IPv6 network computer external environment held by the institution (router, switch) as an initial phase, in addition to the web server configuration application.

Presentación

El mundo modernizado que actualmente vivimos, incorpora sofisticados servicios y aplicaciones tecnológicas que poco a poco forman parte de nuestra rutina y tienen como finalidad la satisfacción del usuario en entornos educativos, científicos, culturales y sociales. La mayor parte de este proceso se ejecuta sobre la gran red de redes Internet.

Para que un usuario acceda a un servicio en la red requiere de una dirección IP (Protocolo de Internet), la versión de dirección IP que se ha utilizado desde la creación del protocolo de red hasta el momento es versión 4; han pasado alrededor de 30 años desde su creación y las direcciones IPv4 libres están decreciendo de manera alarmante en algunas regiones del mundo, para cubrir esta necesidad nace la creación de un nuevo protocolo de Internet versión 6 (IPv6) que proporciona un número inimaginable de direcciones escritas en formato hexadecimal.

Para habilitar IPv6 en la red de datos es necesario seleccionar un mecanismo de transición en el cual se trabaja con las dos versiones de protocolo de Internet, es el proceso inicial para trabajar con direcciones IPv6, todo este proceso es transparente para el usuario final.

En la Universidad Técnica del Norte se analizó cada mecanismo de transición y se realizó la selección en base a las ventajas y desventajas de los mismos y en base a los recursos que dispone la institución como es infraestructura tecnológica y a organizaciones de desarrollo tecnológico que pertenece la misma, para desarrollar aplicaciones educativas y situarse a la vanguardia de las universidades en el Ecuador.

CAPÍTULO 1

CEDIA (CONSORCIO ECUATORIANO PARA EL DESARROLLO DE INTERNET AVANZADO)

En el presente capítulo se expresa la estructura del Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado CEDIA de manera jerárquica, indicando los países que forman parte de la Red CLARA en el continente Americano hasta las Universidades e Instituciones miembros de CEDIA en Ecuador, se explica las ventajas de ser miembro, la conformación de los principales nodos y capacidades para miembros CEDIA. Además se explica la integración de IPv6 (Protocolo de Internet versión 6) a CEDIA como parte del progreso del país.

1.1. INTRODUCCIÓN

En la actualidad los mercados globalizados en busca del éxito llevan a la exploración de nuevas herramientas de investigación, desarrollo e innovación para de esta manera alcanzar los objetivos rápida y efectivamente.

Anteriormente se estimaba que en el país no podía poseer una red con alta capacidad especialmente en al ámbito académico, actualmente gracias a los avances tecnológicos a nivel mundial han impulsado a la obtención de varias metas.

Dentro del progreso de nuestro país en la evolución tecnológica, científica e investigativa, crece en su formación del Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado CEDIA.

1.2. CEDIA

Es el Consorcio de Universidades creado para promover y coordinar el desarrollo de redes de avance de la investigación, se centra en el desarrollo científico, académico y de tecnología del Ecuador. “Logrando que académicos e investigadores, participen en proyectos y equipos nacionales e internacionales usando una red exclusiva y especial de alta velocidad que interconecta a 1Gbps, servicios que no son posibles con la red comercial, siendo CEDIA una de las mejores infraestructuras de Latinoamérica” (www.cedia.ec.org, Sept. 2011).

Sus miembros son: Universidades, Escuelas Politécnicas, Centros de Investigación, Organismos públicos y privados del más alto nivel. Todos trabajando conjuntamente dedicados a fomentar interconexión e interoperabilidad para el desarrollo de proyectos con colaboración de la Unión Europea en distintas áreas como: ciencia, tecnologías, salud, telecomunicaciones.

Misión

“Promover, coordinar y desarrollar redes avanzadas de informática y telecomunicaciones, a fin de impulsar en forma innovadora la investigación científica, tecnológica y educativa, logrando que nuestros académicos e

investigadores participen en proyectos y equipos nacionales e internacionales" (www.cedia.ec.org, Sept. 2011).

Visión

"En el próximo quinquenio, ser el referente nacional del desarrollo y utilización de servicios de las redes avanzadas para el fomento de la investigación científica y la educación del País" (www.cedia.ec.org, Sept. 2011).

1.3. ESTRUCTURA EXTERNA DE CEDIA

CEDIA forma parte de CLARA (Cooperación Latinoamericana de Redes Avanzadas). CLARA, está constituida por redes de Latinoamérica e interconecta a éstas con redes de gran relevancia como Internet2 (Red Académica Avanzada) y Géant2 (Red Avanzada Europea). Red CLARA tiene como metas futuras integrar a más países de la región y mejorar continuamente las infraestructuras para fortalecimiento a nivel mundial.

1.3.1. CLARA

Red CLARA, **C**ooperación **L**atino **A**mericana de **R**edes **A**vanzadas, es una Organización de Derecho Internacional sin fines de lucro, cuya existencia legal data del 23 de diciembre de 2004. Red CLARA es integrada por 15 países latinoamericanos y su Asamblea donde cada nación cuenta con un representante sesiona cada seis meses, para definir las líneas de acción y las políticas a ser implementadas.

La iniciativa CLARA tiene dos vertientes: la formación de una infraestructura que integre a las redes avanzadas latinoamericanas y la

creación de una organización no gubernamental que represente los intereses de esta red de organizaciones.

"Su creación es posible gracias al Proyecto ALICE (América Latina Interconectada con Europa), Red CLARA estableció la interconexión de América Latina con la red de investigación paneuropea Géant2" (www.redclara.net, Feb 2011). En el intento de potenciar Red CLARA, se busca el establecimiento de nuevas interconexiones entre Latinoamérica y las redes avanzadas del resto del mundo; a través de los enlaces de esta sección, se presentan iniciativas de interconexión ya consolidadas.

Mediante la red establecida, CLARA, conecta a las redes de educación e investigación nacionales de Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, México, Panamá, Perú, Uruguay y Venezuela. En la Tabla 1 se encuentran los países miembros con su respectiva organización, los cuales están conectados a la RNIE (Red Nacional de Investigación y Educación) de su país de origen y solo se puede acceder a Red CLARA mediante la conexión de esta red. La Figura 1 muestra la interconexión de los países que forman parte de la Red CLARA.

Tabla 1

Miembros de Red CLARA

PAÍS	ORGANIZACIÓN	LOGOTIPO
Bolivia	ADSIB – Agencia para el Desarrollo de la Sociedad de la Información en Bolivia	
Argentina	INNOVA|RED – Red Nacional de Investigación y Educación en Argentina	

PAÍS	ORGANIZACIÓN	LOGOTIPO
Brasil	RNP – Red Nacional de Enseñanza e Investigación.	
Chile	REUNA – Red Universitaria Nacional	
Colombia	RENATA – Red Nacional Académica de Tecnología Avanzada	
Costa Rica	Red CONARE – Consejo Nacional de Rectores	
Ecuador	CEDIA – Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado	
Perú	RAAP – Red Académica Peruana	
Uruguay	RAU – Red Académica Uruguaya	
Guatemala	RAGIE – Red Avanzada Guatemalteca para la Investigación y Educación	
El Salvador	RAICES – Red Avanzada de Investigación, Ciencia y Educación Salvadoreña	

PAÍS	ORGANIZACIÓN	LOGOTIPO
México	CUDI – Corporación Universitaria para el Desarrollo de Internet	
Panamá	RedCyT – Red Científica y Tecnológica	
Paraguay	ARANDU – Proyecto impulsado por el Centro Nacional de Computación de la Universidad de Asunción	
Venezuela	REACCIUN – Red Académica de Centros de Investigación y Universidades Nacionales	

Fuente: http://www.redclara.net/index.php?option=com_content&view=article&id=33&Itemid=403&lang=es

"Red CLARA es responsable de la implementación y manejo de la infraestructura de red que interconecta a RNIE (Redes Nacionales de Educación e Investigación de América Latina)" (www.redclara.net, Feb 2011) Figura 1.

Con un gran número de universidades y centros de investigación conectados a Red CLARA, existían proyectos que carecían de una infraestructura adecuada para sustentar proyectos y comunidades de investigación o educación, actualmente están en posición de avanzar y lo están haciendo.

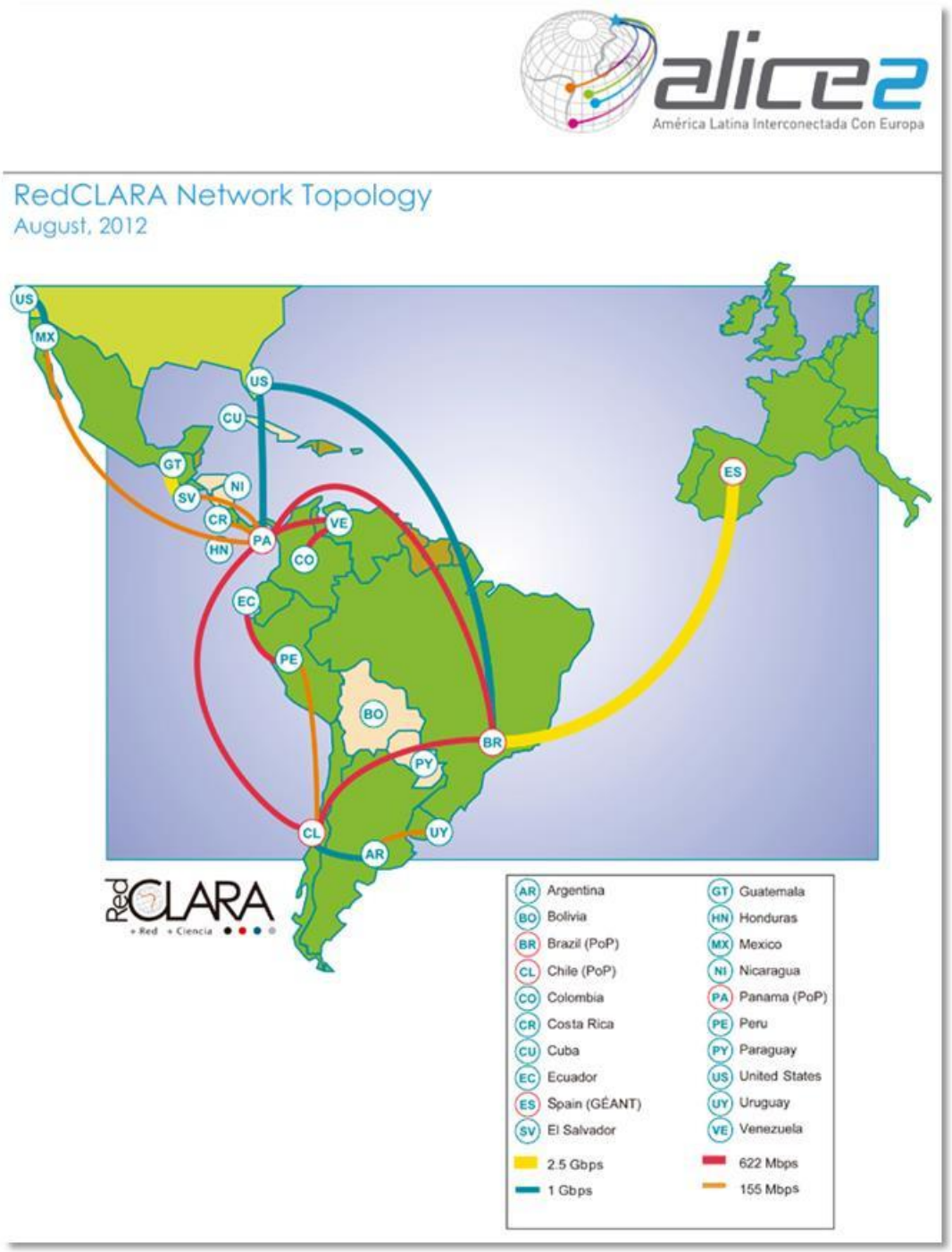


Figura 1. Red CLARA.

Fuente: http://www.redclara.net/index.php?option=com_content&view=article&id=51&Itemid=422&lang=es

"La troncal (backbone) de Red CLARA que tiene un enlace mínimo de 622 Mbps, está compuesta por diez nodos ruteadores, conectados en una

topología punto-a-punto. Cada nodo principal representa a un PoP[1] para Red CLARA, nueve de ellos están ubicados en un país de América Latina -São Paulo (SAO - Brasil), Buenos Aires (BUE - Argentina), Santiago (SCL - Chile), Lima (LIM - Perú), Guayaquil (GYE - Ecuador), Bogotá (BOG - Colombia), Panamá (PTY - Panamá), San Salvador (El Salvador) y Tijuana (TIJ - México)- y el décimo, en Miami (MIA - Estados Unidos) como muestra en la Figura 2" (www.redclara.net, Feb 2012).

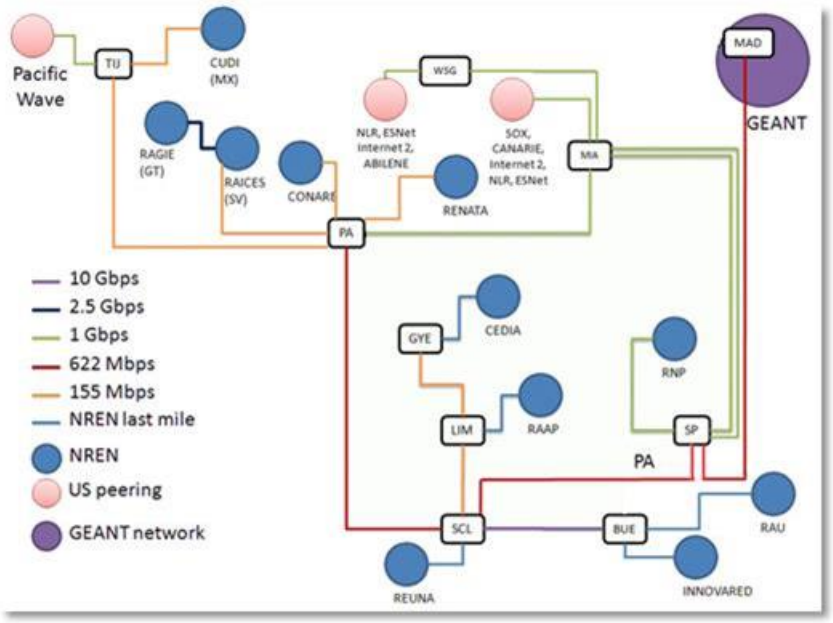


Figura 2. Troncal de Red CLARA y actuales RNIE latinoamericanas conectadas Julio de 2011.

Fuente: http://www.redclara.net/index.php?option=com_content&view=article&id=52&Itemid=423&lang=es

1.3.2. MIEMBROS CEDIA

En el sitio web de CEDIA establece la conformación de miembros compuesta de diversos tipos clasificados de la siguiente manera:

- Miembros académicos de investigación y desarrollo científico son todas las universidades y escuelas politécnicas, centros de investigación y

[1] PoP: Punto de Presencia

desarrollo científico que suscriban el acta de constitución de CEDIA y que cumplan con los requisitos establecidos en el estatuto.

- Miembros estratégicos son los entes establecidos conforme a las leyes del Ecuador que están comprometidos con el desarrollo evolución y utilización de aplicaciones educativas y de tecnología avanzada, redes de telecomunicaciones e informática y que cumplan con los requisitos adicionales establecidos en el estatuto.

- Miembros adherentes las universidades, escuelas politécnicas e institutos de investigación del país que no cuentan con un nodo de computación de alta capacidad de transmisión digital de datos, están comprometidas con el desarrollo, evolución y utilización de aplicaciones educativas y de tecnología avanzada, redes de telecomunicaciones e informática y que cumplan con los requisitos adicionales establecidos en el estatuto.

- Miembros honorarios son las personas naturales o jurídicas que han prestado servicios relevantes al CEDIA y serán designados como tales por el directorio con los votos de por lo menos las tres cuartas partes de sus miembros académicos.

Las instituciones comprometidas con esta iniciativa y que forman parte de CEDIA se encuentran en la Tabla 2 y de manera gráfica como indica en la Figura 3:

Tabla 2

Miembros de Red CEDIA

MIEMBROS	INSTITUCIÓN
Miembros Académicos	Escuela Politécnica del Ejercito – ESPE
	Escuela Politécnica Nacional – EPN
	Escuela Superior Politécnica del Chimborazo – ESPOCH
	Escuela Superior Politécnica del Litoral – ESPOL
	Instituto Oceanográfico de la Armada – INOCAR
	Secretaría Nacional de Educación
	Pontificia Universidad Católica del Ecuador Sede Ibarra – PUCESI
	Pontificia Universidad Católica del Ecuador Sede Quito – PUCE
	Pontificia Universidad Católica Sede Santo Domingo – PUCESD
	Superior, Ciencia, Tecnología e Innovación – SENESCYT
	Universidad Católica de Santiago de Guayaquil – UCSG
	Universidad Central del Ecuador – UCE
	Universidad de Cuenca – UC
	Universidad Estatal de Bolívar – UEB
	Universidad Estatal de Milagro UNEMI
	Universidad Internacional del Ecuador – UIDE
	Universidad Técnica de Ambato. UTA
	Universidad Nacional de Chimborazo
	Universidad Nacional de Loja – UNL
	Universidad Politécnica Salesiana – UPS
Miembros Académicos	Universidad Regional Autónoma de los Andes – UNIANDES
	Universidad San Francisco de Quito – USFQ
	Universidad Técnica del Norte – UTN
	Universidad Técnica Particular de Loja

	– UTPL
	Universidad Tecnológica América – UNITA
	Universidad Tecnológica Equinoccial – UTE
	Universidad Tecnológica INDOAMERICA – UTI
Miembros Honorarios	Steve Hurter, Universidad de Oregón
Miembros Estratégicos	Compañía Nacional de Transmisión Eléctrica – TRANSELECTRIC Ecuador
	Consejo Nacional de Telecomunicaciones – CONATEL Ecuador

Fuente: http://www.cedia.org.ec/index.php?option=com_content&view=article&id=14&Itemid=21

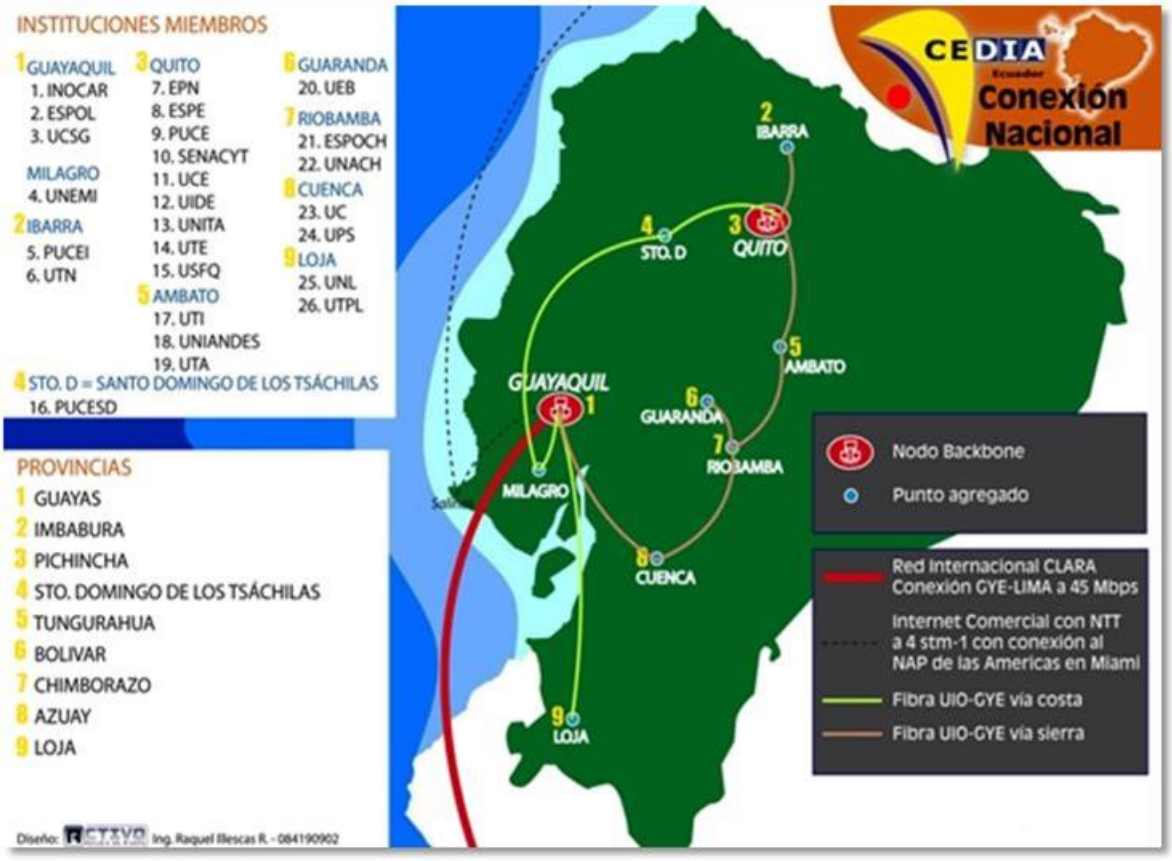


Figura 3. Miembros CEDIA.

Fuente: http://www.cedia.org.ec/index.php?option=com_content&view=article&id=10&Itemid=17

Las ventajas de pertenecer a CEDIA se consideran las siguientes:

- Acceso a bibliotecas digitales.- Las bibliotecas digitales no sólo se establecen como base de datos sino como herramientas que facilitan el acceso al conocimiento desde todas las partes del mundo al mayor número de instituciones posibles.

- Video streaming.- El servicio de video streaming permite la transmisión de contenido multimedia (audio y video) a través de Internet sin necesidad de descargarlo en la computadora del usuario y se reproduce en vivo en la computadora el audio y video de un evento a medida que éste se desarrolla en el sitio de origen.

- Telemedicina / Tele-educación.- El término Telemedicina / Tele-educación se refiere al uso de tecnologías avanzadas de telecomunicaciones, para intercambiar información médica y educativa para proveer servicios tanto de salud como de educación continua a distancia a través de barreras geográficas socioculturales y de tiempo.

- Ambientes de aprendizaje basados en interactividad y simulación.- Son entornos en los cuales los estudiantes pueden resolver problemas apoyados por el ordenador. Las simulaciones interactivas contribuyen al proceso de enseñanza/aprendizaje de diferentes maneras.

- Aprendizaje y educación a distancia, videoconferencias. La videoconferencia es una técnica de comunicación que posibilita a dos o

más grupos distantes, a interactuar en tiempo real, utilizando equipos de audio y vídeo en el lugar donde se encuentren.

- Laboratorios de realidad virtual.- Laboratorios dotados de herramientas para realizar varias actividades de realidad virtual, tanto visual como táctil.

Los miembros de CEDIA logran:

- Ser parte activa del desarrollo de esta iniciativa en ECUADOR.
- Participar activamente en el desarrollo de tecnologías de la nueva generación de Internet.
- Formar parte de los equipos técnicos y científicos involucrados en el desarrollo de aplicaciones de la nueva generación de Internet.
- Integrar el grupo de Universidades y otras Instituciones de investigación y desarrollo que participan en este proyecto a nivel mundial.

1.4. ESTRUCTURA INTERNA DE CEDIA

"La infraestructura de la Red CEDIA se compone de dos nodos situados en las principales ciudades del Ecuador, específicamente en Quito y Guayaquil razón por la cual en las mismas y muy cercanas se encuentran un gran número de universidades y centros de investigación cubriendo de esta manera al país en su totalidad" (Machado L, 2008).

CEDIA con el fin de promover la interconexión entre sus miembros, ha contratado un proveedor de servicios de Internet para todos ellos, con el objetivo de participar activamente en la coordinación de proyectos de investigación, incentivar el desarrollo de nuevas aplicaciones y de igual manera ahorrar costos, se destine a "TELCONET proveedor de servicios de Internet para CEDIA" (Boletines CEDIA, Feb 2009), "el cual opera sobre la Red Nacional NGN[2] que posee TELCONET con capacidad para manejo de IPv6 en el país llegando a un ancho de banda de 5 STM-1" (www.telconet.net, Sept 2011), permitiendo de esta manera aceptar a más universidades e instituciones que pretenden formar parte del Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado.

"La conectividad con la Red Avanzada Latinoamericana Red CLARA será de 45 Mbps, con el fin de prevenir la utilización de aplicaciones y proyectos de I+D+i (Investigación, Desarrollo e Innovación) promovidos de CEDIA que requieran las capacidades diagnosticadas" (Boletines CEDIA, May 2009). "La conectividad hacia Red CLARA se realiza por medio de un enlace internacional con la empresa TRANSELECTRIC desde Guayaquil hacia Lima" (Machado L, 2008), como se observa en la Figura 4. En relación a la salida internacional comercial IPv6 se enlaza a proveedor internacional NTT[3].

Hasta el momento ya se cuenta con la gran mayoría de instituciones que forman parte de CEDIA (Figura 5) "con una capacidad de ancho de banda de 1Gbps enlazadas a la Red Avanzada" (Boletines CEDIA, Dic 2009, Apéndice

[2]NGN: Next Generation Network
[3] NTT :NipponTelegraph and Telephone Communications

A), logrando a convertiste en una de las NREN[4] con mejor conectividad interna en su anillo de fibra óptica a nivel de Sudamérica comparándose así con Redes Avanzadas en Europa. Por este motivo se realizan trabajos intensos para mejorar la interconexión con el anillo internacional a la Red CLARA.

[4] NREN: Red Nacional de Investigación y Educación

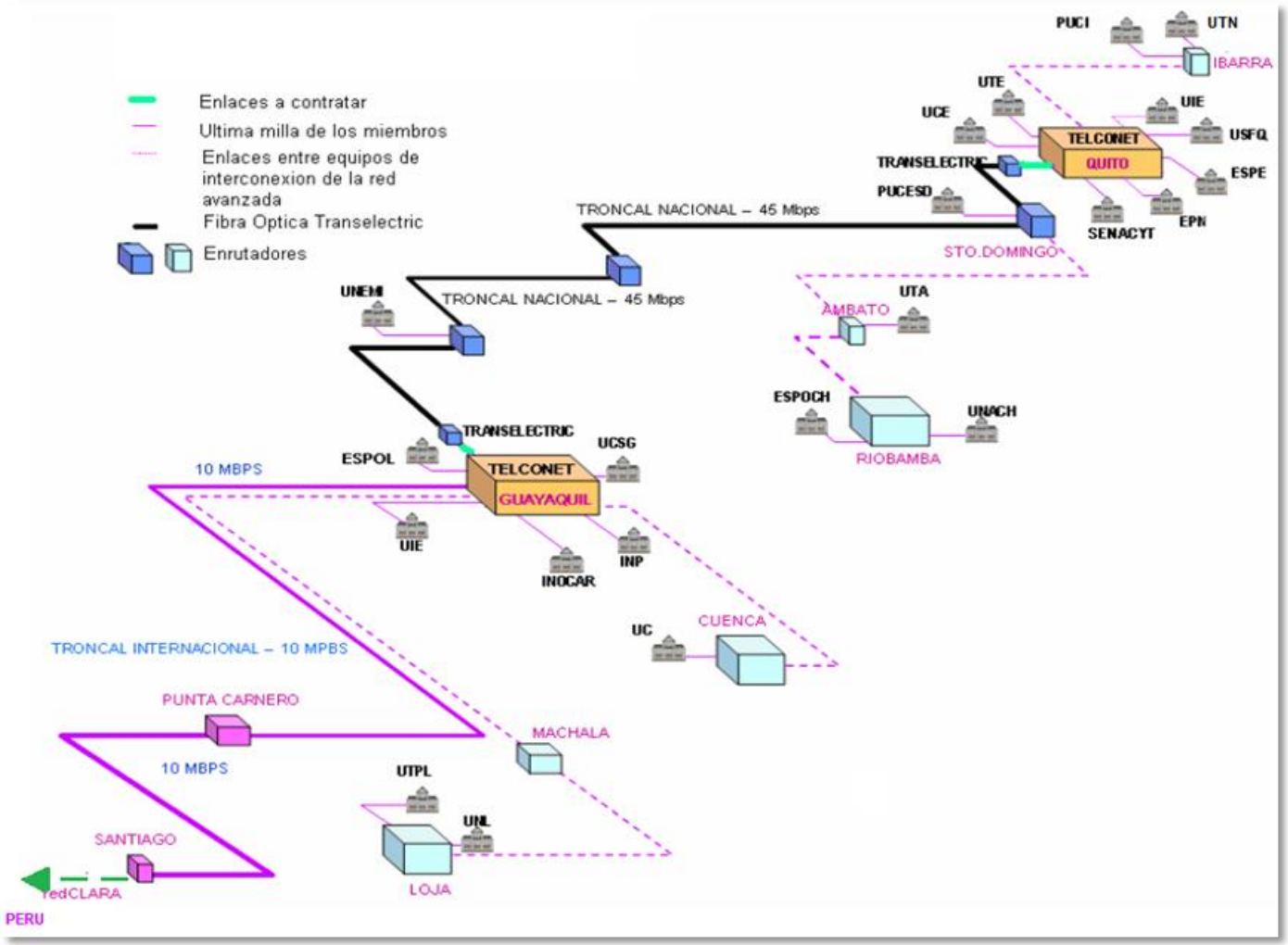


Figura 4. CEDIA conexión a TRANSELECTRIC.
Fuente: bibdigital.epn.edu.ec/bitstream/15000/530/1/CD-1028.pdf

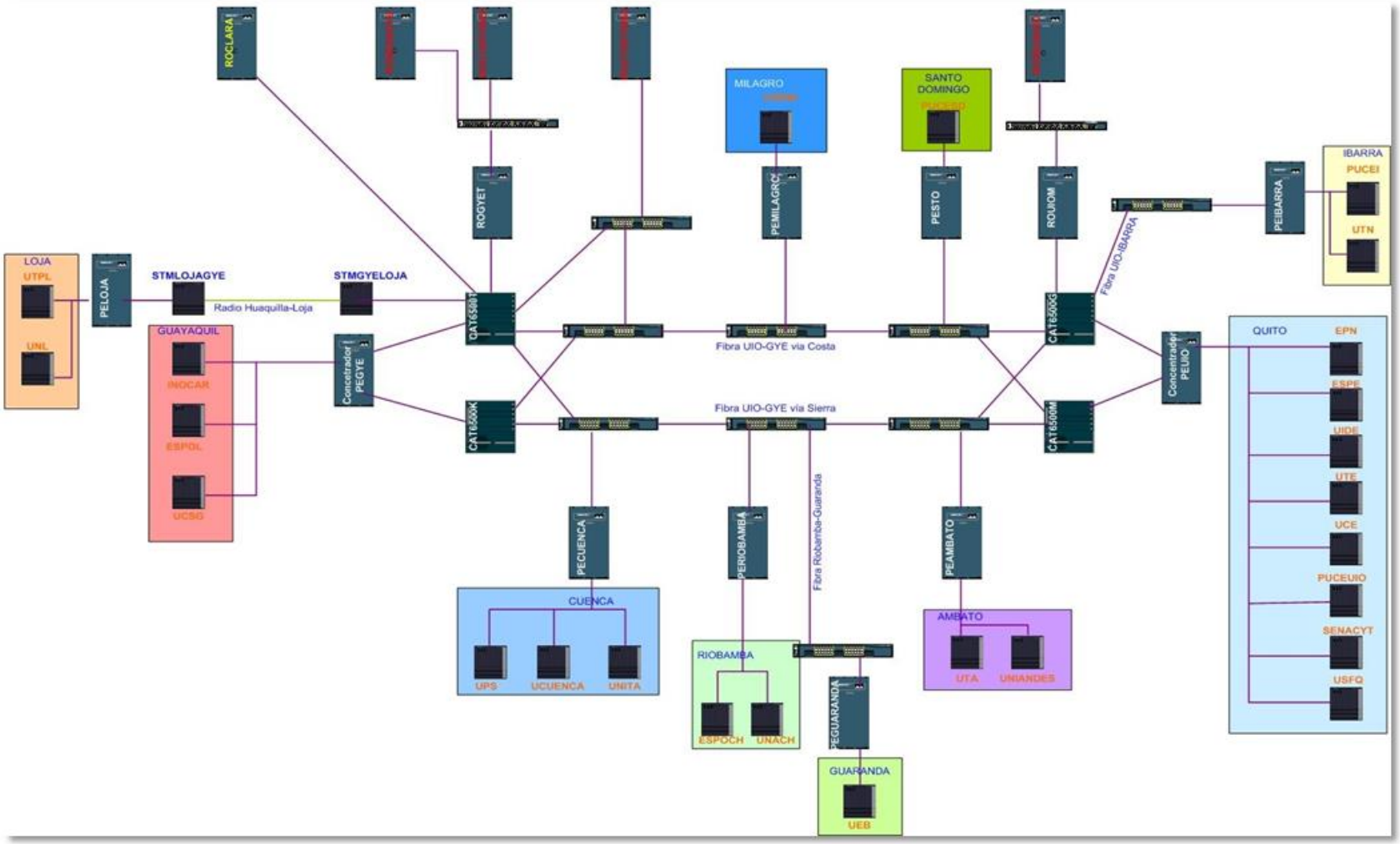


Figura 5. Conexión de CEDIA a nivel nacional.

Fuente: http://www.cedia.org.ec/index.php?option=com_content&view=article&id=9&Itemid=16

1.4.1. CONEXIÓN DE MIEMBROS CEDIA

"CEDIA cuenta con su nodo físico en TELCONET de la ciudad de Guayaquil (PoP Punto de presencia en Ecuador) y para la cuidad de Quito se simula un nodo mediante un enrutador a través de túneles VPN[5]. Estos nodos se encuentran conectados mediante fibra óptica de TELCONET a 20 Mbps" (Boletines CEDIA, Jun 2010).

Para la mayoría de los miembros establecen enlaces de fibra óptica contratada por TELCONET tanto para Internet comercial y para Red Avanzada.

La capacidad para cada miembro CEDIA para Internet Avanzado es de 1Gbps proporcionada por fibra óptica de TELCONET.

LACNIC[6] cuya finalidad es proporcionar direcciones para el acceso a Internet, promueve la activación de IPv6 en base al significativo descenso de direcciones IPv4 disponibles para América Latina y el Caribe, los datos actuales se pueden observar en la pagina oficial de LACNIC: http://www.lacnic.net/es/web/lacnic/reporte-direcciones-ipv4.

LACNIC asignó un rango de direcciones IPv6 a CEDIA, comprende la dirección 2800:68::/32 (dirección IPv6 se explica en capítulo dos), esta asignación de dirección IPv6 comprende el primer campo hexadecimal basado en la asignación por bloque de LACNIC, el segundo campo hexadecimal corresponde a CEDIA y el tercer campo hexadecimal corresponde a la Universidad Técnica del Norte. El rango de CEDIA se encuentra dividida en

[5] VPN: Redes Privadas Virtuales
[6] LACNIC: Registro de Direcciones de Internet para América Latina y Caribe

redes /48 para ser asignarlas a diferentes instituciones como se muestra en la Tabla 3 de la cual la mayoría de instituciones se encuentran investigando todo lo relacionado al nuevo protocolo.

"Existen dos universidades que forman parte de CEDIA que han adquirido directamente de LACNIC un rango de direcciones IPv6, estas son: Universidad Técnica Particular de Loja con asignación 2800:130::/32 y para la Escuela Politécnica del Litoral tiene asignado el rango 2801:0:20::/48" (www.cedia.org.ec, Mar 2010).

Tabla 3

Asignación IPv6 en CEDIA

INSTITUCIÓN	ASIGNACIÓN DE RED IPv6
Reservado para CEDIA	2800:68:0001::/48
INOCAR	2800:68:0002::/48
Universidad Estatal de Milagro	2800:68:0003::/48
Universidad Tecnológica Indoamérica	2800:68:0004::/48
Escuela Superior Politécnica del Litoral	2800:68:0005::/48
Universidad Católica de Guayaquil	2800:68:0006::/48
Universidad Nacional de Loja	2800:68:0007::/48
Universidad Técnica Particular de Loja	2800:68:0008::/48
UTA	2800:68:0009::/48
Escuela Politécnica del Chimborazo	2800:68:000A::/48
Universidad Nacional del Chimborazo	2800:68:000B::/48
Universidad de Cuenca	2800:68:000C::/48
PUCE Ibarra	2800:68:000D::/48
PUCE Santo Domingo	2800:68:000E::/48
FUNDACYT	2800:68:000F::/48
Universidad Internacional del Ecuador	2800:68:0010::/48
Escuela Politécnica Nacional	2800:68:0011::/48

Escuela Superior Politécnica del Ejército	2800:68:0012::/48
Universidad Central del Ecuador	2800:68:0013::/48
Universidad San Francisco de Quito	2800:68:0014::/48
Universidad Tecnológica Equinoccial	2800:68:0015::/48
Universidad Politécnica Salesiana	2800:68:0016::/48
UNITA	2800:68:0017::/48
Universidad Estatal de Bolívar	2800:68:0018::/48
Universidad Técnica del Norte	2800:68:0019::/48
UNIANDES	2800:68:0020::/48

Fuente: http://www.cedia.org.ec/index.php?option=com_content&view=article&id=14&Itemid=21

1.5. UNIVERSIDAD TÉCNICA DEL NORTE MIEMBRO CEDIA

Dentro del plan de desarrollo informático realizado por el Departamento de Informática de la Universidad Técnica del Norte, se encuentra estimado trabajar en su red de datos con el protocolo de Internet versión 6. El proceso inició con el establecimiento de convenios, proyectos organizados y cursos realizados.

1.5.1. CONVENIOS

Son convenios necesarios para que la Universidad Técnica del Norte se identifique como miembro CEDIA.

- Acta de compromiso de miembro académico, de investigación y de desarrollo científico de la Fundación Consorcio para el Desarrollo del Internet Avanzado (CEDIA). La Universidad Técnica del Norte, de acuerdo a su normativa legal y por la Comisión de Membresía de CEDIA, se procede a designar miembro académico a la UTN por cumplir

con los Estatutos de CEDIA, además que la institución sea beneficiada de proyectos relacionados hacia la nueva tecnología de información e Internet 2 (Apéndice B y C).

La Universidad Técnica del Norte participa en el desarrollo de proyectos para que en su red de datos se encuentre activa el protocolo de Internet versión 6 además de la activación de IPv6 en cada uno de sus servicios que posee.

- Convenio Ampliatoria al Convenio Interinstitucional de Financiamiento al Acceso al Internet suscrito entre Universidad Técnica del Norte y CEDIA. Dentro de la resolución de este convenio se menciona que la institución y CEDIA proceden a brindar el servicio de acceso al Internet a través de un servicio de portador de Telecomunicaciones.

- Convenio Interinstitucional de Financiamiento general y de financiamiento para Conexión Internacional ALICE - CLARA. De acuerdo a los Estatutos de CEDIA, la Universidad Técnica del Norte en calidad de miembro, está obligado a pagar cuotas de membrecía para su funcionamiento y aportar con el pago anual de suscripción de servicio de conexión a la red académica avanzada –CLARA.

- Servicios de Redes Avanzadas Académicas Investigación y Desarrollo por Internet mediante el Portal de Compras Públicas. Para la contratación mediante el Portal de Compras Públicas, se hará la invitación a CEDIA tomando en consideración que CEDIA está registrado bajo el Código 84290.00.2 SERVICIOS DE REDES

AVANZADAS ACADÉMICAS INVESTIGACIÓN Y DESARROLLO POR INTERNET. Al ser considerados como los únicos proveedores autorizados a conectarse a Red Clara y a través de ella a las redes avanzadas de investigación y educación del mundo entero, se debe contratar los servicios mediante el sistema de Régimen Especial, de acuerdo al Capítulo VII Régimen Especial, la Sección VIII del Reglamento General de la ley Orgánica del Sistema Nacional de Contratación Pública.

- Convenio para el proyecto “Expansión del IDE REDCEDIA FASE II”, entre el Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado – CEDIA y la Universidad Técnica Del Norte. El objeto del presente Convenio es el de desarrollar el proyecto “Expansión del IDE REDCEDIA Fase II”, proyecto en el cual se amplía los nodos participantes a nivel regional, generación de mapas y manuales para los futuros instituciones o entidades públicas.

1.5.2. PROYECTOS

Son proyectos impulsados por el Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado para todos sus miembros.

- Proyecto Infraestructura de Datos Espaciales IDE - RED CEDIA (Fase I). La Facultad de Ingeniería en Ciencias Agropecuarias y Ambientales, El Laboratorio de Geomática y el Departamento de Sistemas de la Universidad Técnica del Norte (UTN) se encuentra en el emprendimiento

de la IDE Red CEDIA, proyecto que es financiado actualmente por CEDIA.

- Proyecto Infraestructura de Datos Espaciales IDE - RED CEDIA (Fase II). Ampliación de los Nodos Participantes a Nivel Regional. Generación de Mapas y Manuales para los futuros instituciones o entidades públicas.

- Proyecto Infraestructura de Datos Espaciales para Latinoamérica LATIN - IDE. Incorporación de Países a la Infraestructura de Datos espaciales, comprendidos por: Argentina, Colombia, Chile, Perú y otros. Para el compartimiento de Mapas Geográficos entre Universidades, Instituciones Públicas y Privadas.

- Proyecto de Infraestructura de Datos Espaciales - Desastres Naturales. Conjuntamente con el Proyecto del LATIN - IDE se incorpora un nuevo grupo de expertos para la generación de mapas con ámbitos de Desastres Naturales.

- Implementación en las instituciones que forman parte de CEDIA, las cuales se comprometieron en colocar su diagrama de red y su IP (Protocolo de Internet) de sus respectivos servidores para realizar pruebas. Fomentando así en todos los miembros a centrarse en la preparación hacia el nuevo protocolo de Internet versión 6.

1.5.3. CURSOS

De acuerdo al Boletín de CEDIA del mes de diciembre del 2009, la Universidad Técnica del Norte es miembro participativo de los cursos de IPv6 y

seguridades organizados por parte de CEDIA, como parte del proceso de llegar poseer el nuevo protocolo de Internet versión 6 activo en la red de todos los miembros.

- Servicios de Streaming y Codificación. Curso en el cual se centra en conceptos básicos de transmisión de señales de video y datos sobre redes de datos.

- Curso de IPV6 y Seguridades. La finalidad de esta curso es analizar la distribución, asignación de direcciones tanto IPv4 como IPv6, la necesidad del nuevo protocolo de Internet, ventajas, formato de la cabecera, direccionamiento y movilidad.

CAPÍTULO 2

ANÁLISIS COMPARATIVO IPv4 vs IPv6

En el presente capítulo se centra en la descripción de los protocolos de Internet versión 4 y versión 6, posteriormente se realiza una comparación técnica, diferencias de cabeceras indicando sus respectivos campos, dentro del desarrollo se enfoca a las ventajas que posee el nuevo protocolo de Internet incluyendo su nueva terminología y direccionamiento.

2.1. INTRODUCCIÓN

El masivo crecimiento de uso de Internet ha ocasionado que las direcciones IPv4 libres presenten un significativo descenso, frente al diagnóstico de alerta a nivel mundial da lugar a la creación y puesta en marcha del nuevo protocolo de Internet versión 6.

Por este motivo varias son las organizaciones que promueven dar un paso más hacia la tecnología, razón por la cual cada vez se suman más instituciones especialmente educativas que acogen la iniciativa de habilitar IPv6 en su red.

2.2. RESUMEN DE MODELOS OSI Y TCP/IP

Dentro de la conformación de las redes de computadoras, existen modelos de referencia distribuidos en capas, estos modelos son: OSI[7] y TCP/IP[8].

2.2.1. MODELO OSI

El modelo de referencia OSI fue desarrollado por la ISO[9], es un modelo de referencia que sirve para la explicación del funcionamiento en la red. La funcionalidad de sus capas se muestra en la Tabla 4.

Tabla 4

Funciones de capas en modelo OSI

CAPA	FUNCIÓN
Física	Se responsabiliza de la transmisión de bits a través de un canal de comunicación. Hace referencia a características físicas de interfaces, medio de comunicación y modo de transmisión.
Enlace de datos	Delimita el inicio y fin de tramas, responsabilizándose de su transmisión hacia el nodo siguiente. Esta relacionado con direccionamiento físico, control de errores y control de flujo.
Red	Se encarga de entregar paquetes desde un host origen hasta un host destino, en esta capa se realiza direccionamiento lógico. Contiene el protocolo de capa de red que es el protocolo Internet.
Transporte	Acepta datos de capas superiores con la seguridad de que todo su contenido llegue completamente al otro extremo. Se encuentra relacionado con el control de conexión ya que puede ser orientado a conexión o no.
Sesión	Permite el control de diálogo y de sincronización para que usuarios de maquinas diferentes establezcan sesiones entre ellos.

[7] OSI: Interconexión de Sistemas Abiertos
[8] TCP/IP: Protocolo de Control de Transmisión/Protocolo de Internet
[9] ISO: Organización Internacional de Estándares

Presentación	Se responsabiliza de cifrado, codificación y decodificación del flujo de bits.
Aplicación	Se define como la interfaz con el usuario, contiene varios protocolos utilizados con frecuencia por el usuario, proporcionando varios servicios.

2.2.2. MODELO TCP/IP

El modelo de referencia TCP/IP destinado para comunicaciones de internetwork y generalmente se identifica al modelo de Internet con el modelo TCP/IP. La funcionalidad de sus cuatro capas de muestran en la Tabla 5.

Tabla 5

Funciones de capas en modelo TCP/IP

CAPA	FUNCIÓN
Acceso a la red	Controla los dispositivos del hardware y los medios que forman la red.
Internet	Determina la mejor ruta a través de la red.
Transporte	Admite la comunicación entre distintos dispositivos de distintas redes (extremo a extremo).
Aplicación	Representa datos para el usuario mas el control de codificación y de diálogo.

2.2.3. COMPARACIÓN DE MODELOS OSI Y TCP/IP

El modelo OSI y modelo TCP/IP poseen características comunes, en especial se menciona que los dos modelos están conformados por capas las cuales a su vez su funcionalidad es similar como en la capa de red del modelo OSI y la capa de Internet del modelo TCP/IP donde manejan el envío de paquetes a través de la red, en el modelo TCP/IP se reduce el número de capas agrupando funcionalidades de capas del modelo OSI (Figura 6).

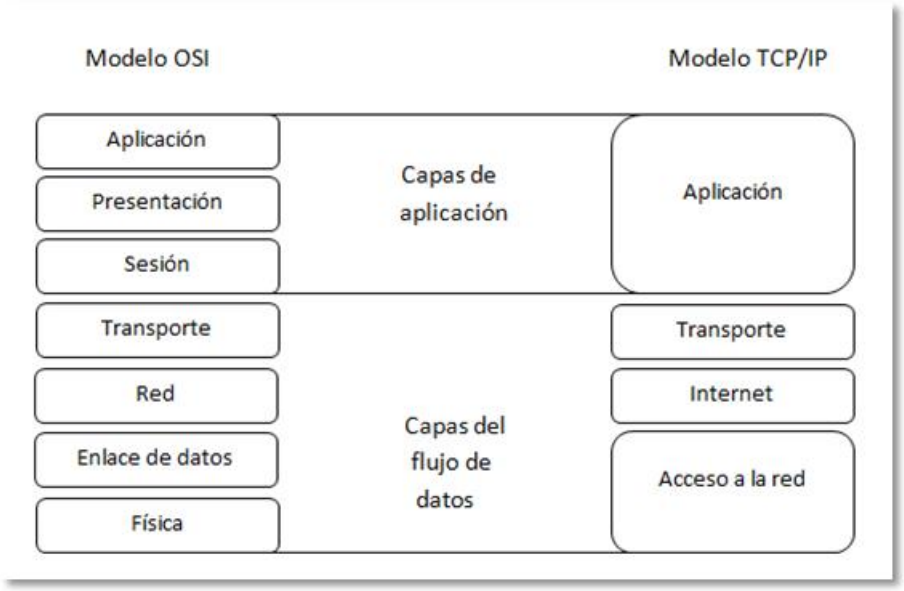


Figura 6. Comparación de modelos OSI y TCP/IP.

Fuente: Adaptado de: Curriculum CISCO Networking Academy Exploration v4.0. Capítulo 3: Protocolos y funcionalidad. Semestre nro. 1

Entre sus diferencias se citan: el número de capas siete en OSI y cuatro en TCP/IP, en OSI se definen protocolos, interfaces, servicios y describe a cualquier tipo de red; en TCP/IP no define protocolos, interfaces, servicios y este modelo puede describir solo a redes que llevan su mismo nombre.

2.3. CONCEPTOS BÁSICOS

Según RFC 791 IP o Protocolo de Internet es el protocolo sobre y bajo el cual funciona la gran red de redes, Internet. El protocolo IP tiene las siguientes características:

- Protocolo orientado a no conexión.
- Fragmenta paquetes si es necesario.
- Direccionamiento mediante direcciones de 32 bits.

- Si un paquete no es recibido, éste permanecerá en la red durante un tiempo finito.

- Realiza el "mejor esfuerzo" para la distribución de paquetes.

- Tamaño máximo del paquete de 65635 bytes.

De las características que posee el Protocolo Internet se destaca lo siguiente: proporciona un servicio de distribución de paquetes de información orientado a no conexión de manera no fiable; la orientación a no conexión quiere decir que los paquetes de información que son emitidos por la red, son tratados independientemente tomando trayectorias diferentes para llegar a su destino. El término no fiable quiere decir que no se garantiza la recepción del paquete hacia su destino.

2.4. PROTOCOLO DE INTERNET VERSIÓN 4

"IPv4 es el protocolo de Internet versión 4 desarrollado por IETF [10], anteriormente las direcciones IP usaban sólo los primeros 8 bits para especificar la porción de red de la dirección pero con la actualización del RFC 791 se establece la dirección de 32 bits IPv4 la cual sirvió para permitir tres clases diferentes de redes proporcionando alrededor de 4.200 millones de direcciones a ser asignadas" (www.ietf.org/rfc791, Nov 2011). El protocolo de Internet versión 4 es utilizado para la comunicación entre redes por medio del envío de paquetes, el modo en que opera es el de mejor esfuerzo de entrega del modelo, ya que no garantiza la entrega, ni garantiza la secuencia correcta o

[10] IETF: Fuerza de Trabajo en Ingeniería de Internet o Internet Engineering Task Force .

la evitación de la entrega duplicada, además para la navegación en Internet ninguna dirección pública de un host debe ser igual a otra a menos que se encuentren en redes diferentes.

2.5. DIRECCIONAMIENTO IPv4

La función principal de IP es entregar mensajes entre dispositivos situados en la red, para que esta función se realice correctamente debe saber en dónde se encuentran los destinatarios en base al direccionamiento y enrutamiento. Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de red NIC[11].

La dirección IPv4 tiene una longitud de 32 bits representadas con 4 octetos, representados en notación decimal separado con un punto por cada octeto variando desde 0 hasta 255 en notación decimal y de 0 hasta 11111111 en notación binaria. Como muestra en la Tabla 6.

Tabla 6

Notaciones de dirección IP

DIRECCIÓN IPv4	NOTACIÓN
220.56.17.144	Notación punto decimal
11011100.00111000.00010001.10010000	Notación binaria

[11] NIC: Network Interface Card

2.5.1. TIPOS DE DIRECCIONES IPv4

Una dirección IP se compone de dos partes: la primera parte indica la red y la segunda parte indica el host (Figura 7). Las clases de direcciones IP se identifican por el número decimal del primer octeto.

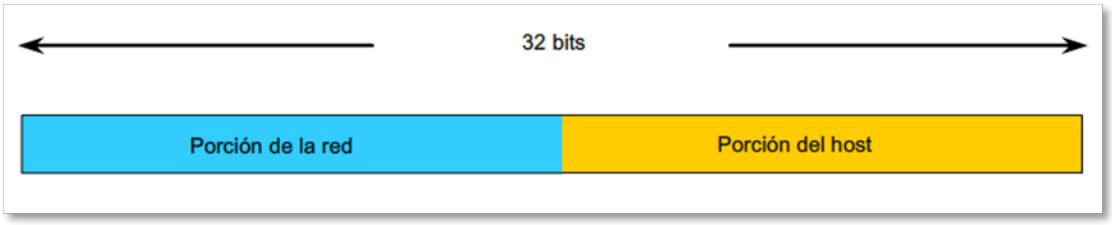


Figura 7. Componentes de la dirección IP.

Fuente: Curriculum CISCO Networking Academy Exploration v4.0. Capítulo 6: Direccionamiento de red IPv4. Semestre nro. 1.

2.5.1.1. Direcciones Clase A

Las direcciones clase A comienzan con un bit 0, cuyo rango de direcciones clase A empiezan desde 0.0.0.0 a 127.255.255.255.

“En el bloque de direcciones clase A, utiliza un prefijo / 8 con el primer octeto para indicar la dirección de red. Los tres octetos restantes se utilizan para las direcciones de hosts” (Curriculum CISCO v4.0). Para reservar espacio de direcciones para las clases de direcciones restantes, todas las direcciones de clase A requiere que el bit más significativo del octeto de orden superior que es un cero.

A este tipo de direcciones están asignadas redes considerablemente grandes, con más de 16 millones de direcciones para host, son pocas las

empresas que tienen esta asignación, ARPAnet [12] es una de ellas, además algunas grandes redes comerciales, aunque son pocas las organizaciones que obtienen una dirección de clase A.

2.5.1.2. Direcciones Clase B

"Las direcciones clase B comienzan con un bit 1 y un bit 0, cuyo rango de las direcciones clase B empieza desde de 128.0.0.0 / 16 a 191.255.255.255 / 16" (Curriculum CISCO v4.0). Los dos últimos octetos de la dirección constituyen el identificador del host permitiendo un número máximo de 64516 ordenadores en la misma red.

2.5.1.3. Direcciones Clase C

Las direcciones clase C comienzan con dos bits 1 y un bit 0 y su rango es el siguiente desde 192.0.0.0 a 223.255.255.255 con un prefijo / 24.

Este espacio de direcciones tenía la intención de proporcionar direcciones para redes pequeñas con un máximo de 254 hosts. Esto significaba que una red de clase C utiliza sólo el último octeto como direcciones de host con los tres octetos de orden superior para indicar la dirección de red.

Clase C bloques de direcciones a un lado del espacio de direcciones de clase D (multicast) y la clase E (experimental) mediante el uso de un valor fijo de 110 para los tres bits más significativos del octeto de orden superior, limitando la dirección del bloque de la clase C de 192.0.0.0 / 16 a 223.255.255.0 / 16.

[12] ARPANET: Advanced Research Projects Agency Network - Red Avanzada de Agencias para Proyectos de Investigación

La Tabla 7 muestra la clasificación de direcciones IP de acuerdo a su rango y en la Tabla 8 muestra el rango de direcciones privadas de cada clase.

Tabla 7

Clasificación de direcciones IP

CLASE	INTERVALO		CAPACIDAD EN HOST
A	1.0.0.1 127.255.255.254	a	Soporta 16 millones de hosts en cada una de 127 redes.
	127.0.0.0		Reservada para loopback (los hosts utilizan esta dirección para dirigir el tráfico hacia ellos mismos)
B	128.1.0.1 191.255.255.254	a	Soporta 65.000 hosts en cada una de 16.000 redes.
C	192.0.1.1 223.255.254.254	a	Soporta 254 hosts en cada una de 2 millones de redes.
D	224.0.0.0 239.255.255.255	a	Reservado para multicast grupos.
E	240.0.0.0 254.255.255.254	a	Reservado para uso futuro, o fines de investigación y desarrollo.

Fuente: Módulo Curriculum CISCO Networking Academy Exploration v4.0. Capítulo 6: Direccionamiento de red IPv4. Semestre nro. 1.

Tabla 8

Rango de direcciones privadas

CLASE	RANGO
A	10.0.0.0 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: Módulo Curriculum CISCO Networking Academy Exploration v4.0. Capítulo 6: Direccionamiento de red IPv4. Semestre nro. 1.

2.6. CABECERA IPv4

La cabecera del protocolo de Internet versión 4 se encuentra definido por campos (Figura 8) y estos a su vez contienen valores binarios, donde los servicios IPv4 toman como referencia a medida que envían los paquetes a través de la red.

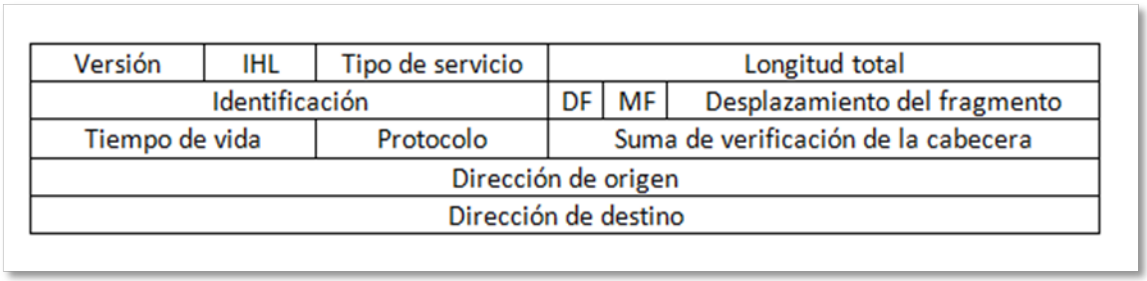


Figura 8. Campos de la cabecera IPv4.

Fuente: Curriculum CISCO Networking Academy Exploration v4.0. Capítulo 6: Direccionamiento de red IPv4. Semestre nro. 1.

- Versión: Contiene la versión del protocolo (versión 4).

- Longitud de la cabecera (IHL): Especifica el tamaño de la cabecera del paquete.

- Tipo de servicio: El campo de tipo de servicio contiene un valor binario de 8 bits que se usa para determinar la prioridad de cada paquete. Este valor permite aplicar un mecanismo de Calidad del Servicio (QoS) a paquetes de alta prioridad, como aquellos que llevan datos de voz en telefonía.

- Longitud total del paquete: Este campo muestra el tamaño completo del paquete, incluyendo la cabecera y los datos, en bytes.

- Identificación: Este campo es principalmente utilizad para identificar únicamente fragmentos de un paquete IP original.

- Señalizador:
    - Señalizador de Más fragmentos (MF): Es un único bit en el campo del señalizador usado con el Desplazamiento de fragmentos para la fragmentación y reconstrucción de paquetes.
    - Señalizador de No Fragmentar (DF): Es un solo bit en el campo del señalizador que indica que no se permite la fragmentación del paquete porque es incapaz de unir las piezas de nuevo.

- Desplazamiento de fragmentos: Cuando se produce una fragmentación, el paquete IPv4 utiliza el campo Desplazamiento de fragmento y el señalizador MF en la cabecera IP para reconstruir el paquete cuando llega al host destino. El campo de desplazamiento del fragmento identifica el orden en el cual ubicar el fragmento del paquete en la reconstrucción.

- Tiempo o período de vida: Cantidad de saltos antes de que se descarte el paquete. Este valor se reduce en cada salto para evitar que los paquetes se transmitan a través de la red en routing loops (paquetes que siguen circulando en la red sin fin).

- Protocolo: Indica el tipo de relleno de carga que el paquete traslada, si el contenido que se traslada en los datos son un datagrama UDP o segmento TCP. El campo de protocolo permite a la capa de red pasar los datos al protocolo apropiado de la capa superior.

- Suma de verificación de la cabecera: Se recalcula cada vez que algún nodo cambia alguno de sus campos (por ejemplo, el Tiempo o período de vida). El método de cálculo consiste en sumar el complemento a 1 de cada palabra de 16 bits de la cabecera y hacer el complemento a 1 del valor resultante.

- Dirección de origen: Es la dirección IPv4 del host que envía el paquete el cual se mantiene inalterable a lo largo de todo el recorrido del paquete a través de internetwork. Habilita al host de destino para responder al de origen si es necesario.

- Dirección de destino: Es la dirección IPv4 del host que recibe el paquete y de igual manera se mantiene inalterable a lo largo de todo el recorrido del paquete a través de internetwork. Habilita a los routers de cada salto para reenviar el paquete hacia el destino.

- Opciones: Cabeceras de campos adicional para suministrar otros servicios, utilizado con escasa frecuencia.

2.6.1. PROTOCOLOS EN IPv4

Para el correcto funcionamiento de IPv4 en la red se basa en protocolos propios que brindan servicios, que se resumen a continuación:

2.6.1.1. ARP (Address Resolution Protocol, Protocolo de Resolución de Direcciones)

Es un protocolo utilizado en la compatibilidad de direcciones públicas y privadas, donde intervienen las direcciones de hardware (dirección física de una tarjeta de interfaz de red) y de software (dirección IP). Al comunicarse un equipo con otro, ARP pregunta a los equipos de red sus direcciones de hardware para la creación de una tabla donde queda registrado dichas direcciones de hardware y software en una memoria cache, para el continuo uso de comunicación con otros equipos.

2.6.1.2. RARP (Reversee Address Resolution Protocol, Protocolo de Resolución Reversa de Direcciones)

Sirve para que los equipos descubran sus direcciones IP por medio de una tabla de búsqueda de direcciones, cuando estos trabajan sin discos duros, ya que al momento de arrancar solo conocen su interfaz de hardware. Posee algunas limitaciones que lo hacen poco utilizado ya que requiere uno o más host de servidor para mantener una tabla con información de asignaciones de direcciones de protocolos.

2.6.1.3. ICMP (Internet Control Message Protocol, Protocolo de Control de Mensajes de Internet)

“Es un protocolo utilizado por IP para la notificación de errores que pueden suceder en la red dando lugar a ser un mecanismo de gestión de red

ya que se encarga de avisar al emisor posibles situaciones de error que ha sufrido un paquete IP impidiendo llegar a su destino" (Robles M, 2008).

2.6.2. LIMITACIONES EN IPv4

Dentro de las motivaciones en la búsqueda de un nuevo protocolo de Internet se tomaron en cuenta las actuales limitaciones que posee IPv4. En materia avanzada de redes de computadores indica las siguientes limitaciones:

- Con la escasa asignación de direcciones libres limita el crecimiento de Internet.

- La manera de organización en clases, existe desperdicio de muchas direcciones.

- Multicast es opcional en IPv4 y no se ha llegado a utilizar de manera eficaz.

- En la actualidad existen más aplicaciones de videoconferencia, multimedia basado en tiempo real.

- No es amplio el soporte para aplicaciones con alta calidad de servicio, inclusive soportando el protocolo RSVP[13].

- Con el uso de NAT[14], IPsec (Internet Protocol Security, Protocolo de Seguridad en Internet) pierde integridad al modificarse la dirección de la cabecera.

[13] RSVP: Resource Reservation Protocol, Protocolo de Reserva de Recursos

- No se pensó en la movilidad.

2.7. PROTOCOLO DE INTERNER VERSIÓN 6

El protocolo de Internet versión 6 (IPv6) surge para cubrir las necesidades actuales de direccionamiento a nivel mundial que están presentes con el actual protocolo de Internet versión 4, especialmente para asignaciones a nuevos clientes.

"IPv6 contiene un número inimaginable de direcciones para ser asignadas, dando lugar a 340 sextillones de direcciones, logrando asignar direcciones a todos los usuarios finales q podamos imaginar" (Palet J, Feb 2012).

IPv6 también llamado protocolo de la siguiente generación ya que en muchos aspectos es una extensión conservadora del actual protocolo de Internet versión 4.

2.7.1. CARACTERÍSTICAS

Protocolo de Internet versión 6 proporciona varias mejoras que hacen atractivo e interesante la implementación en dispositivos de red, se mencionan las siguientes:

[14] NAT: *Network Address Translation*

- Incremento en el tamaño de las direcciones manejando 128 bits en IPv6 frente a 32 bits de IPv4
- Nuevo formato de la cabecera en el cual se simplifica eliminando campos redundantes y al mover los campos de opciones a cabeceras de extensión que se sitúan a continuación de la cabecera IPv6, dando como resultado un procesamiento eficaz en enrutadores intermedios.
- Se incrementa la flexibilidad del protocolo permitiendo ampliación al añadir nuevas características en un futuro, sin necesidad de rediseñar por completo toda la estructura del paquete, gracias al uso de cabeceras de extensión.
- Capacidades de soporte en Calidad de Servicio y Clase de Servicio, donde se define la manera de controlar el tráfico. Por parte del campo etiqueta de flujo en la cabecera IPv6, permite etiquetar paquetes pertenecientes a un flujo particular para que los enrutadores proporcionen un control.

- Simplificación de configuraciones de hosts *con estado* bajo la presencia de un servidor DHCPv6[15] o *sin estado* sin la presencia de un servidor DCHPv6, permitiendo la configuración automática de hosts dentro de un vínculo (direcciones locales).

- Las direcciones globales usadas en IPv6 están creadas de tal manera que establecen una infraestructura eficaz y jerárquica.

[15] DHCPv6: Protocolo de configuración dinámica de host para IPv6

- Posee seguridad integrada mediante IPSec es parte del conjunto de protocolos IPv6, basado en estándares para cubrir las necesidades de seguridad en la red.

- Presenta protocolo para descubrimiento de nodos vecinos en base a un conjunto de mensajes del ICMPv6[16], remplaza a los mensajes ARP

- Computación móvil, redes LAN inalámbricas (MIPv6[17]), para dispositivos móviles PDA's[18], autos, entre otros, de igual forma para el ámbito del hogar en electrodomésticos.

- Soporte de tráfico multimedia en tiempo real.

- Envío y aplicaciones multicast (envío destinado a un grupo de receptores) y anycast (envió destinado a un receptor dentro de un grupo).

- Existen mecanismos de transición gradual de IPv4 a IPv6, permitiendo coexistencia con IPv4.

- El mínimo MTU[19] en IPv6 es de 1280 bytes (680 bytes en Ipv4).

- Los paquetes con carga útil (datos) pueden llegar a más de 65.535 bytes.

- Escalabilidad su propia estructura permite que crezca.

[16] ICMPv6: Protocolo de mensajes de control de Internet para IPv6
[17] MIPv6: Protocolo de Internet versión 6 móvil
[18] PDA: Asistente Digital Personal
[19] MTU: Unidad Máxima de Transmisión

2.7.1.1. Nueva terminología en IPv6

Al ser un nuevo protocolo existen términos propios de IPv6 los cuales con el pasar del tiempo se difundirán de tal manera que serán parte del lenguaje informático. La nueva terminología se encuentra basada en el actual protocolo de Internet versión 4, es decir en casi la mayoría de términos son semejantes al protocolo usado actualmente. Los términos más usados y/o frecuentados se encuentran en la Tabla 9.

Tabla 9

Nueva terminología en IPv6

ÍTEM	SIGNIFICADO
Anuncio de routers	Mensaje de descubrimiento de vecinos enviado por un router o de forma periódica como respuesta a un mensaje de solitud de router.
Autoconfiguración de direcciones	Proceso de configuración automática de direcciones IPv6 en un interfaz (stateful & stateless).
Descubrimiento de vecinos	Es un conjunto de mensajes y procesos ICMPv6 que determinan las relaciones entre nodos vecinos (similar al protocolo ARP en IPv4).
Direcciones de compatibilidad	Direcciones IPv6 empleadas para enviar tráfico IPv6 sobre una infraestructura IPv4 (se utilizan en direcciones 6to4 e ISATAP).
Dirección de uso local	Dirección unicast IPv6 que no es alcanzable en la Internet IPv6, incluyen direcciones locales del enlace y direcciones locales del sitio.
Dirección EUI-64	Dirección del nivel de enlace de 64 bits que se usa como base para la generación de identificadores de interfaz en IPv6.
Dirección IPv4 mapeada (dirección asignada de IPv4)	Es una dirección de la forma 0:0:0:0:FFFF:w.x.y.z ó ::FFFF:w.x.y.z, donde w.x.y.z es una dirección IPv4. Representan un nodo con soporte solo IPv4 ante un nodo IPv6.

ÍTEM	SIGNIFICADO
Interfaz	Una representación de un conexión física (interfaz de red) o lógica (interfaz de túnel de un nodo a un enlace.
Nodo IPv4	Un host o router que puede enviar y recibir paquetes IPv4, también soporta nodo dual IPv4/IPv6.
Nodo IPv6	Un host o router que puede enviar y recibir paquetes IPv6, también soporta nodo dual IPv4/IPv6.
Prefijo de red	Es la parte de la dirección que se utiliza para determinar el identificador de la subred, ruta o rango de direcciones.
Prefijo de sitio	Se refiere a todas las direcciones del sitio, generalmente con prefijo de 48 bits. Se emplean para limitar todo el tráfico asociado a prefijos dentro del sitio.
Vecino (Neighbor)	Nodo conectado al mismo enlace.

Fuente: Glosario IPv6, IPv6 Servicio de Información y Soporte, num 12, pág.3. EL PROTOCOLO IPV6

2.7.2. CABECERA IPv6

La cabecera del protocolo de Internet versión 6 se encuentra compuesta de menos campos a diferencia de la cabecera IPv4. En la Figura 9 muestra la cabecera IPv6 y a continuación sus campos que la componen.

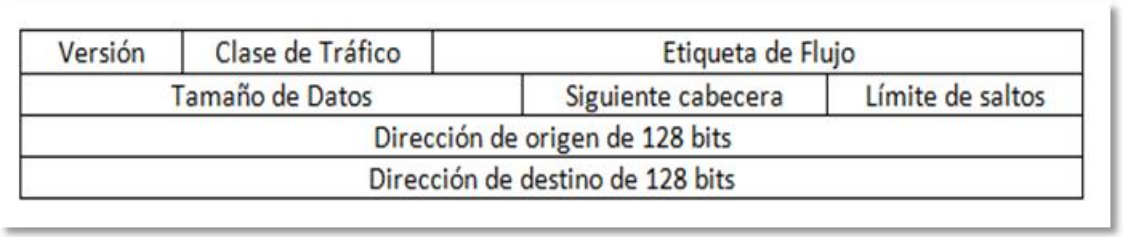


Figura 9. Campos de cabecera IPv6

Fuente: Curriculum CISCO Networking Academy Exploration v4.0. Capítulo 6: Direccionamiento de red IPv4. Semestre nro. 1.

- Versión: Similarmente en IPv4, identifica la versión del protocolo utilizado, el valor asignado es 6.

- Clase de Tráfico: Identifica y diferencia los paquetes por clases de servicios o prioridad.
- Etiqueta de Flujo: Identifica y diferencia paquetes del mismo flujo en la de red. Este campo permite que el router identifique el tipo de flujo de cada paquete, sin necesidad de verificar su aplicación.

- Tamaño de Datos: Indica el tamaño solo de los datos enviados junto con la cabecera de IPv6. Incluye el tamaño de las cabeceras de extensión.

- Siguiente cabecera: Indica sucesivamente las siguientes cabeceras, las cuales no son examinadas en cada nodo de la ruta sino en nodos destino y son opcionales. En este campo se sitúan las denominadas cabeceras de extensión incluyen información sobre tipo de extensión o identificador de protocolo de nivel superior. En la Tabla 10 se observa los tipos de cabeceras de extensión.

Tabla 10

Tipos de cabecera de extensión

CABECERA DE EXTENSIÓN	DESCRIPCIÓN
Opciones salto a salto (Hop-By-Hop Options)	Contiene datos que deben ser examinados por cada nodo a lo largo de la ruta
Ruteo (Routing)	Proporciona métodos para especificar la forma de rutear un datagrama (utilizado en IPv6 móvil).
Cabecera de fragmentación	Indica parámetros para la fragmentación

CABECERA DE EXTENSIÓN	DESCRIPCIÓN
(Fragment)	de los datagramas.
Cabecera de autenticación (Authentication Header - AH)	Contiene información para verificar la autentificación de la mayoría de los datos del paquete.
Encapsulado de seguridad de la carga útil (Encapsulating Security Payload - ESP)	Lleva información cifrada evitando inseguridad en la comunicación.
Opciones para el destino (Destination Options)	Posee información que es examinada solo en nodos destino del paquete.
No Next Header	Indica que es el fin de cabeceras de extensión

Fuente: Tutorial de IPv6. Consulintel. IPv6 Forum. Autor Jordi Palet, Director de Producto Consulinte

- Límite de Saltos: Indica el número máximo de routers que el paquete IPv6 puede pasar antes de ser descartado se decrementa en cada salto.

- Dirección de Origen: Indica la dirección de origen de 128 bits del paquete.

- Dirección de Destino: Indica la dirección de destino de 128 bits del paquete.

2.7.3. COMPARACIÓN CABECERAS IPv4 E IPv6

Dentro de los campos de la cabecera del protocolo IPv4 en comparación a la cabecera del protocolo IPv6 existen algunos campos que fueron modificados y en otros fueron eliminados con la finalidad de evitar el redundancia como muestra la Figura 10 que indica los campos que se encuentran en letra negrita fueron campos eliminados y los restantes fueron

campos modificados, mientras que los campos: versión, dirección de origen y de dirección destino mantienen la denominación en las dos cabeceras mas no en su tamaño, dando lugar a la cabecera IPv6 (Figura 11). El resumen de las diferencias de las dos cabeceras se presenta en la Tabla 11.

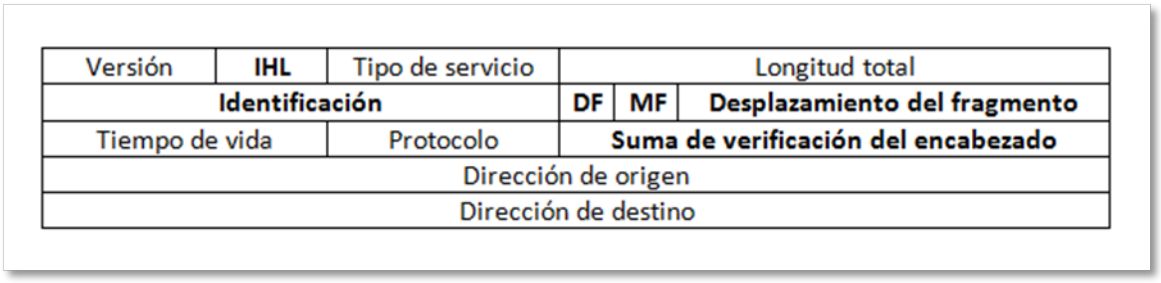


Figura 10. Campos eliminados y modificados de la cabecera IPv4

Fuente: Propia

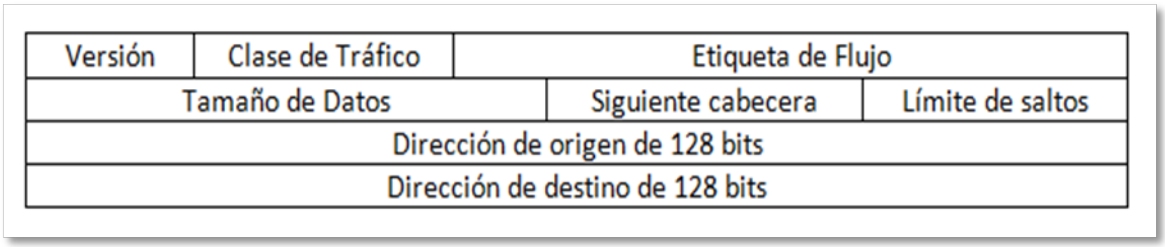


Figura 11. Cabecera final IPv6

Fuente: Curriculum CISCO Networking Academy Exploration v4.0. Capítulo 6: Direccionamiento de red IPv4. Semestre nro. 1.

Tabla 11

Comparación campos de cabeceras IPv4 e IPv6

CAMPO	IPv4	IPv6
Versión	Muestra la versión del protocolo que se esta trabajando	Muestra la versión del protocolo que se esta trabajando
Longitud de la cabecera (IHL)	Muestra el tamaño de la cabecera del paquete.	Campo eliminado en IPv6
Tipo de servicio / Clase	Aplican QoS de acuerdo a	Aplican CoS de acuerdo a

CAMPO	IPv4	IPv6
de tráfico	prioridad establecida	prioridad establecida
Longitud total	Muestra el tamaño total de paquete	Campo eliminado en IPv6
Etiqueta de flujo	Campo propio de IPv6	Reduce el proceso de ruteo, permitiendo tráfico de tiempo real
Identificación	Identifica fragmentos de un paquete	Campo eliminado en IPv6
Tamaño de datos	Campo propio de IPv6	Muestra tamaños de datos enviados
DF y MF	Muestran si existen fragmentos o no	Campos eliminados en IPv6
Desplazamiento del fragmento	Usado en base a DF y MF	Campo eliminado en IPv6
Protocolo / Siguiente cabecera	Muestra el siguiente contenido a enviar	Muestra la siguiente cabecera de extensión
Tiempo de vida / Límite de saltos	Muestra el número de saltos antes que el paquete sea descartado	Muestra el número de saltos antes que el paquete sea descartado
Suma de verificación del encabezado	Actualiza la cabecera si algún campo ha cambiado	Campo eliminado en IPv6
Dirección de origen	Dirección de 32 bits	Dirección de 128 bits
Dirección de destino	Dirección de 32 bits	Dirección de 128 bits

2.7.4. DIRECCIONAMIENTO IPv6

Una dirección IPv6 es representada en notación hexadecimal, compuesta de 8 campos de 16 bits separados con dos puntos cada campo. Si una dirección IPv6 contiene en sus campos los valores de ceros, estos pueden

ser reemplazados por dos puntos y solo puede remplazar una sola vez dentro de la dirección IPv6 como indica en la Tabla 12.

Tabla 12

Notación hexadecimal de dirección IPv6

DIRECCIÓN IPv6	NOTACIÓN
2800:68:19:6:**0000:0000:0000**:136	Notación hexadecimal
2800:68:19:6**::**136	Notación hexadecimal comprimida

La dirección IPv6 va acompañada del prefijo que es un identificador de subred, routers y rangos de direcciones similar a la forma utilizada en IPv4, explicada en la Tabla 13.

Tabla 13

Prefijo en IPv6

DIRECCIÓN IPv6		
ÍTEM	**SIGNIFICADO**	**EJEMPLOS**
Dirección IPv6	Dirección IPv6 expresada en formato hexadecimal en cualquiera de las notaciones descritas anteriormente.	A:B:C:D:E:FFF:129.144.52.38 2002:aad2:ee19::1
Longitud de prefijo	Es un valor decimal que especifica cuántos de los bits más significativos, representan el prefijo de la dirección hexadecimal.	2800:68:19:6::136/64

2.7.4.1. TIPOS DE DIRECCIONES IPv6

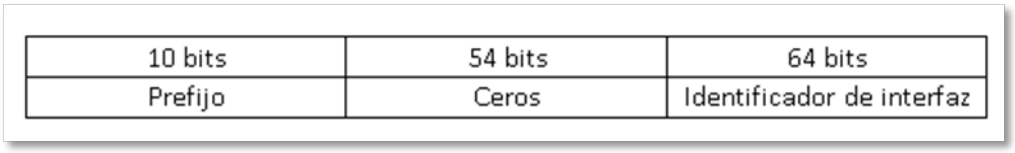
En el RFC 2406 se identifican tres tipos de direcciones en IPv6 clasificadas de la siguiente manera para identificar a una o conjunto de interfaces:

2.7.4.1.1. Unicast

Direcciones Unicast o unidirigidas especifican a una sola dirección de una interface del nodo terminal. En este tipo de direcciones los paquetes son entregados a una interfaz específica del nodo destino.

Se definen dos tipos de direcciones unicast de uso local: local de enlace y local de sitio.

- Local de enlace o “link local”: Son direcciones diseñadas para redireccionar un único enlace para fines de autoconfiguración, descubrir vecinos o en situaciones en las que no existen routers. Tiene limitación a solo red local, asignación FE80::<ID de Interfaz>/10. Posee el siguiente formato (Figura 12):



10 bits	54 bits	64 bits
Prefijo	Ceros	Identificador de interfaz

Figura 12. Formato link local

Fuente: Olifer, N., Olifer, V. (2009). Redes de computadoras.

- Local de sitio o “site local”: Son direcciones que permiten direccionar dentro de un “sitio” u organización. Se configuran a partir de un

identificador de subred de 16 bits. Se limita al envío de paquetes dentro de local de sitio, asignación FEC0::<ID de Subred>:<ID de Interfaz>/10. Posee el siguiente formato (Figura 13):

10 bits	38 bits	16 bits	64 bits
Prefijo	Ceros	ID de subred	Identificador de interfaz

Figura 13. Formato site local

Fuente: Olifer, N., Olifer, V. (2009). Redes de computadoras.

2.7.4.1.2. Multicast

Direcciones multicast o multidirigidas identifican un grupo de interfaces contenidas por diferentes hosts, son paquetes se entregan a todas las interfaces que tienen esa dirección. Se identifican mediante la dirección FF00::/8.

Un nodo puede pertenecer a uno o varios grupos multicast. Direcciones multicast poseen el siguiente formato (Figura 14):

8 bits	4 bits	4 bits	112 bits
Prefijo	Ceros	ID de subred	Identificador de grupo

Figura 14. Formato multicast

Fuente: Olifer, N., Olifer, V. (2009). Redes de computadoras.

Dentro del formato multicast existe el bit “T” el cual puede contener valores de cero (indica que es dirección multicast permanente) y valor uno (indica que es dirección multicast temporal).

Los valores del bit “ámbito” del formato multicast pueden tener los siguientes significados como indica en la Tabla 14 (los valores restantes aún no están asignados):

Tabla 14

Significados del bit ámbito

BIT	SIGNIFICADO
0	Reservado
1	Ámbito Local de Nodo
2	Ámbito Local de Enlace
5	Ámbito Local de Sitio
8	Ámbito Local de Organización
E	Ámbito Global
F	Reservado

Fuente: Tutorial de IPv6. Consulintel. IPv6 Forum. Autor Jordi Palet, Director de Producto Consulinte

Y por último el identificador de grupo, como su nombre indica identifica si el grupo multicast es temporal o permanente en un ámbito determinado.

2.7.4.1.3. Anycast

Direcciones anycast son similares a direcciones multicast. El paquete se entrega a solo una interfaz dentro del grupo de interfaces que contengan este tipo de dirección. Se puede decir que una dirección anycast surge a partir de la asignación unicast a más de una interfaz (Figura 15).

Existe una dirección anycast, requerida para cada subred, denominada "dirección anycast del router de la subred", en la cual todos los routers dentro de esa subred soportaran esta dirección y los paquetes enviados a esta dirección serán entregados a un router de la subred.

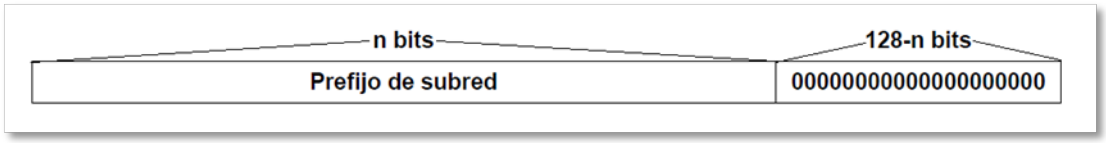


Figura 15. Formato anycast

Fuente: Olifer, N., Olifer, V. (2009). Redes de computadoras. México: Litografía Ingramex

2.7.5. AUTOCONFIGURACIÓN

"IPv6 tiene una característica que permite a un host decidir la manera de autoconfigurar sus direcciones de interfaces, dando lugar a que el nuevo protocolo de Internet sea Plug & Play[20]" (Palet J, Feb 2012).

Existen dos maneras de permitir que un host decida como auto-configurarse, puede ser por medio de configuración predeterminada (stateful) o automática (stateless). Las dos configuraciones automáticas poseen un algoritmo para la detección de direcciones duplicadas.

2.7.5.1. Autoconfiguración de direcciones stateful

En autoconfiguración stateful se lleva a cabo mediante la utilización de un protocolo de autoconfiguración de direcciones stateful por ejemplo DHCPv6,

[20] Plug &Play: Término que se refiere a la capacidad de un sistema informático de configurar automáticamente los dispositivos al conectarlos.

obteniendo direcciones de interfaz, parámetros de configuración asociados y base de datos de direcciones que han sido asignadas a otros hosts.

2.7.5.2. Autoconfiguración de direcciones stateless

En autoconfiguración stateless se basa en el uso de procedimientos como: utilización de combinación de información disponible localmente, descubrimiento de vecinos, anuncios de routers para obtener direcciones IPv6 y parámetros de configuración asociados.

En el caso de no existir routers, un host solo puede generar direcciones de enlace local, siendo muy útil para la comunicación de varios nodos en el mismo enlace.

2.7.6. PROTOCOLOS EN IPv6

Los protocolos utilizados en IPv6 poseen el mismo fundamento que los protocolos en IPv4, los cuales han sido adaptados para trabajar con el nuevo protocolo.

2.7.6.1. ICMPv6 (Internet Control Message Protocol version 6, Protocolo de Control de Mensajes de Internet versión 6)

“Protocolo actualizado para permitir su uso bajo IPv6 y de igual forma que en IPv4 es utilizado para reportar errores en el trascurso de envío de paquetes hacia diferentes destinos” (Palet J, Feb 2012).

ICMPv6 tiene el siguiente formato (Figura 16), compuesta de los siguientes campos:

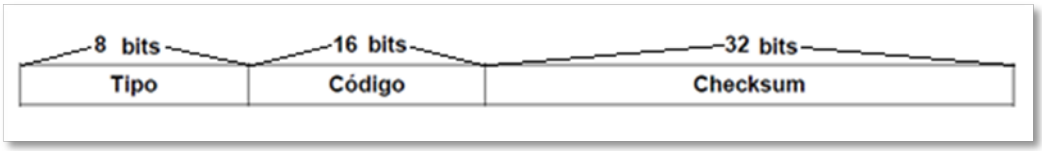


Figura 16. Formato ICMPv6

Fuente: Tutorial de IPv6. Consulintel. IPv6 Forum. Autor Jordi Palet

- Tipo: indica el tipo de mensaje y su valor determina el formato del resto de la cabecera.

- Código: depende del tipo de mensaje, crea un nivel adicional de jerarquía para la clasificación del mensaje.

- Checksum: permite detección de errores en el mensaje ICMPv6.

Los mensajes ICMPv6 se agrupan en dos tipos: mensajes de error con valores entre 0 y 127 y los mensajes informativos con valores desde 128 y 255, como indica la Figura 17.

Mensajes de error ICMPv6		
Tipo	Descripción y Códigos	
1	Destino no alcanzable (Destination Unreachable)	
	Código	Descripción
	0	Sin ruta hacia el destino
	1	Comunicación prohibida administrativamente
	2	Sin asignar
	3	Dirección no alcanzable
	4	Puerto no alcanzable
2	Paquete demasiado grande (Packet Too Big)	
3	Tiempo excedido (Time Exceeded)	
	Código	Descripción
	0	Límite de saltos excedido
	1	Tiempo de desfragmentación excedido
4	Problema de parámetros (Parameter Problem)	
	Código	Descripción
	0	Campo erróneo en cabecera
	1	Tipo de "cabecera siguiente" desconocida
	2	Opción IPv6 desconocida
Mensajes informativos ICMPv6		
Tipo	Descripción	
128	Solicitud de eco (Echo Request)	
129	Respuesta de eco (Echo Reply)	

Figura 17. Especificación de mensajes de error e informativos de ICMPv6

Fuente: Tutorial de IPv6. Consulintel. IPv6 Forum. Autor Jordi Palet,

2.7.6.2. Neighbor discovery (ND)

Descubrimiento de vecinos corresponde en cierto modo a ARP en IPv4. Se basa en un mecanismo en el cual un nodo que se incorpora en la red descubre la presencia de otros nodos dentro de su mismo enlace para así determinar sus direcciones en la capa de enlace y localizar routers para mantener la información de conectividad sobre las rutas activas de vecinos.

Descubrimiento de vecinos es un protocolo completo y sofisticado ya que por medio de él permite realizar el mecanismo de autoconfiguración en IPv6.

Para los servicios proporcionados en ND utiliza mensajes ICMPv6, definiendo cinco tipos de paquetes ICMPv6:

- Solicitud de Router (Router Solicitacion): Generado por una interfaz cuando es activada, para solicitar que los routers se anuncien inmediatamente. Tipo de paquete ICMPv6 = 133.

- Anunciación de Router (Router Advertisement): Generado en forma periódica por los routers para informar sobre ciertos parámetros como: presencia, enlace, Internet, tiempos de vida, configuración de direcciones, límite de salto, entre otros. Tipo de paquete ICMPv6 = 134.

- Solicitud de Vecino (Neighbor Solicitacion): Generado por nodos para verificar que el nodo sigue activo y/o es alcanzable, también detecta direcciones duplicadas. Tipo de paquete ICMPv6 = 135.

- Anunciación de Vecino (Neighbor Advertisement): Generado por los nodos en respuesta a la solicitud de vecino o para indicar cambios de direcciones en la capa de enlace. Tipo de paquete ICMPv6 = 136.

- Redirección (Redirect): Generado por routers para informar a los hosts acerca de mejor salto para llegar a su destino. Tipo de paquete ICMPv6= 137.

2.7.6.3. DHCPv6

Protocolo para el soporte de IPv6, diseñado para reducir el coste de gestión de nodos IPv6 en ambientes donde los administradores requieren control sobre la asignación de recursos de red, proporcionados por el mecanismo de configuración stateless.

La manera en que DHCPv6 reduce coste de gestión es al enfocarse en la gestión de recursos de red de uno o varios servidores DHCP como es direcciones IP, brindar información de encaminamiento, información de instalación de sistemas operativos, información de servicios de directorios con la finalidad de no distribuir esta información en ficheros de configuración local en cada nodo.

Las características DHCPv6 se presentan a continuación:

- DHCPv6 es un mecanismo, más no una política.
- Es compatible con el mecanismo de autoconfiguración stateless.
- No requiere configuración manual de parámetros de red.
- No requiere un servidor en cada enlace (realimentadores DHCP).
- Coexiste con nodos configurados estáticamente.
- Clientes DHCPv6 pueden operar en enlaces donde no hay routers IPv6.
- Clientes DHCPv6 proporcionan la habilidad de renumerar la red.

- Configuración de actualización dinámica de DNS.
- Autenticación.
- Los clientes pueden solicitar múltiples direcciones IP.
- Integración entre autoconfiguración de direcciones stateless y stateful.
- DHCPv6 incorpora mecanismos apropiados de control de tiempo y retransmisiones para operar eficazmente en entornos con alta latencia y/o reducido ancho de banda.

2.6.7. PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento en IPv6 se basan en los principios manejados por los protocolos de enrutamiento en IPv4, adaptados en algunos aspectos para trabajar con el nuevo protocolo.

2.6.7.1. RIPng

En base a RFC 2080 RIPng Protocolo RIP de nueva generación contiene características similares que RIPv2 en IPv4 como se muestra en la Tabla 15.

Tabla 15

Diferencias de RIP para IPv4 e IPv6

ÍTEM	RIPv2 EN IPv4	RIPNG EN IPv6
Protocolo vector distancia	Si	Si
Número mínimo de saltos	15	15
Horizonte dividido	Si	Si
Dirección multicast para envío de actualizaciones	224.0.0.9	FF02 :: 9
Puerto UDP	520	521

Al aplicar RIPng en un router se estima que cada interfaz contiene una o mas redes y este a su vez realiza un seguimiento al siguiente salto de acuerdo a la dirección local de enlace (link local) y no de acuerdo a la dirección global.

2.6.7.2. OSPFv3

Es importante aclarar que la versión que tiene OSPF en IPv6 (OSPFv3) es la continuación de la versión que maneja OSPF en IPv4 (OSPFv2). OSPFv3 es un protocolo específico para IPv6 y mantiene los principios de OSPF en IPv4, características similares como el manejo de áreas autónomas en un sistema, hacen uso del algoritmo de Dijkstra y las diferencias que se indican en la Tabla 16.

Tabla 16

Diferencias de OSPF para IPv4 e IPv6

ÍTEM	OSPFv2 EN IPv4	OSPFv3 EN IPv6
Dirección multicast para envió de actualizaciones	224.0.0.5 para routers OSPFv2 224.0.0.6 para routers OSPFv2 designados	FF02 :: 5 para routers OSPFv3 FF02 :: 6 para routers OSPFv3 designados
ID Router, ID de área, ID de LSA	Direcciones IPv4 establecidas	Direcciones IPv6 no establecidas

2.6.8. SEGURIDAD EN IPv6

La seguridad en IPv6 incluye IPSec con el mismo principio de funcionamiento que en IPv4, maneja mecanismos de seguridad, autenticación y encriptación, en su núcleo del protocolo. IPSec (Internet Protocol Security) es el protocolo de seguridad en Internet, diseñado para brindar seguridad y protección al trafico IP.

Fernando Gont especialista en seguridad IPv6, explica que el manejo de seguridad en IPv6 posee algunas debilidades que son atractivas para los atacantes descritas a continuación:

- Scaneo de direcciones.- Consiste en identificar dentro de todo un rango de direcciones hasta encontrar la indicada, IPv6 contempla un rango de 2 elevado 128 combinaciones posibles de direcciones, como resultado de este escaneo de direcciones

casi imposible para el atacante. Para abordar por este medio el atacante identifica patrones que son útiles para su fin como identificar el formato EUI-64 porque algunas direcciones IPv6 se componen de esta manera.

Como mecanismo de defensa se sugiere escoger direcciones IPv6 aleatoriamente.

- Comunicación extremo a extremo.- La red actual funciona bajo NAT que proporciona inteligencia a la red, la ausencia de NAT provocaría vulnerabilidad en la red, en IPv6 no incluye NAT en su implementación, para este caso se sugiere el uso de Firewall con una política de seguridad definida.

- Resolución de direcciones y autoconfiguración de direcciones.- Los atacantes pueden utilizar una resolución de dirección y autoconfiguración para realizar ataques de Man in the Middle (Hombre en la mitad) y ataques de denegación de servicio. Se sugiere particionar la red o delimitar algunos accesos.

- Mecanismos de transición.- Al realizar un tunelamiento o una traducción de direcciones IPv4 a IPv6 y viceversa el atacante puede aprovechar el único punto de fallo que es un host donde se realizan cualquiera de estos procesos.

2.6.9. COMPARACIÓN TÉCNICA IPv4 E IPv6

De las versiones de protocolos de Internet podemos citar sus características que han hecho relevante su uso y aplicación, se presentan en la siguiente Tabla 17:

Tabla 17

Comparación técnica IPv4/IPv6

ÍTEM	IPv4	IPv6
Direcciones disponibles	Alrededor de 4.200 millones	Alrededor de 340 sextillones representados en formato hexadecimal
Longitud de direcciones	32 bits	128 bits
Representación de direcciones	Formato Decimal	Formato Hexadecimal
Tipos de direcciones	Clasificadas en clase A,B,C,D,E, orientado al direccionamiento	Clasificadas en unicast, multicast, anycast; orientado al encaminamiento
Campos de cabecera	12 campos	8 campos, cabecera reducida
Configuración de direcciones	Automática con el uso de servidor DHCP	Automática con o sin el uso de servidor DHCP, Staleless y/o Statefull
Cabecera	Incluye suma de comprobación (checksum)	No incluye suma de comprobación (checksum). Capa enlace de datos y capa transporte protegen la integridad del paquete
Fragmentación	Realizan routers y host, MTU de 680 bytes	Realizan solo hosts, generalmente no hay fragmentación por MTU de 1500 bytes
Cabecera	No contiene campo siguiente cabecera	Contiene campo siguiente cabecera donde se sitúan las cabeceras de extensión que identificar características que serán utilizadas a futuro

Seguridad	IPSec es opcional	IPSec es propio, al no existir NAT la cabecera no tiene modificaciones
Dirección Loopback	172.0.0.1	::1/128 dirección unicast del localhost
Dirección no especificada	0.0.0.0	::/128
NAT	Requiere su uso	No requiere su uso existen direcciones suficientes
Movilidad	No es aplicable	Es aplicable, posee MIPv6 (Protocolo de Internet versión 6 móvil)
Escalabilidad	IPv4 no posee escalabilidad	IPv6 posee escalabilidad gracias al numero de direcciones posibles

2.6.10. VENTAJAS Y BENEFICIOS DE IPv6

El poseer el nuevo protocolo de Internet en la red proporciona varias ventajas y beneficios que opacan la versión usada actualmente. Se mencionan las siguientes:

- Por medio de la autoconfiguración de direcciones en la cual un host decide como autoconfigurar sus interfaces, permite afirmar la ventaja de que IPv6 sea Plug & Play.

- Actualmente casi todos los equipos informáticos ya poseen en su sistema operativo el soporte para el nuevo protocolo, evitando de esa manera su instalación.

- El interminable número de direcciones disponibles permitirá tranquilidad sobre la asignación de direcciones y más bien permitirá el desarrollo de nuevas aplicaciones orientadas domótica en el hogar.

- Al examinar menos campos dentro de la cabecera del paquete IP por parte de los routers, facilita el envío y recepción de paquetes de manera efectiva.

- Permite la evolución de aplicaciones en tiempo real orientados al aprendizaje a distancia como tele-educación, tele-medicina basados en interactividad y simulación. Así como también aplicaciones avanzadas como Grid[21], ambientes inteligentes, entre otros.

- Con el manejo de IPv6, NAT queda en desuso, permite realizar comunicaciones extremo a extremo bajo el protocolo de seguridad IPSec.

- Sin la necesidad de modificar la cabecera IPv6, podemos identificar características en el campo cabeceras de extensión que serán utilizadas a futuro.

- Con IPv6 se puede diferenciar aquellos paquetes de datos cuyo contenido pertenecen a un flujo de datos en particular, para destinar un ancho de banda de acuerdo a cada necesidad, dando lugar a poseer Calidad de Servicio (QoS).

- Videoconferencias sin retardo, routers realizan menor procesamiento en analizar una cabecera IPv6 al contener menos campos y con ayuda de

[21] Grid: Es una tecnología que permite utilizar de manera coordinado todo tipo de recurso como es computadores.

los campos clase de tráfico y etiqueta de flujo en cabecera IPv6; no se usa NAT pudiendo establecer comunicaciones extremo a extremo.

- De igual manera se fusiona la ventaja de Grid y la movilidad al facilitar acceso a los recursos desde cualquier organización cuando los investigadores se trasladan hacia otro grupo de trabajo.

2.6.11. FUTURO DE IPv6

La activación de IPv6 produce cambios en todo el entorno tecnológico iniciando con proveedores de servicios de Internet, hardware, software y sobre todo personal capacitado. Las aplicaciones que surgen a partir de estos cambios están enfocadas a mejorar servicios a usuarios finales.

Con la gran cantidad de direcciones que posee IPv6 pretende conectar a todo lo queremos que este conectado. Varios desarrolladores ya poseen su plan de trabajo y otros se encuentran implementando aplicaciones como las siguientes:

- Movilidad.- Es la ventaja más atractiva que posee el nuevo protocolo permitiendo la conexión o desconexión de muestro dispositivo a redes IPv6 directamente sin el requerimiento de alguna aplicación adicional. Con IPv6 hace posible el desplazamiento del dispositivo de una red a otra, evitando el cambio de dirección IP de origen. En movilidad IPV6 se presenta el siguiente escenario, el dispositivo móvil con su dirección de origen recibe paquetes de su propia red donde se encuentra, al

iniciar el desplazamiento obtiene una dirección remota proporcionada por autoconfiguración stateless o stateful, se realiza una asociación entre dirección de origen y dirección remota para que la dirección que dio como resultado sea registrado en el agente remoto por medio del envío de un mensaje Binding Updates, la respuesta al mensaje proviene del router de la red de origen y envía un mensaje Binding Acknowledgement de esta manera el dispositivo móvil se registra en el nodo correspondiente. Cuando el dispositivo regresa envía un mensaje Binding Updates para informar al agente de origen que regresa a su red.

- IPv6 and The Smart Grid (IPv6 y Grid Inteligente).- “Combinación de la red de energía eléctrica y de la información y comunicaciones (TIC) con los objetivos de entrega de suministros eléctricos de manera eficiente, sostenible, económico y seguro.” Grossetete Patrick (2011, Junio 07). Esta poderosa aplicación incluye al manejo de tres áreas importantes como arquitectura, seguridad y conexión a la red inteligente.

- IPv6 in the Safety World (IPv6 en el Mundo de la Seguridad).- Contempla seguridad y vigilancia a nuestros vienes conectados a la red, divididas en tres categorías:
    - Seguridad de las infraestructuras críticas (distribución de energía, suministro de alimentos, apoyo médico, Transporte).

- Seguridad de la gestión de crisis (alarmas / advertencias, apoyo a las decisiones, mando y control).
- Seguridad de las características en soluciones TIC (confidencialidad, integridad, disponibilidad, autenticación, utilidad).

CAPÍTULO 3

MECANISMOS DE TRANSICIÓN

En el capítulo tres muestra los mecanismos de transición para que los protocolos de Internet versión 4 y versión 6 puedan coexistir. Estos mecanismos definidos por la IETF se encuentran agrupados de tres categorías: doble pila, túneles y traducción de los cuales se muestra sus características, métodos, pros y contras en su proceso de implementación, de acuerdo al análisis se selecciona el mecanismo de transición para la UTN.

3.1. INTRODUCCIÓN

La precaución por parte de los administradores de red, ha originado que poco a poco se difunda las ventajas que posee el nuevo protocolo de Internet versión 6 para posteriormente implementar en la gran red de redes, Internet, donde IPv6 llega a proporcionar una transición de manera gradual permitiendo que se puedan aplicar varias alternativas para los dos protocolos.

Para lograr este objetivo se presenta el escenario donde IPv4 trabaja en conjunto con IPv6, para ello se encuentran establecidos mecanismos de transición que deben ser seleccionados por los administradores de red o técnicos capacitados sobre el tema.

La transición es casi transparente en capas superiores a partir de la capa donde se encuentra el protocolo IP.

La clave del éxito de la transición con IPv6 se centra en la compatibilidad con la mayor parte de la red existente, para ello existen tres modelos de implementación para la transición de IPv4 a IPv6 y son los siguientes:

a) Doble pila: Servidores y dispositivos trabajando y/o hablando con los dos protocolos.

b) Túneles: Técnica de encapsular paquetes IPv6 dentro de un paquete IPv4

c) Traducción: Técnica que permite comunicación entre dispositivos que son solo IPv4 con dispositivos que son solo IPv6.

3.2. DUAL STACK / DOBLE PILA

Doble pila es un mecanismo de transición que habilita la pila IPv6 al sistema operativo, trabajando conjuntamente los dos protocolos de Internet. Al mantener doble pila los equipos de red y demás dispositivos deben soportar ambos protocolos IPv4/IPv6. Doble pila también se conoce como mecanismo de integración de IPv6 a las redes actuales.

Al incluir la pila IPv6, los protocolos de capas superiores funcionan con normalidad hasta llegar a capa aplicación, debido a la compatibilidad que poseen con el nuevo protocolo.

Cada nodo doble pila lleva configurado direcciones IPv4 e IPv6, admitiendo recibir y enviar paquetes con ambos protocolos con la finalidad de

permitir comunicación en la nube de Internet con nodos duales. En una comunicación con el mecanismo doble pila el comportamiento de la red se efectúa en dos situaciones: cuando se utiliza IPv6 se comporte como un nodo IPv6 y si se utiliza IPv4 se comporte como un nodo IPv4. Es la opción más aceptada hacia una transición completa (migración) para una Internet que maneje solo IPv6 en un futuro cercano.

Es importante saber que al mantener doble pila cada protocolo de Internet funciona independiente uno del otro, es decir que cada protocolo posee un enrutamiento propio y reglas para filtrar tráfico propias. La experiencia de trabajar simultáneamente con ambos protocolos proporciona una gran ventaja a largo plazo al poseer conocimiento y/o dominio sobre IPv6.

En esta técnica de transición todos los dispositivos de red deben soportar servicios y aplicaciones IPv4 como servicios y aplicaciones IPv6.

Dependiendo sobre cual nodo se esté trabajando, la aplicación hace uso de la dirección requerida IPv4 o IPv6 como la apropiada. Esto es determinado por la respuesta del DNS a un nombre de nodo, en la cual la tiene como prioridad responder en IPv6 y luego en IPv4. Finalizando su respuesta hacia la solicitud si el DNS regresa una dirección IPv4, ésta será usada y si regresa una dirección IPv6, ésta será utilizada.

Al habilitar IPv6 en un equipo que trabaja con IPv4, la información transmitida es encaminada de acuerdo al tipo de protocolo identificado en la trama Ethernet (Figura 18).

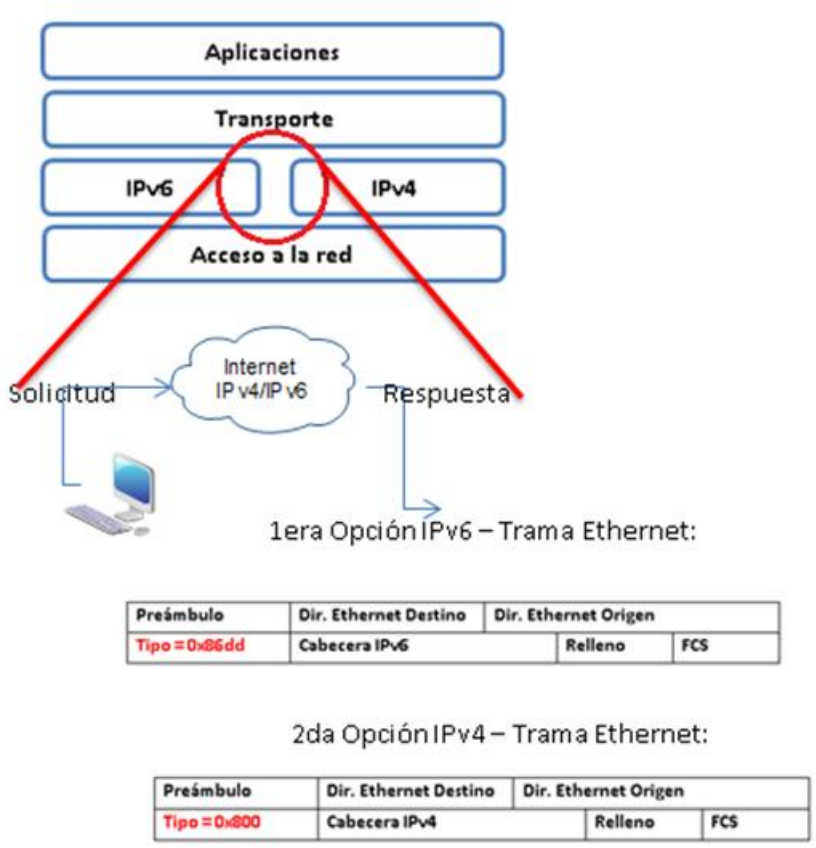


Figura 18. Mecanismo de transición Dual Stack

Fuente: Propia

"Cuando un paquete llega al router es identificado por su trama Ethernet (RFC 2464) por el campo Ethertype que indica el protocolo transportado de capa superior es IPv6, seguidamente se procesa el encabezado y se analiza la dirección de destino, el router busca en la tabla de enrutamiento unicast (RIB – Router Information Base) si existe alguna entrada a la red de destino. El router tiene configurado en cada interfaz con una dirección IPv6, información que forma parte de la tabla de rutas que posee el mismo. Cuando el router identifica la interfaz hacia donde va a dirigir el tráfico, decrementa el limite de salto, arma la trama Ethernet y envía el paquete" (Enrutamiento IPv6, 2011).

Una desventaja es la sobre carga para los routers que ejecutan dos tablas de enrutamiento para ambos protocolos al querer comunicarse con el mundo exterior.

3.3. TÚNELES

Para establecer una comunicación utilizando el mecanismo de transición denominado túneles, se efectúa mediante el encapsulamiento de paquetes IPv6 dentro de paquetes IPv4, sobre la infraestructura actual que es IPv4.

Dentro del proceso de realizar túnel o tunelamiento intervienen tres componentes:

- Encapsulación: El nodo de la entrada del túnel crea la encapsulación dentro de la cabecera IPv4 y transmite los paquetes encapsulados.

- Desencapsulación: El nodo de salida del túnel recibe el paquete encapsulado para quitar la cabecera IPv4.

- Administración del túnel: Configuración de parámetros del túnel en el extremo (router de la institución).

En los extremos del túnel se sitúan nodos doble pila cuya función es la de encapsular y desencapsular un paquete. Un paquete puede ser encapsulado de cuatro maneras diferentes:

a) De router a router: El segmento de la ruta se extiende de extremo a extremo entre dos hosts.

b) Host a router: El primer segmento de la ruta se extiende de extremo a extremo entre dos hosts.

c) Router a host: El último segmento de la ruta se extiende de extremo a extremo entre dos hosts.

d) Host a host: Se extiende la ruta completa extremo a extremo entre dos hosts.

Generalmente se utiliza la configuración de router a router porque es el principal medio para la configuración de túnel en los puntos finales.

En el momento de encapsular un paquete IPv6 dentro de un paquete IPv4, se pueden presentar algunas situaciones complejas como la fragmentación de paquetes dentro del túnel cuando el paquete es demasiado grande.

Existen algunos mecanismos de transición disponibles basados en túneles para ser aplicados dependiendo de la situación de la red, cada uno de los que se explican a continuación:

- 6to4
- 6over4
- Teredo
- Túnel Broker
- DSTM

3.3.1. 6to4

"El mecanismo 6to4 permite comunicar dominios IPv6 a través de nubes IPv4, encapsulando paquetes IPv6 dentro de un paquete IPv4 y enviarlo hacia un equipo que posea las dos redes para que llegue a su destino en IPv6" (www.ietf.org/rfc3056, Feb 2012).

En 6to4 se define el rango con su respectivo prefijo 2002::/16 de direcciones IPv6 utilizadas en el encapsulamiento para la comunicación bajo el protocolo de Internet versión 4. Su implementación es generalmente asignada en los routers frontera determinándose a una configuración de router a router. En una comunicación 6to4 se requieren los siguientes elementos:

a) Router 6to4: Permite el encaminamiento de paquetes encapsulados con 6to4.

b) Dirección IPv4 pública: La dirección pública se utiliza para establecer una dirección 6to4, por ejemplo se tiene 192.1.2.3 dirección IPv4, que se transforma cada octeto en formato hexadecimal, dando lugar a la dirección final 6to4 2002:c001:0203::/48 (dirección compatible IPv4/IPv6).

c) Relay 6to4: Relay o retransmisor 6to4 se encuentra situado en la nube de Internet IPv4 tiene como dirección propia 192.88.99.1, su función es retransmitir los paquetes 6to4 encapsulados para que lleguen a su destino.

Cuando un paquete IPv6 es encapsulado con 6to4, se asigna en el campo protocolo el valor 41 en su cabecera IPv4, siendo un requisito en este tipo de transición que las redes que deseen implementar 6to4 sean capaces de enviar paquetes IPv4 con el valor mencionado.

En una dirección 6to4 los primeros 16 bits del prefijo es 2002, los siguientes 32 bits son de la dirección IPv4 global del router del extremo local del túnel y los últimos 16 bits se eligen arbitrariamente por el router.

En la comunicación entre dominios 6to4 cada extremo del túnel se determina por el prefijo de dirección destino IPv6 obtenida del paquete. Si la comunicación se establece entre un dominio 6to4 y un dominio no 6to4, requiere el uso de un relay 6to4 que tiene conexión dual stack, cuando los paquetes llegan a la interfaz IPv4 con su contenido IPv6, dicho contenido se dirige a la red IPv6; cuando un paquete llega a la interfaz IPv6 con prefijo de dirección 2002 sirve para que los routers lo reconozcan y envíen paquetes encapsulados sobre IPv4.

Los dominios IPv6 construyen su prefijo en base a la dirección del router de frontera IPv4. Donde la dirección es el prefijo 2002 seguido por los siguientes 32 bits de dirección del router de frontera IPv4.

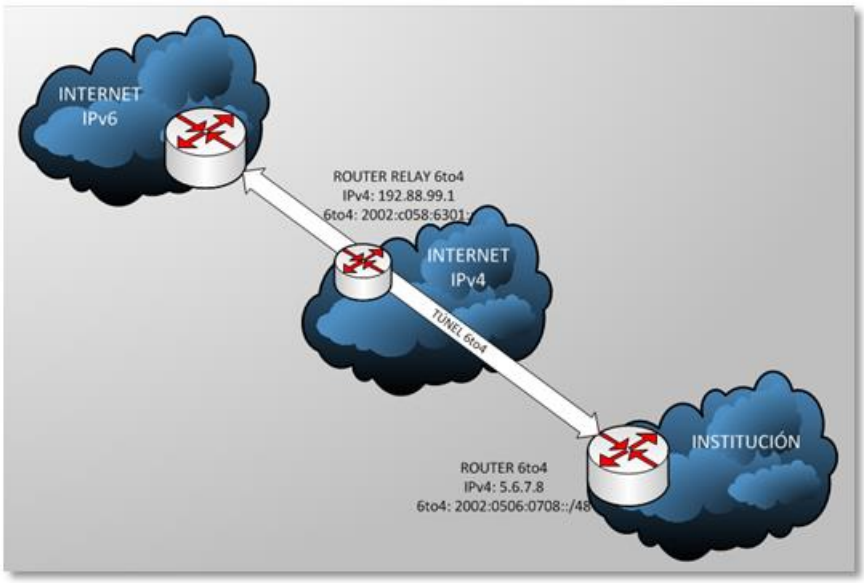


Figura 19. Mecanismo de transición 6to4.

Fuente: Propia

En la Figura 19 muestra el esquema de una comunicación 6to4, cuando la institución que quiere acceder a Internet IPv6 debe configurar en su router la dirección 6to4 se obtiene en base a la dirección pública, para comunicarse hacia otro router 6to4 en la gran nube de Internet existen routers relay 6to4 que sirven para la retransmisión de paquetes 6to4.

Posee como ventaja la buena conectividad IPv6 en una Intranet cuando el proveedor de servicios de Internet es solo IPv4.

3.3.2. 6over4

6over4 mecanismo para transmisión de IPv6 sobre dominios IPv4 sin túneles establecidos, en el escenario corre una red IPv6 usando la red actual bajo el protocolo de descubrimiento de vecinos NDP[22].

[22] NDP: Neighbor Discovery Protocol

La finalidad de 6over4 es interconectar host IPv6 aislados en un sitio por medio de una encapsulación, usa direcciones IPv4 como identificadores de interfaces creando un enlace virtual utilizando un grupo multicast (multidifusión). En este tipo de transición de túnel se requiere que la infraestructura IPv4 se encuentre habilitada en modo multicast. IPv6 multicast se implementa a través de IPv4 multicast del cual se deriva la utilización de descubrimiento de vecinos con IPv6, pero son pocas las redes que soportan multicast con el protocolo de Internet actual (se utiliza IPv4 multicast como Ethernet virtual). La Figura 20 muestra el escenario de 6over4.

Este mecanismo se establece para permitir a host IPv6 aislados situados en un vínculo físico que no tienen conectado directamente IPv6 en el router, lleguen a tener conectividad utilizando un dominio IPv4 como su enlace virtual. Para una interfaz virtual las direcciones locales IPv6 poseen el prefijo FE80::/64, los host configuran por defecto automáticamente cada interface 6over4 con la sintaxis FE80::w.x.y.z.

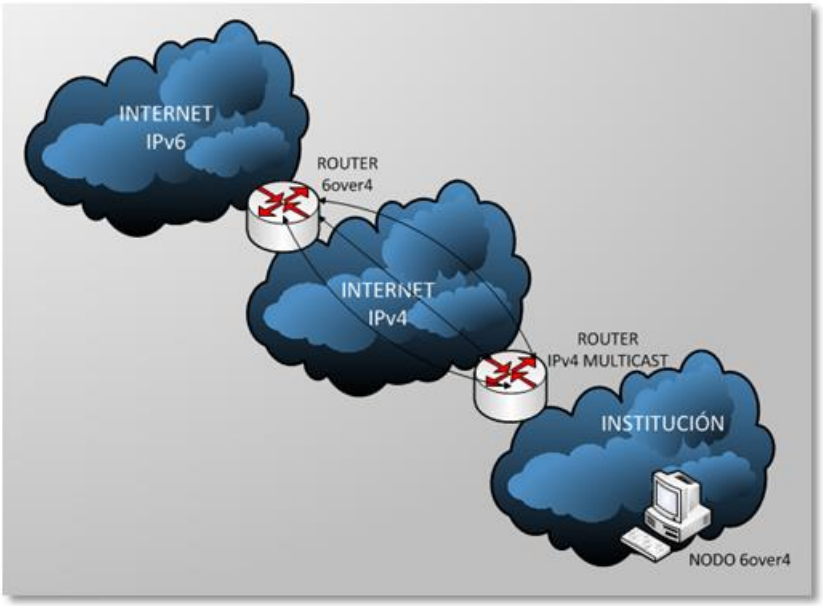


Figura 20. Mecanismo de transición 6over4.
Fuente: Propia

Los paquetes que se transmiten con 6over4 hacen uso de tipo protocolo 41 en los paquetes IPv4 que contienen la cabecera IPv6 seguido de los datos. La encapsulación de paquetes IPv6 en paquetes IPv4 es basada en la compatibilidad de direcciones IPv4, de esta manera se encapsula automáticamente.

"Cuando un sitio quiere acceder a IPv6 con este mecanismo de transición requiere de la configuración de 6over4 en el router y este a su vez tendrá una interfaz para IPv4 y otra para IPv6" (www.ietf.org/rfc2529, Feb 2012). Se puede aplicar configuración de túneles de host a host, host a router y router a host. Tiene como desventaja su uso especifico para redes multicast que ha hecho de este mecanismo no posea gran éxito.

3.3.3. TEREDO

Teredo establece comunicación IPv6 sobre UDP[23], es un mecanismo de transición que proporciona conexión IPv6 a nodos ubicados detrás de NAT. Posee un rango con su respectivo prefijo para hosts 2001:0000::/32 de direcciones IPv6 utilizadas en el encapsulamiento.

En Teredo se definen algunos elementos que intervienen en la conectividad:

- Servicio Teredo: Es la transmisión de paquetes IPv6 sobre UDP.
- Cliente Teredo: Un nodo con acceso a Internet IPv4 y solicita acceso a Internet con IPv6.

[23] UDP: User Datagram Protocol – Protocolo de Datagrama de Usuario

- Servidor Teredo: Un nodo con acceso a la red mundial con IPv4 y brinda conectividad IPv6 a sus clientes.

- Relay Teredo: Un router que recibe tráfico hacia clientes Teredo, bajo el servicio Teredo.

El puerto UDP-Teredo 3544 es el puerto donde llegan los paquetes transmitidos con este mecanismo de transición. Teredo transporta los paquetes IPv6 dentro de datagramas UDP sobre IPv4 para el envío hacia Internet atravesando NAT

"Teredo permite envío y recepción de tráfico IPv6 a través de NAT, los nodos que requieran conectarse a la Internet IPv6 deben utilizar el servicio de Teredo como último recurso, ya que es preferible usar directamente IPv6 en conectividad a enlaces locales" (www.ietf.org/rfc4380, Feb 2012).

La lista de servidores Teredo a nivel mundial se encuentra en el siguiente enlace de Internet http://www.ipv6day.org/action.php?n=En.GetConnected-Teredo, Figura 21.

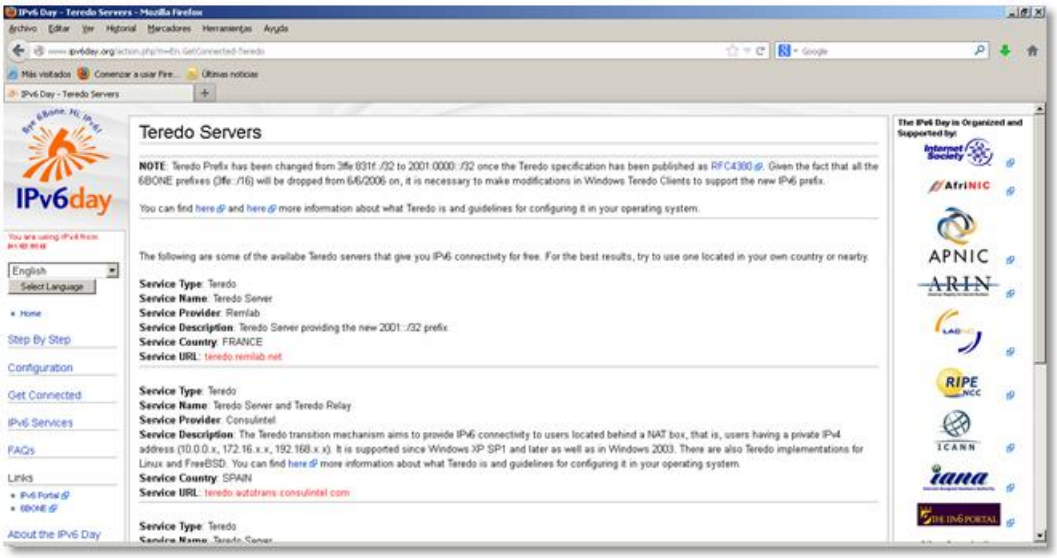


Figura 21. Sitio web de servidores Teredo.

Fuente: Propia

Un cliente Teredo detrás de un NAT que desea conectarse hacia un nodo IPv6 envía una solicitud encapsulada en UDP sobre IPv4 a un servidor Teredo que se encarga de la configuración de direcciones de sus clientes Teredo, posteriormente los paquetes encapsulados llegan a un router relay Teredo para entregar los paquetes al nodo IPv6 (Figura 22).

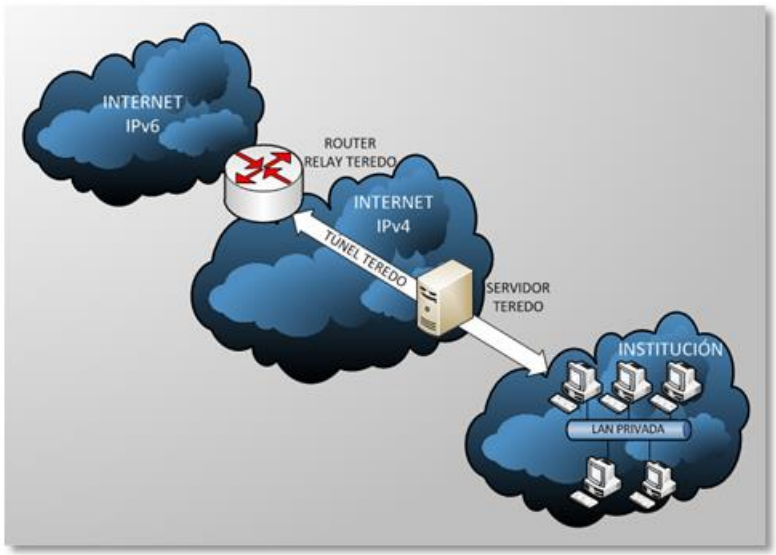


Figura 22. Mecanismo de transición Teredo.
Fuente: Propia

3.3.4. Túnel BROKER

Túnel Broker se presenta con un enfoque diferente basado en la prestación de servicios dedicados, realizando control de acceso a los usuarios, control de políticas de aplicación y la utilización de recursos de red. Una de las características que posee túnel Broker es que se adapta fácilmente a pequeños sitios IPv6 aislados, también se conoce como túnel de corredores.

En túnel Broker existen túneles intermediarios que proporcionan conectividad IPv6 a usuarios conectados a Internet IPv4, de los cuales existe una lista para que el usuario elija uno de ellos de acuerdo a cercanía, costo y beneficios.

“Para acceder a un túnel Broker el usuario debe conectarse para registrarse y activar el túnel, el túnel Broker se encarga del registro del usuario, gestionando la creación, modificación y eliminación del usuario” (www.ietf.org/rfc3035, Feb 2012). Para tener conectividad hacia IPv6 interviene un servidor de túnel Broker, cuya función recibir órdenes del túnel Broker para gestionar el lado del servidor de cada túnel. La comunicación entre el túnel Broker y servidor pueden ser bajo IPv4 o IPv6.

Un cliente túnel Broker posee doble pila conectado a la Internet IPv4, el cliente en el momento de solicitar conexión es autenticado indicando su identidad, credenciales para permitir acceso controlado. El cliente debe proporcionar información como por ejemplo su dirección IPv4.

La activación de este tipo de túnel ocasiona que se consuman memoria y tiempo de procesamiento, por esta razón se aconseja mantener al mínimo los

túneles sin utilizarlos. El mecanismo de transición túnel Broker es de fácil implementación orientado a que no se requiere ningún software adicional en la máquina cliente.

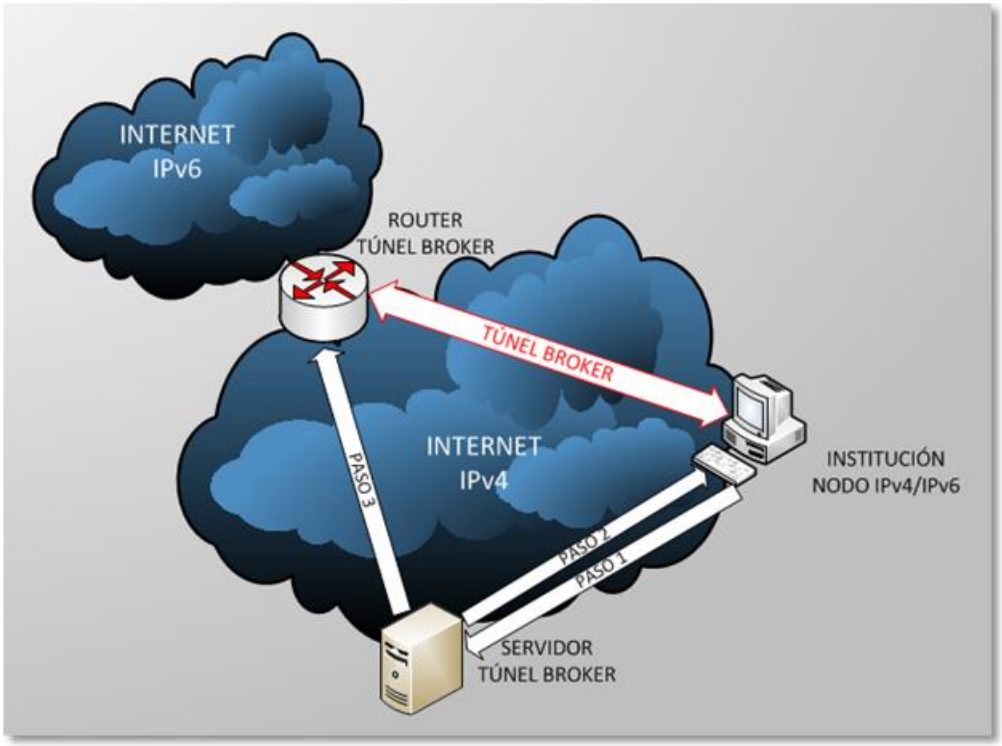


Figura 23. Mecanismo de transición Túnel Broker.

Fuente: Propia

Mecanismo de transición túnel Broker funciona de la siguiente manera el cliente realiza una petición al servidor túnel Broker (Paso 1 de la Figura 23), se establece autentificación y el servidor responde proporcionando información para configurar el túnel (Paso 2 de la Figura 23), el servidor también se encarga de configurar el extremo del túnel Broker (Paso 3 de la Figura 23), el cliente también configura el otro extremo del túnel para comenzar la comunicación.

Desventaja, túnel Broker posee complicaciones en su funcionamiento cuando el usuario usa direcciones IPv4 privadas y están detrás de NAT.

3.3.5. DSTM

DSTM Dual Stack Transition Mechanism, es un mecanismo que consiste en transportar paquetes IPv4 sobre túneles dentro de una red IPv6, llevando tráfico IPv4 dentro de la red IPv6. Contiene un método para asignar direcciones IPv4 para uso temporal. La característica principal de este mecanismo es el manejo dominante de IPv6 en la red acompañado de direcciones IPv4 temporales.

El objetivo de DSTM es proporcionar a los nodos IPv6 un medio para adquirir una dirección para las comunicaciones con nodos solo IPv4 o aplicaciones IPv4, asegurando de esta manera la comunicación entre aplicaciones IPv4 en redes que son solo IPv6 y el resto de Internet.

DSTM esta orientado a empresas o instituciones que poseen un escenario donde domine IPv6 y para aplicaciones específicas requieren necesariamente el uso de IPv4, para lo cual los ordenadores poseen doble pila con direcciones temporales IPv4.

"Una arquitectura DSTM esta compuesta de un servidor de direcciones DSTM, clientes DSTM y una puerta de enlace router DSTM conocida también como TEP[24]" (tools.ietf.org/html/draft-bound-dstm-exp-, Mar 2012).

[24] TEP: Punto Final del Túnel

En el escenario DSTM el cliente quiere enviar un paquete hacia Internet IPv4 solicita al servidor DSTM una dirección IPv4 para un determinado tiempo (Paso 1 de la Figura 24), cuya función del servidor es gestionar la creación del túnel indicando la dirección IPv4 asignada (Paso 2 de la Figura 24), controla a la puerta de enlace agregando un TEP de acuerdo a la petición del cliente DSTM encapsula paquetes IPv4 en cabeceras IPv6 de la red local, actuando como un túnel 4over6. El router de borde DSTM desencapsula el paquete IPv4 para ser transmitido hacia su destino ya sea aplicación o cliente.

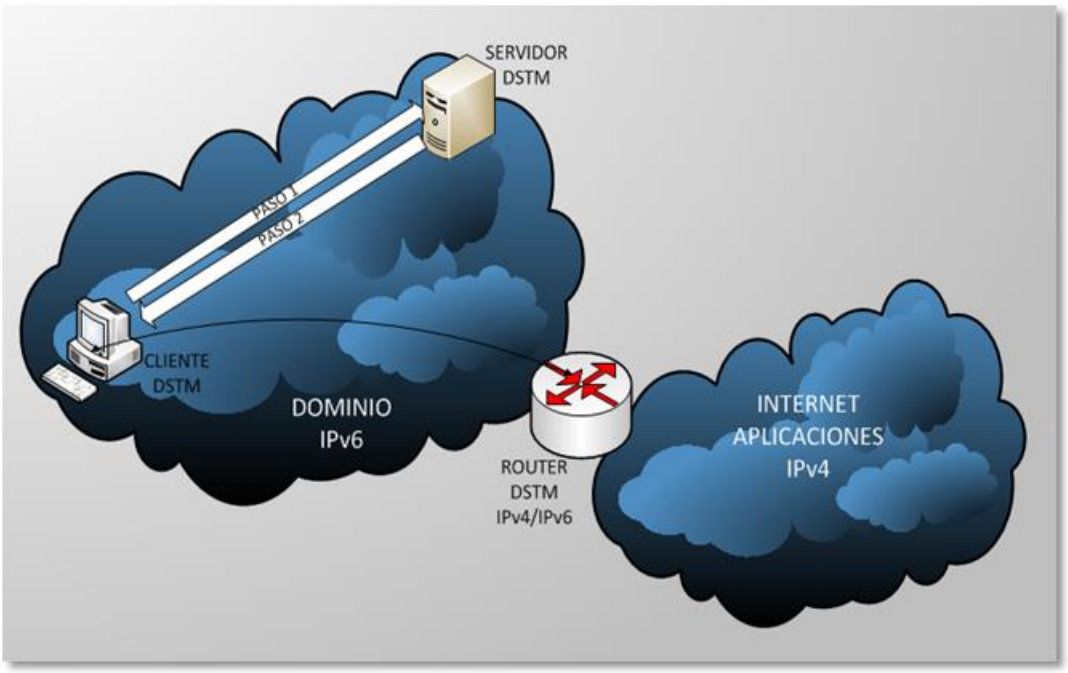


Figura 24. Mecanismo de transición DSTM.

Fuente: Propia

El funcionamiento del servidor DSTM se encuentra en actividad cuando se requiere de conectividad hacia Internet y/o aplicaciones IPv4, la asignación de dirección temporal IPv4 puede prolongarse hasta llegar a ser permanente reduciendo la gestión por parte del servidor.

En la red DSTM donde domina IPv6 se encuentra habilitado enrutamiento IPv6 para que todos los nodos dentro de ese dominio sean capaces de comunicarse. Una ventaja de este tipo de mecanismo es la transparencia para las aplicaciones que manejan IPv4 donde toda la red es IPv6.

3.4. TRADUCCIÓN

En esta técnica se lleva a cabo bajo la traducción de cabeceras IPv4 en cabeceras IPv6 y viceversa. Posee similitud a la técnica NAT, convirtiendo totalmente la cabecera.

Cuando un nodo IPv6 se encuentra detrás de un traductor posee completa funcionalidad cuando habla con otro nodo IPv6. Cuando nodos IPv4 quieren comunicarse poseen funcionalidad normal de NAT.

El mecanismo de traducción puede clasificarse dependiendo del nivel de la capa donde se produce la misma:

- Capa de red: La traducción se realiza en las cabeceras IPv4 e IPv6, basadas en la traducción de las reglas de SIIT (Staleless IP/ICMP Translation Mechanism), se caracterizan por resolver problemas de fragmentación los ejemplos que se derivan de esta traducción son SIIT, NAT-PT, BIS.
- Capa transporte: La traducción se realiza a nivel de transporte (Transport Relay). Cuando se traduce a nivel de transporte actúan como

intermediarios de conexiones TCP/IPv4 <=> TCP/IPv6 o conexiones UDP/IPv4 <=> UDP/IPv6, TRT [25] y SOCKS64 son ejemplos de traducción Transport Relay.

- Capa aplicación: La traducción se realiza a nivel de aplicación (Application Layer Gateway - ALG), los ejemplos son SOCKS 64 y BIA[26].

Los mecanismos de transición basados en traducción que se especifican a continuación son a nivel capa de red:

- SIIT
- NAT-PT
- BIS

3.4.1. SIIT

SIIT Stateless IP/ICMP Translation Mechanism, mecanismo de transición sin estado (véase capítulo dos, autoconfiguración stateles) que traduce cabeceras IPv4 e IPv6 además de traducir paquetes ICMPv4 e ICMPv6 y viceversa por separado para que exista comunicación entre nodos.

Generalmente los traductores de protocolo deben formar parte de la topología en nodos sólo IPv6, nodos sólo IPv4 o nodos duales. También debe existir un traductor para cada nube o sitio utilizado por los paquetes traducidos

[25] TRT: Trasport Relay Trasnlator
[26] BIA: Bump in the API

que ingresan o salen de la nube, asegurando que todos los paquetes que atraviesan el traductor en la nube siempre se traduzcan.

Cuando un nodo sólo IPv6 quiere comunicarse con un nodo IPv4 utilizando un traductor, éste verá como una dirección IPv4 mapeada (tiene la forma ::FFFF:a.b.c.d) y hace uso de una dirección IPv4 traducible de su dirección local para que exista comunicación, de esta manera con la dirección IPv4 mapeada por parte del nodo IPv6 el traductor sabe que tiene que traducir el paquete.

Los nodos que funcionan a través de un traductor necesitan determinar la dirección IPv4-traducible y esta a su vez debe ser actualizada constantemente para su determinado uso.

Las operaciones del traductor y la ruta del descubrimiento del MTU funcionan independientes para cada paquete y no retiene ningún estado de un paquete a otro, dando lugar a que los paquetes pueden pasar por diferentes traductores (redundancia). Adicionalmente el uso de traductores requiere de un nivel más alto de lógica en la capa de red.

“Utiliza una dirección IPv4-mapeada en IPv6, en el formato ::FFFF:a.b.c.d, que identifica el destino IPv4, y una dirección IPv4-traducida, en el formato ::FFFF:0:a.b.c.d, para identificar el nodo IPv6” (tools.ietf.org/html/rfc2765, May 2012).

3.4.1.1. Traducción de cabecera IPv4 a cabecera IPv6

La traducción de un paquete IPv4 a IPv6 inicia cuando el traductor recibe el paquete IPv4 traduce su cabecera a una cabecera IPv6, dando lugar a la eliminación de la cabecera IPv4 y remplazo por la cabecera IPv6.

IPv6 hace uso obligatorio de Path MTU Discovery [27] y en IPv4 es opcional, dando lugar a que los routers IPv6 no van a fragmentar un paquete a excepción del remitente.

Si el nodo IPv4 con el campo DF establecido opera con Path MTU Discovery puede trabajar de extremo a extremo a través del traductor al igual que los mensajes ICMP, cuando existen mensajes de error ICMP enviados de regreso por un router IPv6 son enviados por medio del traductor y este traduce de tal manera que sea entendido por el remitente.

Los campos de la cabecera IPv4 se traducen a cabecera IPv6 como indica la Tabla 18:

Tabla 18

Traducción de cabecera IPv4 a cabecera IPv6

CAMPO	ASIGNACIÓN
Versión	6
Clase de tráfico	Campo Tipo de servicio (TOS) de IPv4
Etiqueta de flujo	Todos los bits a cero
Tamaño de datos	Campo Longitud total menos naño de la cabecera IPv4
Siguiente cabecera	Campo Protocolo IPv4
Límite de saltos	Campo Tiempo de vida (TTL) IPv4 crementado en 1

[27] Path MTU Discovery busca garantizar que el paquete encaminado sea del mayor tamaño posible.

CAMPO	ASIGNACIÓN
Dirección origen	Tiene la forma ::FFFF:0:0/96 nde los 32 bits de la derecha rtenecen a la dirección IPv4 de gen
Dirección destino	Tiene la forma ::FFFF:0:0:0/96 nde los 32 bits de la derecha rtenecen a la dirección IPv4 de stino

Fuente: http://tools.ietf.org/html/rfc2765

3.4.1.2. Traducción de cabecera IPv6 a cabecera IPv4

Cuando el traductor recibe un paquete IPv6 dirigido a una dirección IPv4 mapeada, realiza la traducción de cabecera IPv6 a cabecera IPv4, posteriormente se envía el paquete hacia la dirección destino IPv4. La cabecera del paquete IPv6 es removida para ser remplazada por la cabecera IPv4.

En IPv6 el MTU es de 1500 bytes y en IPv4 el MTU es de 680 bytes, dando lugar a que una comunicación de IPv6 a IPv4 no sea posible realizarla de extremo a extremo. Existe una medida para reducir el MTU desde los routers IPv6 cuando los paquetes son muy grandes, se incluye un fragmento de cabecera IPv6 para cada paquete permitiendo el descubrimiento del MTU a través del traductor. Cuando los paquetes enviados por routers IPv6 poseen un valor inferior de 1280 bytes no requieren de cabeceras adicionales pudiendo atravesar los traductores para luego ser fragmentados por los routers IPv4.

Los campos de la cabecera IPv6 se traducen a cabecera IPv4 como indica la Tabla 19, referente a las opciones de cabecera IPv6 no requieren de traducción.

Tabla 19

Traducción de cabecera IPv6 a cabecera IPv4

CAMPO	ASIGNACIÓN
Versión	4
Longitud de la cabecera (IHL)	5
Tipo de servicio	Campo Clase de tráfico de IPv6
Longitud total	Valor de longitud de carga útil IPv6 más tamaño de cabecera IPv4
Identificación	0
Señalizador (banderas)	DF=1, MF=0
Desplazamiento del fragmento	0
Tiempo de vida (TTL)	Campo Límite de saltos IPv6 decrementado 1
Protocolo	IPv6 Siguiente Cabecera
Suma de verificación de la cabecera	Se calcula suma de verificación de la cabecera IPv4
Dirección origen	Si la dirección IPv6 de origen es una dirección de tipo IPv4-traducida se copia a la dirección IPv4 de origen
Dirección destino	Los paquetes traducidos IPv6 poseen una dirección IPv4-mapeada

Fuente: http://tools.ietf.org/html/rfc2765

Pueden existir escenarios donde se aplica SIIT para redes pequeñas y establecer comunicación a una sola subred IPv6 (Figura 25) o usar SIIT para comunicarse con hosts IPv6 a través de una red dual hacia hosts IPv4 (Figura 26).

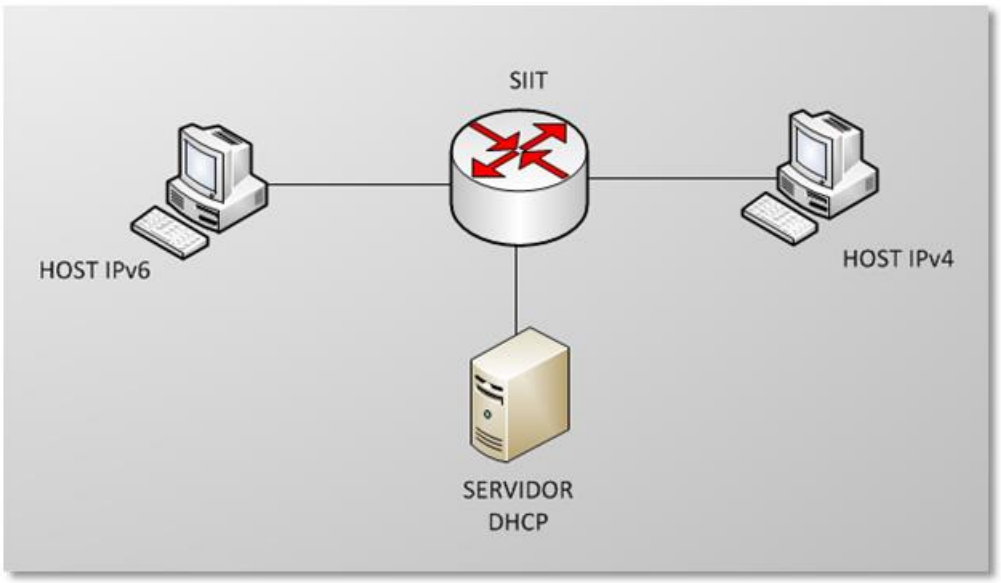


Figura 25. SIIT en redes pequeñas.

Fuente: http://tools.ietf.org/html/rfc2765

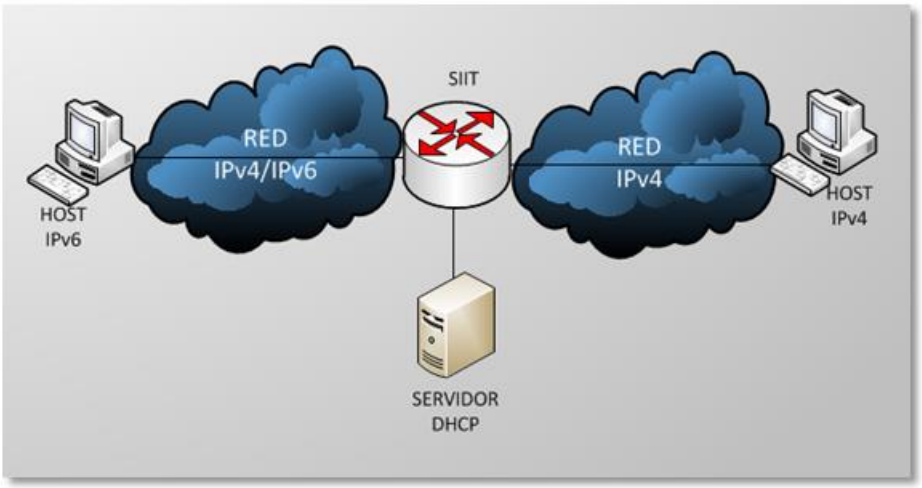


Figura 26. SIIT en redes grandes.

Fuente: http://tools.ietf.org/html/rfc2765

La traducción utilizada en SIIT especifica que no es posible aplicar seguridad de extremo a extremo IPSec, AH se ve afectada a través del traductor a diferencia de ESP que si se puede traducir.

3.4.2. NAT-PT

En base al RFC 2766 el mecanismo de traducción NAT-PT (Network Address Trasnlation – Protocol Translation / Traducción de Direcciones de Red – Protocolo de Traducción) se encuentra fundamentado en el NAT tradicional que es la traducción de direcciones públicas a privadas o viceversa, NAT-PT realiza traducción de direcciones y protocolo basado en la traducción de SIIT (comunica a hosts sólo IPv4 con hosts sólo IPv6). Proporciona una solución combinada con SITT para traducir cabeceras y NAT referente a traducir direcciones IPv4 a IPv6 y viceversa (usando los principios de NAT en IPv4). NAT-PT utiliza un conjunto de direcciones de sesión localizadas en una base de datos dinámica. NAT-PT posee variaciones tradicional NAT-PT y NAPT-PT.

3.4.2.1. Tradicional NAT-PT

Permite a los hosts IPv4 dentro de la red acceder a la red IPv6 unidireccionalmente. De igual manera se incluyen variaciones NAT-PT básico y NAPT-PT (Network Address Port Translation – Protocol Translation).

- NAT-PT básico: En esta traducción se determina un bloque de direcciones IPv4 utilizadas para la traducción a direcciones IPv6.

  Cuando nodos en diferentes dominios (IPv4 o IPv6) quieren comunicarse, el nodo IPv4 crea dirección de origen y destino IPv6 con un prefijo ::/96 siendo un identificativo para que los paquetes se direccionen hacia NAT-PT que contiene un servidor DHCP (Figura 27).

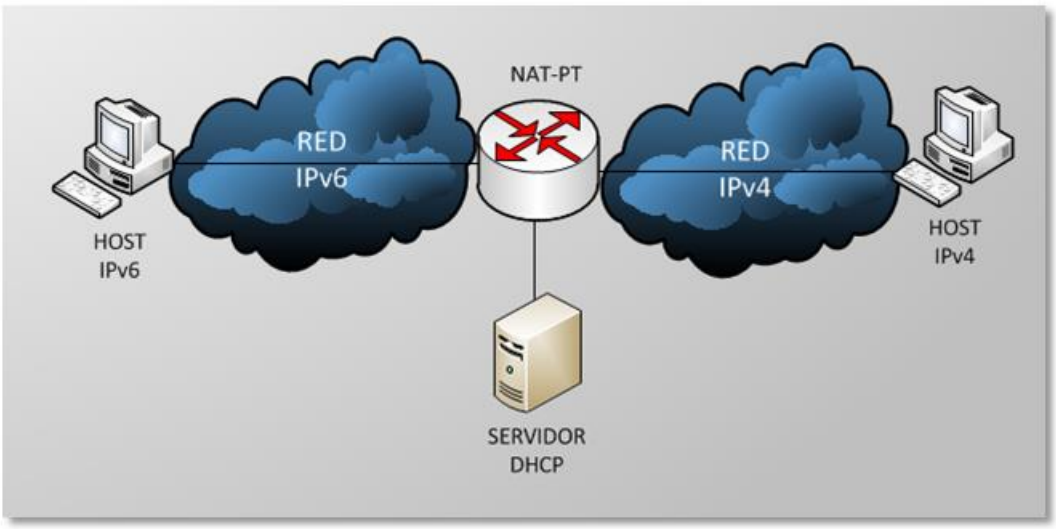


Figura 27. NAT-PT básico.

Fuente: http://www.ietf.org/rfc/rfc2766.txt

- NAPT-PT: Hace uso de la traducción a capa superior donde se realiza traducción de TCP, UDP y puertos. Se permite la combinación entre NAT-PT básico y NAPT-PT.

  Su funcionamiento es permitir comunicación a nodos IPv6 con nodos IPv4, con NAPT-PT los puertos TCP/UDP del paquete IPv6 se convierten en los puertos TCP/UDP del paquete IPv4.

3.4.2.2. NAT-PT Bidireccional

Se traduce las direcciones bidireccionalmente al ingresar o salir los paquetes dentro de un dominio, NAT-PT bidireccional trabaja en conjunto con un DNS-ALG [28] para suministrar fácilmente el mapeo entre nombres y direcciones. La finalidad de DNS-ALG es proporcionar sesiones de entrada o salida en los dominios IPv4 e IPv6.

[28] DNS-ALG transforma peticiones DNS “A” a peticiones “AAAA”

3.4.2.3. Protocolo de Traducción

PT traduce las cabeceras IPv4 a IPv6 y cabeceras ICMP a ICMPv6 y viceversa respectivamente para que exista comunicación de extremo a extremo. La traducción de cabeceras se basa en SIIT con algunas observaciones para los campos de dirección origen y dirección destino como indica la Tabla 20 y la Tabla 21.

Tabla 20

Campos traducidos de IPv4 a IPv6

CAMPO	ASIGNACIÓN
Dirección origen	Los 32 bits de la derecha es dirección IPv4, los 96 bits restantes es el identificativo de NAT-PT (prefijo::/96)
Dirección destino	La dirección IPv4 destino se remplaza por una dirección IPv6, seleccionada entre mapeo de direcciones.

Fuente: http://www.ietf.org/rfc/rfc2766.txt

Tabla 21

Campos traducidos de IPv6 a IPv4

CAMPO	ASIGNACIÓN
Dirección origen	La dirección IPv4 origen se remplaza por una dirección IPv6, seleccionada entre mapeo de direcciones.
Dirección destino	La dirección destino traducida posee el prefijo::IPv4/96 incluyendo la dirección IPv4 destino.

Fuente: http://www.ietf.org/rfc/rfc2766.txt

3.4.3. BIS

Orientado a brindar conectividad a hosts IPv6 utilizando aplicaciones IPv4 existentes, tomando en cuenta que hay muy pocas aplicaciones desarrolladas para IPv6.

"BIS (Bump in the Stack) mecanismo de transición que realiza traducción de la pila IPv4. BIS intercepta los paquetes al salir del nivel IP de la máquina, antes de enviarlos a la tarjeta de red, y realiza la traducción entre IPv4 e IPv6 según los paquetes sean entrantes o salientes" (tools.ietf.org/html/rfc2767, Mar 2012).

Traducción de IPv4 a IPv6 y viceversa basado en la traducción definido en SIIT. El traductor funciona cuando se reciben paquetes de aplicaciones IPv4, convierte la cabecera IPv4 en cabecera IPv6 posteriormente se realiza la fragmentación de paquetes IPv6 debido a su mayor extensión para ser enviadas a las redes IPv6.

El paquete IPv4 llega al traductor y éste hace uso del mapeo de direcciones para traducir la dirección origen y destino, comprueba su tabla de mapeo para encontrar de acuerdo a la llegada su respectiva dirección origen y destino IPv6.

Se requiere una actualización de pila del protocolo IPv4, si un host quiere comunicarse usando BIS debe incorporar tres módulos a la pila IPv4. Los módulos de BIS se describen a continuación (Figura 28):

- Traductor: Su función es traducir cabeceras IPv4 a IPv6 y viceversa usando el mecanismo de conversión de SIIT.

- Extensión de resolución de nombres: Puede asignar direcciones IPv6 a un solo host IPv4, la asignación es únicamente para el host que ha solicitado la dirección en el otro extremo de la comunicación.

- Asignación de dirección: Para asignar una dirección posee un rango de direcciones IPv4, también mantiene un conjunto de pares de direcciones IPv4 e IPv6 en una tabla dinámica, para cuando recibe un paquete IPv6.

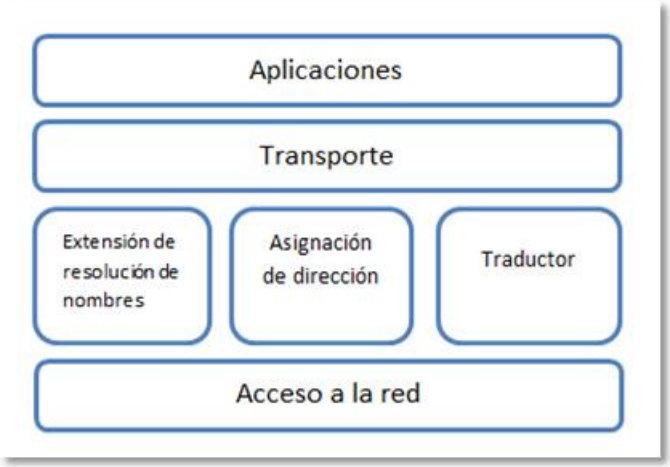


Figura 28. Módulos en BIS.

Fuente: http://tools.ietf.org/html/rfc2767

BIS es usado en situaciones donde se necesita comunicación con hosts IPv6 utilizando recursos existentes como aplicaciones IPv4 obteniendo como resultado conectividad IPv6 para el actual protocolo sin necesidad de que proporcione aplicaciones IPv6.

En RFC 2767 mencionan los inconvenientes que tiene BIS:

- Requiere del cambio de pila en los hosts agregando tres módulos.

- Sirve solo para comunicaciones unicast.

- Su forma de comunicación puede no ser tan efectiva ya que resulta casi imposible traducir las opciones de IPv4 en IPv6.

3.5. MECANISMO DE TRANSICIÓN SELECCIONADO EN UTN

Al finalizar la descripción de las categorías de mecanismos de transición en el cual se describe su proceso, características, ventajas y desventajas, se observa que el mecanismo de transición doble pila o dual stack que sobresale por las siguientes razones:

- La Universidad Técnica del Norte posee un rango IPv6 asignado de CEDIA a su proveedor de servicios de Internet (TELCONET), razón por la cual no requiere la configuración de túneles para llegar a Internet versión 6.

- Usar doble pila o dula stack genera una ventaja hacia un futuro cercano, gracias a la administración conjunta de ambos protocolos de Internet.

- Se descarta utilizar traducción por su complejidad al traducir cabeceras IPv4 en cabeceras IPv6 y viceversa.

- DSTM al ser un mecanismo de transición relativamente nuevo y poseer características atractivas, tiene como desventaja el uso exclusivo de direcciones IPv4 públicas para navegar.

- El uso de túneles provoca retardo en la transmisión de datos en una red, dando lugar a que este mecanismo de transición sea descartado.

- Respecto a seguridad no se puede brindar seguridad por encima de la capa de red cuando se comunican a capa aplicación de IPv6 con hosts IPv4 y viceversa.

En la Tabla 22 muestra en resumen cada uno de los mecanismos de transición referente a retardo, seguridad y configuración en routers; de la información visualizada se concluye que independientemente cualquier mecanismo de transición utiliza en su configuración de routers Dual Stack y además posee menor retardo y podemos aplicar seguridad al ser un protocolo independiente.

Tabla 22

Comparación de mecanismos de transición

Mecanismo de Transición	Retardo	Seguridad	Configuración en routers
Dual Stack	Protocolo Independiente	Protocolo Independiente	Dual Stack
Túnel 6to4	Encapsulación	Riesgo	Dual Stack
Túnel Teredo	Encapsulación	Riesgo	Dual Stack
Túnel Broker	Encapsulación	Riesgo	Dual Stack
DSTM	Protocolo dependiente	Protocolo dependiente	Dual Stack
Traducción SIIT	Traducción	Riesgo	Dual Stack
Traducción NAT-PT	Traducción	Riesgo	Dual Stack
Traducción BIS	Traducción	Riesgo	Dual Stack

CAPÍTULO 4

DIAGNÓSTICO ACTUAL DE LA TOPOLOGÍA DE RED DE LA UNIVERSIDAD

El capítulo cuatro describe la topología de red de datos de la Universidad Técnica del Norte, principalmente con el cuarto de equipos situado en el edificio central de la institución y su conexión con las facultades que la conforman. Una vez recolectada la información, se procede a habilitar IPv6 en la red de datos en equipos seleccionados en base a al soporte de IPv6 que posee cada equipo.

4.1. INTRODUCCIÓN

La Universidad Técnica del Norte desde sus inicios siempre ha luchado por alcanzar grandes logros en ámbitos educativos, tecnológicos y sociales, donde es parte fundamental el talento humano que se desarrolla dentro y fuera de la institución.

El trabajo conjunto de cada sección, departamento y facultad se ve reflejado en el avance diario que tiene la institución. El Departamento de Informática no es la excepción, ya que con el uso de nuevas tecnologías acompañado de personal capacitado (profesionales y tesistas) se fusiona para obtener excelentes resultados.

4.2. RED DE DATOS UTN

La red de datos de la Universidad Técnica del Norte se encuentra administrada por el Departamento de Informática situado en la planta baja del Edificio Central de la institución, al interior del Departamento de Informática se encuentra el cuarto frio o cuarto de equipos (Figura 29).

La red de datos UTN se basa en topología híbrida estrella-malla con tecnología Gigabit Ethernet y Fast Ethernet que conecta a todas las facultades y edificios del campus universitario, existe redundancia para capa distribución con la Facultad de Ingeniería en Ciencias Aplicadas (FICA) por medio del quipo de red Catalyst 4506, la red trabaja sobre medio de transmisión guiado fibra óptica multimodo en conexión a la FICA, para los demás edificios como Facultad de Ingeniería en Ciencias Agropecuarias y Ambientales (FICAYA), Facultad de Educación, Ciencia y Tecnología (FECYT), Facultad de ciencias de la salud (FF.CC.SS), Facultad de Ciencias Administrativas y Económicas (FACAE) que se encuentran dentro del campus universitario poseen conexión sobre medio de transmisión guiado multimodo (Tabla 23, Figura 30, Apéndice D), para lugares fuera del campus universitario como: Granja Experimental La Pradera, Granja Experimental Yuyucocha, Colegio Universitario y antiguo Hospital San Vicente de Paúl se enlaza usando medio de transmisión no guiado con radioenlaces con una frecuencia de 2.4 GHZ (Tabla 24).

Tabla 23

Conexiones Edificio Central y Dependencias Internas

Origen	Medio de Transmisión	Velocidad	Destino
Edificio Central	Fibra Óptica 12 hilos	1 Gbps	FICA
Edificio Central	Fibra Óptica 6 hilos	1 Gbps	FICAYA
Edificio Central	Fibra Óptica 6 hilos	1 Gbps	FECYT
Edificio Central	Fibra Óptica 6 hilos	1 Gbps	FACAE
Edificio Central	Fibra Óptica 6 hilos	1 Gbps	FF.SS.CC
Edificio Central	Fibra Óptica 6 hilos	1 Gbps	POSTGRADO
Edificio Central	Fibra Óptica 6 hilos	1 Gbps	BIBLIOTECA
Edificio Central	Fibra Óptica 6 hilos	1 Gbps	AUDITORIO

Tabla 24

Conexiones Edificio Central y Dependencias Externas

Origen	Medio de Transmisión	Velocidad	Destino
Edificio Central	Radio Enlace	20 Mbps	Granja La Pradera
Edificio Central	Radio Enlace	20 Mbps	Granja Yuyucocha
Edificio Central	Radio Enlace	20 Mbps	Colegio Universitario
Edificio Central	Radio Enlace	20 Mbps	Antiguo Hospital S.V.P

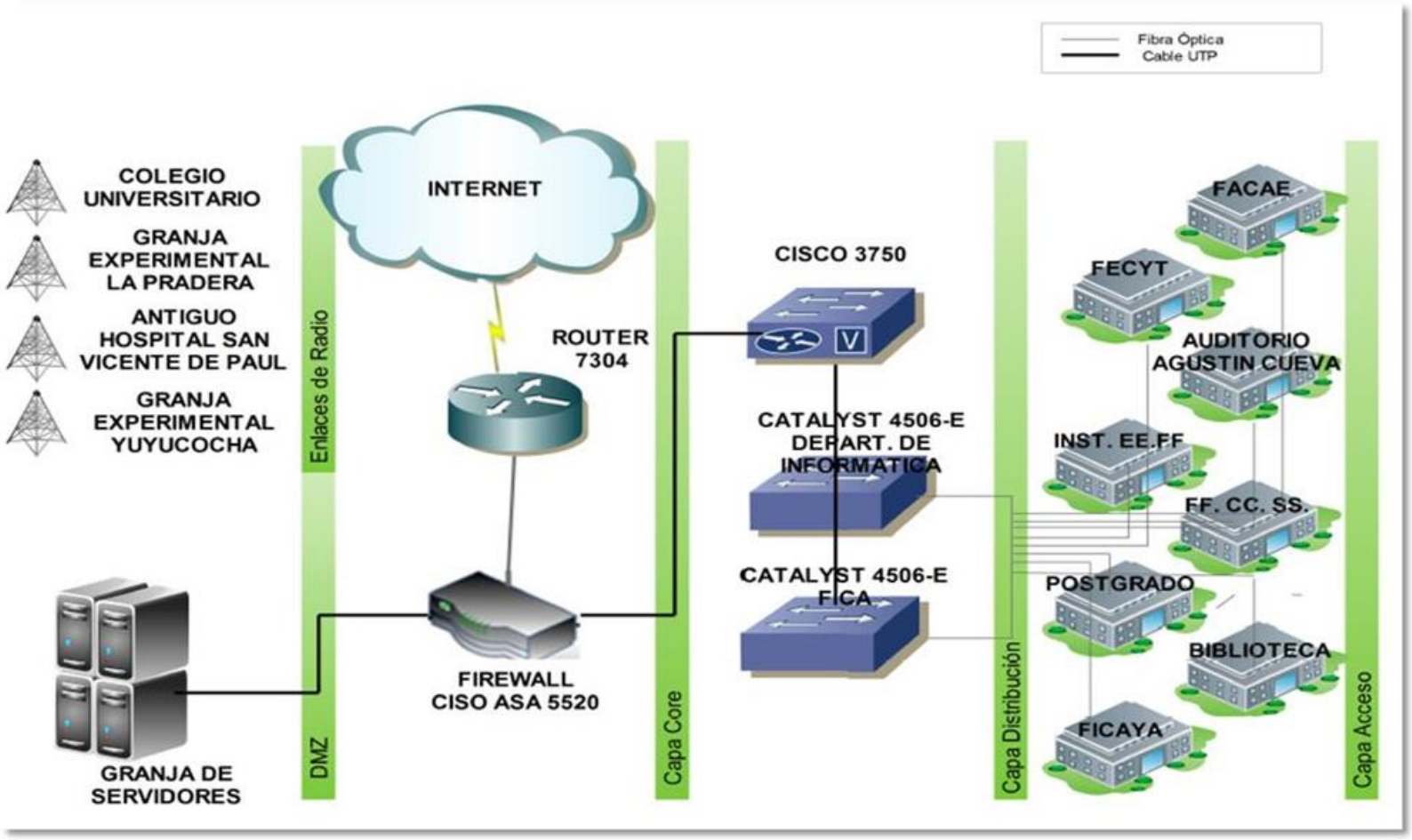


Figura 29. Red de datos UTN

Fuente: Propia

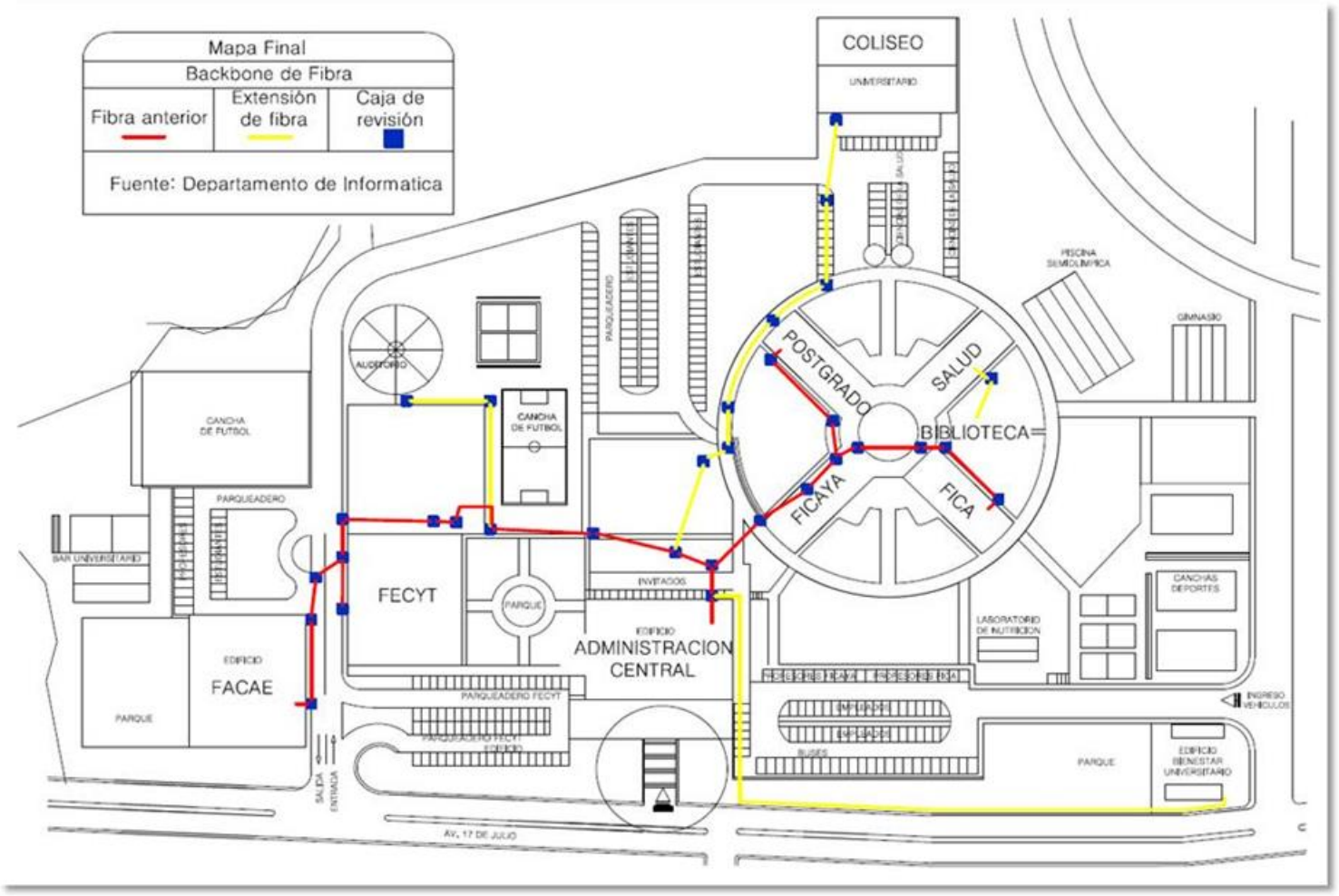


Figura 30. Backbone de Fibra Óptica UTN

Fuente: Departamento de Informática UTN

Dentro de cada edificio que conforma la Universidad Técnica del Norte existe cableado estructurado bajo la norma EIA/TIA 568B el nuevo cableado y para el cableado antiguo bajo la norma EIA/TIA 568A, usando cable UTP categoría 6 y categoría 5 respectivamente.

Para el acceso a Internet inalámbrico la institución posee un equipo Wireless LAN Controller CISCO 5500 aplicando un sistema de radio (AIRONET) situados en lugares estratégicos para cubrir a todo el campus universitario (Figura 31).

Figura 31. Red inalámbrica UTN

Fuente: Departamento de Informática UTN

Para mayor visibilidad el sistema de radio para acceso inalámbrico se encuentra de color rojo en la Figura 31.

4.2.1. CUARTO DE EQUIPOS

El cuarto de equipos de la institución se encuentra estructurado de varios equipos de red como indica la Figura 29 en la capa de core y capa de distribución. Cada elemento de la red de datos de la institución cumple una función específica, trabajando normalmente bajo el protocolo de Internet versión 4.

Firewall CISCO ASA 5520 que forma parte de la red de datos UTN, se encuentra conformado por tres interfaces conectadas hacia Router 7304, DMZ y Packet Shape 3500, este equipo se encarga de la seguridad interna de la red evitan\do acceso a personas no deseadas.

Switch Cisco Catalyst 3750 equipo que se encuentra conectado a Switch Cisco Catalyst 4506-E. Catalyst 3750 permite configuración de listas de acceso (ACL, Control Access List).

En la Tabla 25 indica las versiones de los equipos de red para verificar si soporta la habilitación del nuevo protocolo de Internet versión 6.

Tabla 25

Soporte de IPv6 en elementos de red de datos en UTN

CAPA	EQUIPO DE RED	VERSIÓN	SOPORTE IPv6
Capa de core	Router 7604	IOS 12.2	Si
	Firewall 5520	IOS 8.2	Si
	Switch 3750	IOS 12.2	Si
Capa de distribución	Switch 4506	IOS 12.2	Si
Capa de acceso	Estaciones de trabajo con sistema operativo Windows	Windows XP	Requiere instalación
		Windows 7	Si
		Windows Vista	Si
		Windows 8	Si
	Estaciones de trabajo con sistema operativo LINUX	Ubuntu	Kernel 9.04
		Debian	Kernel 2.2
		SuSE	Kernel 11.2
		Fedora	Kernel 2.4
		Red Hat	Kernel 2.4
	MAC	MAC	Si

Las estaciones de trabajo con sistema operativo Linux provienen de la Facultad de Ingeniería en Ciencias Aplicadas (FICA) para proyectos y trabajos eventuales.

El soporte de IPv6 que muestra en la Tabla 25 cumple con un aspecto importante para la fase inicial hacia la transición con el nuevo protocolo que es soporte del nuevo protocolo en equipos de red de la institución, dando lugar a que sea posible implementar IPv6 en UTN. En la Tabla 26 muestra la compatibilidad de IPv6 con los equipos de distribución para cada edificio dentro y fuera del campus universitario.

Tabla 26

Compatibilidad de IPv6 con equipos de distribución de red

EDIFICIO	EQUIPO DE RED	VERSIÓN IOS	SOPORTE IPv6
FICA	Switch Cisco 4506-E	12.2	Compatible con ipv6
FICAYA	Switch 3COM 4228 G	2.0	No
	Switch 3COM 4400	5.1	Actualizar software
FACAE	Switch 3COM 4400 SE	5.1	Actualizar software
	Switch 3COM 4400	5.1	Actualizar software
	Switch 3COM 5500G	3.0	Compatible con ipv6
	Switch TPLINK TL-SG2224WEB	1.2	No
LAB. FACAE	Switch Cisco WS-C2960G-48TC-L	12.2	Compatible con ipv6
SALUD	Switch 3COM 4400	5.1	Actualizar software
POSTGRADO 1er PISO	Switch LINKSYS SRW2048	1.1	No
	Switch LINKSYS SRW2024	1.3	Compatible con ipv6
POSTGRADO 3er PISO	Switch LINKSYS SRW2048	1.1	No
	Switch 3COM 4200	2.0	No
	Switch LINKSYS SRW2024	1.3	Compatible con ipv6
BIBLIOTECA	Switch 3COM 4400SE	5.1	Actualizar software
	Switch	2.5	No

EDIFICIO	EQUIPO DE RED	VERSIÓN IOS	SOPORTE IPv6
	3COM SG 300-52		
	Switch 3COM 5500 SI	3.0	Compatible con ipv6
FECYT	Switch 3COM 4400SE	5.1	Actualizar software
9ED. FÍSICA	Switch 3COM 4400SE	5.1	Actualizar software
AUDITORIO	Switch 3COM 4400SE	5.1	Actualizar software
COLEGIO UTN	Switch 3COM 4226T	2.0	No
ANTIGUO HSVP	Switch TP-LINK TL-SG2216WEB	1.2	No
TERRAZA	Switch 3COM 4400SE	5.1	Actualizar software
GRANJA YUYUCOCHA	Switch CISCO SG 300-28	2.5	No
GRANJA LA PRADERA	Switch LINKSYS SRW248G4	1.2	No

En la Tabla 26 se observa que algunos equipos de red actualmente pueden trabajar conjuntamente con el protocolo de Internet versión 6, las características de estos equipos se muestran en Apéndice E.

4.3. RED DE DATOS UTN (TOPOLOGIA LÓGICA)

La Universidad Técnica del Norte posee un pool de 32 direcciones públicas IPv4 de las cuales están siendo utilizadas 16 direcciones. La

institución posee configuración de VLANs para edificios dentro y fuera del campus universitario como indica la Tabla 27 (por motivo de seguridad no se muestra toda la dirección privada versión 4 al igual que su máscara de red).

Tabla 27

Distribución de VLANs

UBICACIÓN	VLAN ID	DESCRIPCIÓN	SUBRED	MÁSCARA DE SUBRED
EDIFICIO CENTRAL	1	Servidores	172.X.X.X	255.X.X.X
	2	Equipos activos	172.X.X.X	255.X.X.X
	4	Financiero	172.X.X.X	255.X.X.X
	6	Departamento de Informática	172.X.X.X	255.X.X.X
	7	CECI	172.X.X.X	255.X.X.X
	8	Autoridades	172.X.X.X	255.X.X.X
	10	Administrativos	172.X.X.X	255.X.X.X
	12	Comunicación Organizacional	172.X.X.X	255.X.X.X
FICA	14	Administración	172.X.X.X	255.X.X.X
	16	Laboratorios	172.X.X.X	255.X.X.X
	18	Academia Cisco	172.X.X.X	255.X.X.X
FICAYA	20	Administración	172.X.X.X	255.X.X.X
	22	Laboratorios	172.X.X.X	255.X.X.X
POSTGRADO	24	Administración	172.X.X.X	255.X.X.X
	26	Laboratorios	172.X.X.X	255.X.X.X
CENTRO ACADÉMICO DE IDIOMAS	28	Administración	172.X.X.X	255.X.X.X
	30	Estudiantes	172.X.X.X	255.X.X.X
FCCSS	32	Administración	172.X.X.X	255.X.X.X
	34	Laboratorios	172.X.X.X	255.X.X.X
BIBLIOTECA	36	Administración	172.X.X.X	255.X.X.X
	37	Estudiantes	172.X.X.X	255.X.X.X
FECYT	40	Administración	172.X.X.X	255.X.X.X
	42	Laboratorios	172.X.X.X	255.X.X.X
FACAE	44	Administración	172.X.X.X	255.X.X.X

UBICACIÓN	VLAN ID	DESCRIPCIÓN	SUBRED	MÁSCARA DE SUBRED
	46	Laboratorios	172.X.X.X	255.X.X.X
A. AGUSTÍN CUEVA	48	Auditorio	172.X.X.X	255.X.X.X
COLEGIO UTN	52	Administración	172.X.X.X	255.X.X.X
	54	Laboratorios	172.X.X.X	255.X.X.X
WIRELESS	56	Docentes	172.X.X.X	255.X.X.X
	58	Administrativos	172.X.X.X	255.X.X.X
	60	Estudiantes	172.X.X.X	255.X.X.X
EDIFICIO CENTRAL	64	Telefonía IP	172.X.X.X	255.X.X.X
COPIADORA	66	Copiadora	172.X.X.X	255.X.X.X
EDIFICIO CENTRAL	120	NAT Interno	172.X.X.X	255.X.X.X
	168	Enlace Banco-Pacífico	172.X.X.X	255.X.X.X

Fuente: Departamento de Informática Universidad Técnica del Norte

Las VLANs utilizadas para la transición a IPv6 son: VLAN 1 donde se sitúan los servidores y VLAN 6 del Departamento de Informática destinado para realizar pruebas de implementación.

4.4. DIAGNÓSTICO RED DE DATOS UTN

Con la finalidad de que la Universidad Técnica del Norte posea nuevas aplicaciones tecnológicas relacionadas a la excelencia educativa como tele-educación o aplicaciones Grid; surge la necesidad de activar IPv6 en la red de datos de la institución que sirva de plataforma en la creación y ejecución de estas y más aplicaciones.

4.4.1. ANTECEDENTES

Hasta el momento la gran mayoría de instituciones como el caso de la Universidad Técnica del Norte trabajan en su red de datos sobre IPv4, en la actualidad al conocer que se pueden mejorar aplicaciones existentes al trabajar sobre la red de datos con IPv6, da lugar a que previamente realizada una investigación se seleccione el mecanismo de transición para posteriormente configurar IPv6 en routers, switchs y para hosts solo se necesitaría activar el protocolo de Internet versión 6 gracias a la autoconfiguración de direcciones de red que posee para hosts.

En cada facultad de la UTN existen switchs para la distribución de red de los cuales no todos soportan IPv6, impidiendo la propagación de IPv6 en toda la institución, por este motivo se centra la configuración en la VLAN 6 que pertenece al Departamento de Informática del edificio central de la institución para posibles depuraciones.

4.4.2. METODOLOGÍA UTILIZADA

La metodología utilizada hacia la transición al protocolo de Internet versión 6 se basa desde el punto de vista de red y en conjunto con el mecanismo de transición seleccionado se configura siguiendo el proceso jerárquico que se encuentran los equipos en UTN (Figura 29):

a) Router 7304 (TELCONET)
b) Firewall CISCO ASA 5520
c) Siwtchs CISCO 3750

d) Host (opcional)

Para el mecanismo de transición Dual Stack donde se agrega la pila versión 6, interviene procesos similares en la configuración de equipos referente al protocolo de Internet versión 4.

4.4.3. CONFIGURACIÓN DE IPv6 EN EQUIPOS DE RED

Al verificar si los equipos de red que posee la UTN soportan IPv6, amplía la selección del mecanismo de transición al seleccionar cualquiera de las tres categorías; en el escenario contrario si los equipos de red no soportan IPv6 se limita la selección del mecanismo de transición a escoger túneles y traducción.

Al identificar el mecanismo de transición a utilizarse, es necesario iniciar la configuración en el equipo propio de UTN que es Firewall CISCO ASA 5520 que es el primer lugar donde llega la información (Internet) desde el exterior a la institución luego de que la información ha pasado por el router 7304 equipo propio de TELCONET (proveedor de servicios de Internet para UTN).

Para el caso de la Universidad Técnica del Norte se configura IPv6 en el equipo Firewall CISCO ASA 5520 y en el equipo CISCO 3750 en base al mecanismo de transición seleccionado Dual Stack, las VLANs que van trabajan con IPv6 se configuran en el equipo CISCO 3750.

CAPÍTULO 5

IMPLEMENTACIÓN IPv6

En este capítulo se realiza la configuración con el protocolo de Internet versión 6 en equipos de red del edificio central de la Universidad Técnica del Norte. Se inicia con la configuración de equipos en firewall, switch y host; se verifica la correcta configuración al observar el tráfico de paquetes bajo los protocolos IPv4 e IPv6 visualizando sus campos en cada cabecera respectiva al modelo TCP/IP y como aplicación se configura en una máquina virtual un servidor web que trabaja sobre IPv6.

5.1. INTRODUCCIÓN

Para logar el objetivo de activar IPv6 en la red de datos UTN, se realiza configuración en firewall, switch y host de la institución, los usuarios finales de la institución podrán acceder a redes IPv6 bajo los parámetros descritos capítulos tres y cuatro.

5.2. CONFIGURACIÓN DUAL STACK EN RED UTN

La configuración inicia con la activación de IPv6 en forma paralela dando lugar a que ambos protocolos se ejecuten al mismo tiempo, se utiliza el rango IPv6 proporcionado por CEDIA para UTN es 2800:68:19::/48 como indica la

Figura 32. La asignación de direcciones de puerta de enlace IPv6 para router y firewall se indica en la Tabla 28.

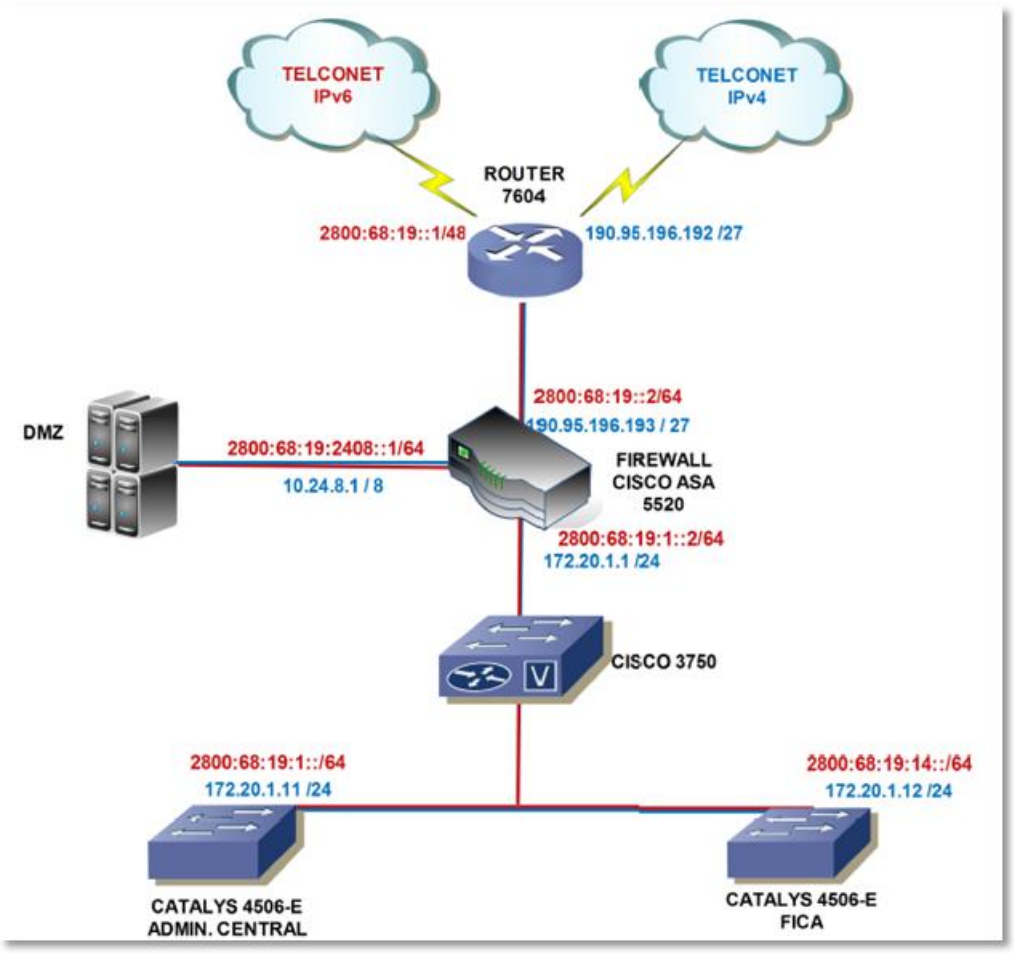


Figura 32. Red Dual Stcak UTN

Fuente: Propia

Tabla 28

Asignación de direcciones IPv4 e IPv6

EQUIPO DE RED	INTERFAZ	DIRECCIÓN IPv4	DIRECCIÓN IPv6
Router 7604		190.95.196.192 /27	2800:68:19::1/48
Firewall ASA 5520	Salida GigabitEthernet0/0	190.95.196.193 /27	2800:68:19::2/64
Firewall ASA 5520	Entrada GigabitEthernet0/1	172.20.1.1 /24	2800:68:19:1::2/64

EQUIPO DE RED	INTERFAZ	DIRECCIÓN IPv4	DIRECCIÓN IPv6
Firewall ASA 5520	DMZ GigabitEthernet0/2	10.24.8.1/8	2800:68:19:2408::2/64
Catalys 4506-E Admin. Central		172.20.1.11 /24	2800:68:19:1::/64
Catalys 4506-E FICA		172.20.1.12 /24	2800:68:19:14::/64

5.2.1. CONFIGURACIONES EN ROUTER 7604

Las configuraciones existentes en el router 7604 de la institución son realizadas por el personal técnico de TELCONET y no se tiene acceso a las mismas.

5.2.2. CONFIGURACIONES EN FIREWALL CISCO ASA 5520

La configuración de IPv6 con el mecanismo de transición dual stack en el firewall CISCO ASA 5520, se basa en la configuración de los dos protocolos de Internet y el tipo de ruteo para la configuración de ambos protocolos es ruteo estático.

El firewall de la institución se compone de tres interfaces de entrada, salida y para la DMZ[29], su configuración se muestra a continuación en la Tabla 29.

[29]DMZ: Zona desmilitarizada

Tabla 29

Configuración IPv6 en interfaces de firewall

INTERFÁZ	CONFIGURACIÓN
Salida	*firewall>enable* *ingreso a modo usuario* *firewall# configure terminal* *ingreso a modo privilegiado* *firewall(config)#interface GigabitEthernet0/0* *ingreso a interfaz de salida* *firewall(config-if)#ipv6 enable* *activación de IPv6* *firewall(config-if)#ip address 190.95.196.194 255.255.255.224* *ingreso dirección IPv4* *firewall(config-if)#ipv6 address 2800:68:19::2/64* *ingreso dirección IPv6* *firewall(confi-ifg)#exit* *salir de modo privilegiado*
Entrada	*firewall>enable* *ingreso a modo usuario* *firewall# configure terminal* *ingreso a modo privilegiado* *firewall(config)#interface GigabitEthernet0/1* *ingreso a interfaz de entrada* *firewall(config-if)#ipv6 enable* *activación de IPv6* *firewall(config-if)#ip address 172.20.1.1 255.255.255.0* *ingreso direccion IPv4* *firewall(config-if)#ipv6 address 2800:68:19:1::2/64* *ingreso dirección IPv6* *firewall(config-if)#exit* *salir*
DMZ	*firewall>enable* *ingreso a modo usuario* *firewall# configure terminal* *ingreso a modo de privilegiado* *firewall(config)#interface GigabitEthernet0/2* *ingreso a interfaz DMZ* *firewall(config-if)#ipv6 enable* *activación de IPv6* *firewall(config-if)#ip address 10.24.8.1 255.255.255.0* *ingreso direction IPv4* *firewall(config-if)#ipv6 address 2800:68:19:2408::6/64* *ingreso dirección IPv6*

INTERFÁZ	CONFIGURACIÓN
	firewall(config-if)#exit *salir*

5.2.3. CONFIGURACIONES EN SWITCH CISCO 3750

La finalidad de los switchs es la correcta distribución del tráfico hacia los usuarios finales, en el switch se centra en la configuración de VLANs y su distribución se muestra en la Tabla 27 (capítulo 4). Las VLANs activas con IPv6 hasta el momento son la VLAN 1 y VLAN 6 como indica la Tabla 30.

Tabla 30

Configuración IPv6 en VLAN 1 y VLAN 6

VLAN	CONFIGURACIÓN
VLAN 1	*SW_CORECENTRAL>enable* *ingreso a modo usuario* *SW_CORECENTRAL#configure terminal* *ingreso a modo privilegiado* *SW_CORECENTRAL(config-if)#ipv6 enable* *activación de IPv6* *SW_CORECENTRAL(config)#interface vlan 1* *ingreso a VLAN 1* *SW_CORECENTRAL(config-if)#ip address 172.20.1.11 255.255.255.0* *ingreso dirección IPv4* *SW_CORECENTRAL(config-if)#ipv6 address 2800:68:19:1::1/64* *ingreso dirección IPv6* *SW_CORECENTRAL(config)#exit* *salir*
VLAN 6	*SW_CORECENTRAL>enable* *ingreso a modo usuario* *SW_CORECENTRAL#configure terminal* *ingreso a modo privilegiado* *SW_CORECENTRAL(config-if)#ipv6 enable* *activación de IPv6* *SW_CORECENTRAL(config)#interface vlan 6* *ingreso a*

VLAN	CONFIGURACIÓN	
	VLAN 6	
	SW_CORECENTRAL(config-if)#ip address 172.20.6.2 255.255.255.0	*ingreso dirección IPv4*
	SW_CORECENTRAL(config-if)#ipv6 address 2800:68:19:6::1/64	*ingreso dirección IPv6*
	SW_CORECENTRAL(config)#exit	*salir*

Una vez realizadas las configuraciones en equipos descritas anteriormente se realizan pruebas de conectividad efectuadas en el manual de administrador (Apéndice F), al tener establecida la red en Dual Stack se analizan los paquetes de los dos protocolos.

5.3. ANALIZANDO PAQUETES IPv4 E IPv6

Para analizar paquetes IPv4 e IPv6, nos ubicamos en una máquina situada en el Departamento de Informática de la UTN que posee el direccionamiento asignado a Vlan 6, con ayuda del software Wireshark se identifica las diferencias de los paquetes IPv4 e IPv6 (al utilizar el mecanismo de transición doble pila, los paquetes IPv6 llegan totalmente independientes al protocolo IPv4). Para la verificación se seleccionó paquetes TCP en donde se presentan las siguientes características en base al modelo TCP/IP. Los paquetes IPv6 se transmiten en tramas Ethernet de acuerdo al RFC 2464.

5.3.1. PAQUETE IPv4

El análisis en Wireshark describe los valores de cada campo de las capas: acceso a la red, internet y transporte, para capa aplicación los datos se

transmiten bajos los mismos protocolos de usuario final (HTTP, DNS, FTP) que en IPv4. La dirección IPv4 que se analiza es: 69.175.21.99.

- Capa Acceso a la Red - Cabecera Ethernet: la Figura 33 muestra la captura desde el programa Wireshark en la sección Ethernet II, con la información obtenida se establece la cabecera de la capa enlace de datos como muestra la Figura 34.

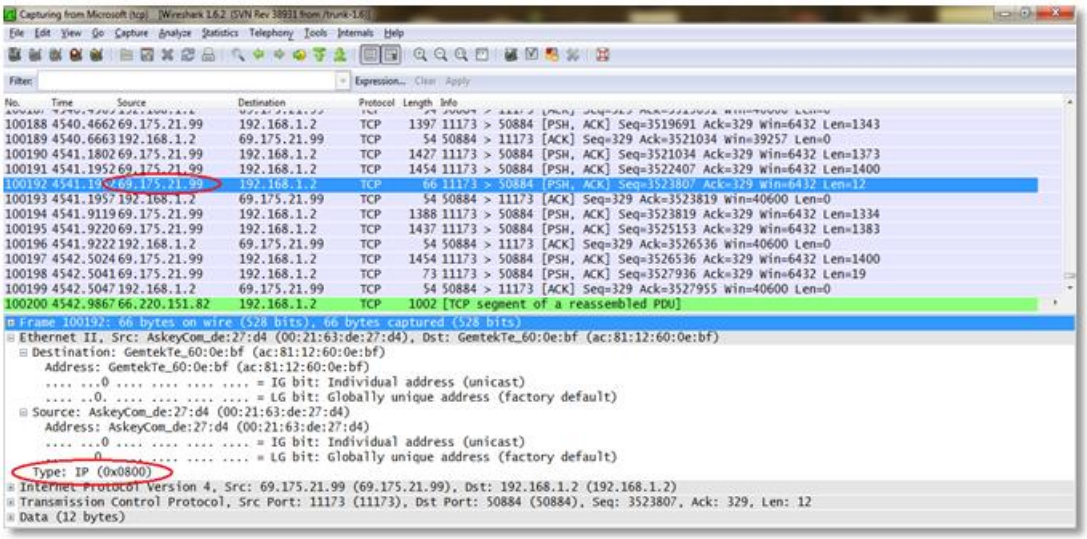


Figura 33. Wireshark cabecera Ethernet.

Fuente: Propia

Preámbulo = 8	Dir. Ethernet Destino MAC Destino = ac:81:12:60:0e:bf	Dir. Ethernet Origen MAC Origen= 00:21:63:de:27:d4
Tipo = 0x800	Cabecera IPv4	Relleno / FCS

Figura 34. Cabecera Ethernet.

Fuente: Propia

En la cabecera Ethernet muestra direcciones MAC origen y destino (direcciones físicas de las tarjetas de host origen y destino), el campo

preámbulo contiene el valor de ocho valor propio de la cabecera Ethernet, el campo tipo indica el valor del protocolo que se utiliza en IPv4, este valor se encuentra en formato de numeración hexadecimal.

Al identificarse el valor del campo tipo (0x800) de la cabecera indica bajo que protocolo va a trabajar y hacia dónde se dirige la información, proceso inicial en la desencapsulación de paquetes.

- Capa Internet - Cabecera IP: la Figura 35 muestra la captura desde el programa Wireshark en la sección Protocolo de Internet versión 4 y continua con la captura visualizada en la Figura 36, con la información obtenida de las dos capturas se establece la cabecera de la capa IP como muestra la Figura 37.

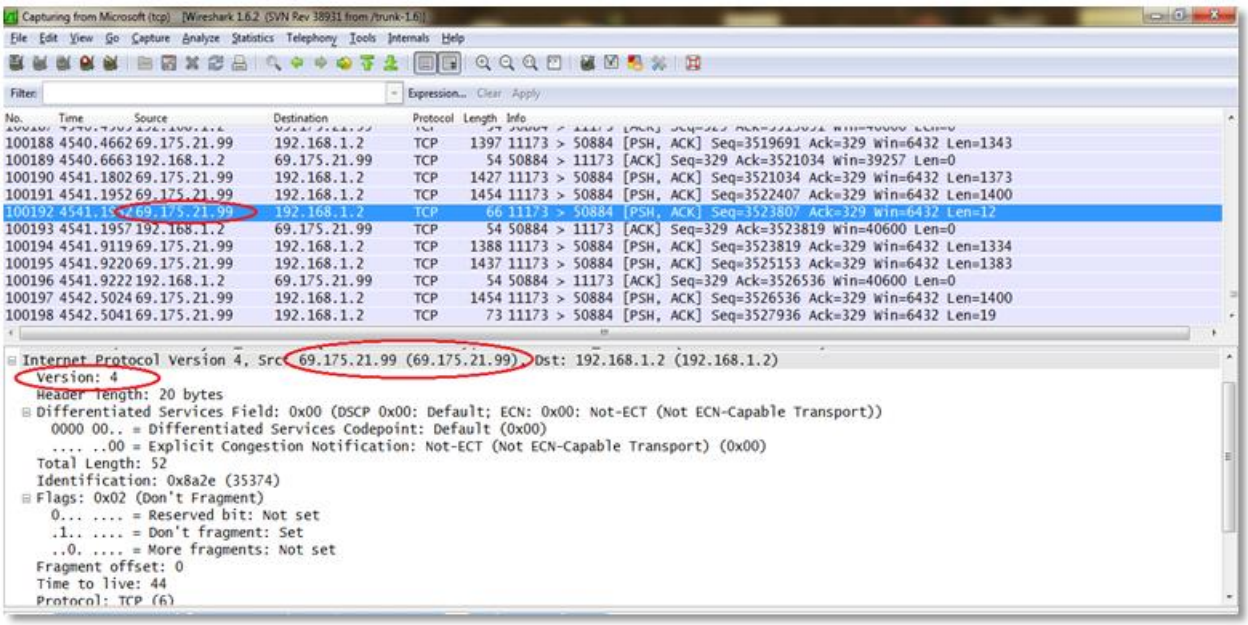


Figura 35. Wireshark cabecera IPv4 (1).

Fuente: Propia

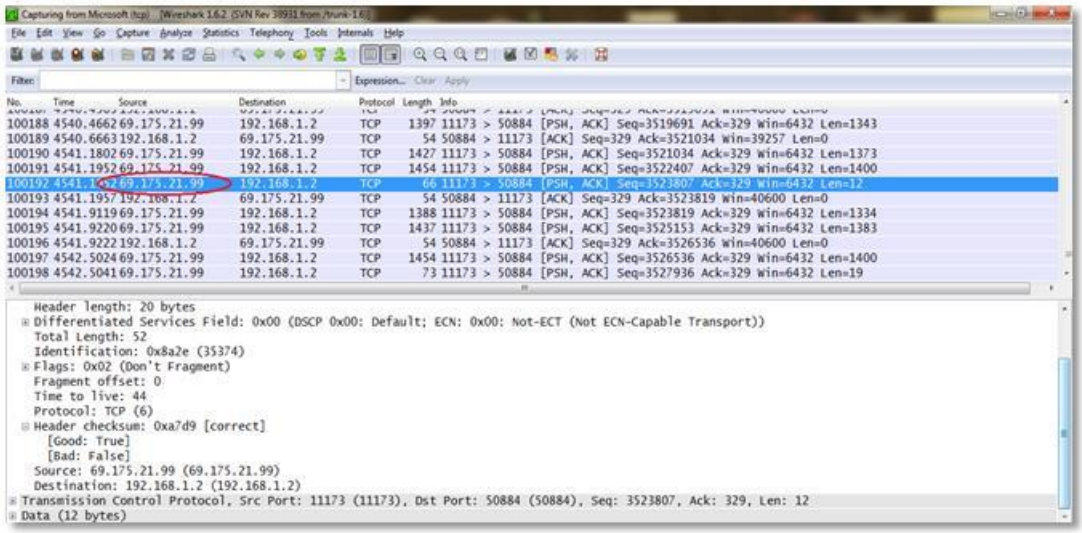


Figura 36. Wireshark cabecera IPv4 (2).
Fuente: Propia

Versión =4	IHL = 20 bytes	Tipo de servicio = 0x00	Longitud total =52
Identificación = 0x8a2e (35374)	DF = 0x02 (No Fragmentar)	MF = No Establecido	Desplazamiento del fragmento = 0
Tiempo de vida = 44	Protocolo = TCP (6)	Suma de verificación de la cabecera = 0xa7d9	
Dirección de origen = 69.175.21.99			
Dirección de destino = 192.168.1.2			

Figura 37. Cabecera IPv4.
Fuente: Propia

La cabecera IP muestra la versión del protocolo de Internet que se esta trabajando, la longitud total de paquete, indica bajo que protocolo se transmite la información en este ejemplo es TCP.

La información trasmitida es bajo el protocolo de Internet versión 4 como indica el campo versión, en base a esta versión se completa la cabecera con las direcciones origen y destino en formato decimal.

- Capa Transporte - Cabecera TCP: las Figuras 38, 39 y 40 muestran las capturas desde el programa Wireshark en la sección Protocolo de Control de Transmisión, con la información obtenida se establece la cabecera de la capa transporte como muestra la Figura 41.

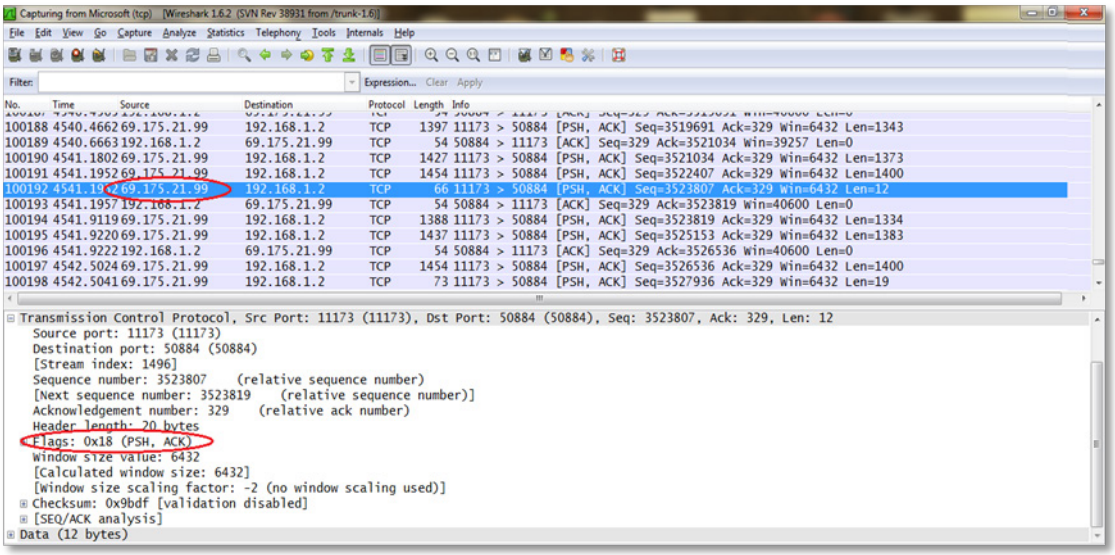


Figura 38. Wireshark cabecera TCP (1).
Fuente: Propia

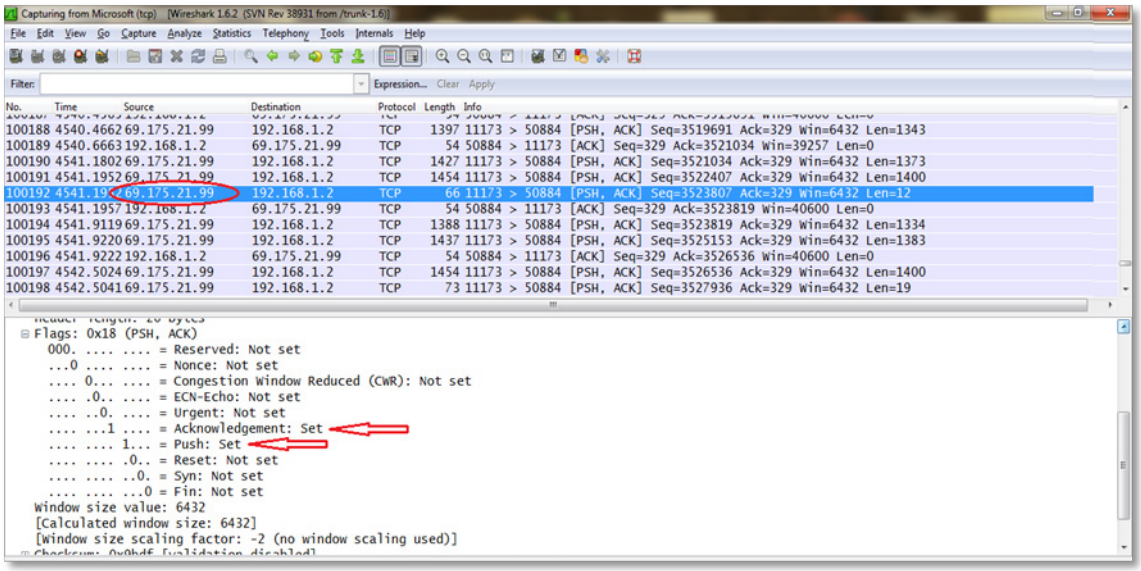


Figura 39. Wireshark cabecera TCP (2).

Fuente: Propia

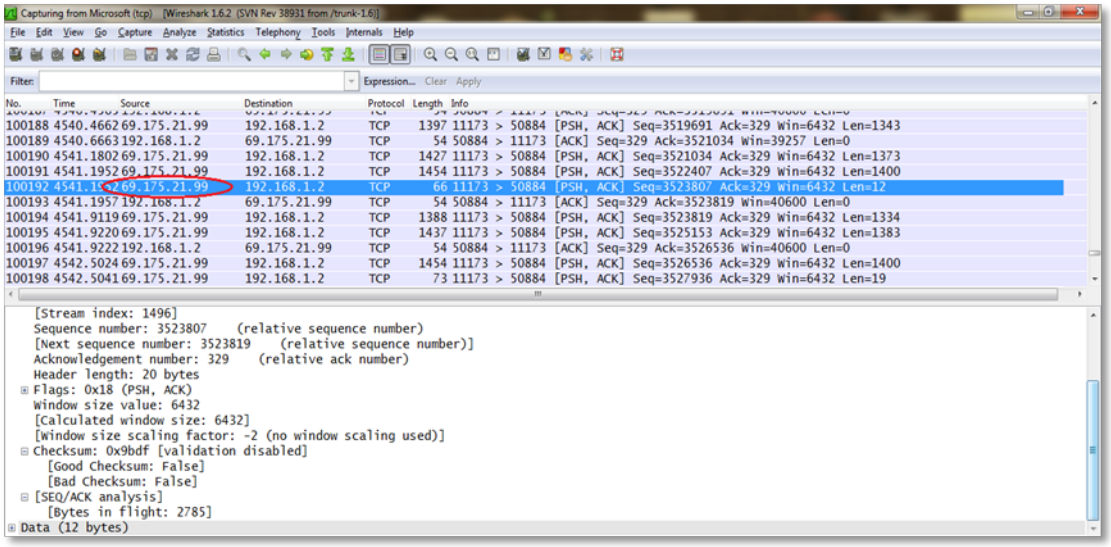


Figura 40. Wireshark cabecera TCP (3).

Fuente: Propia

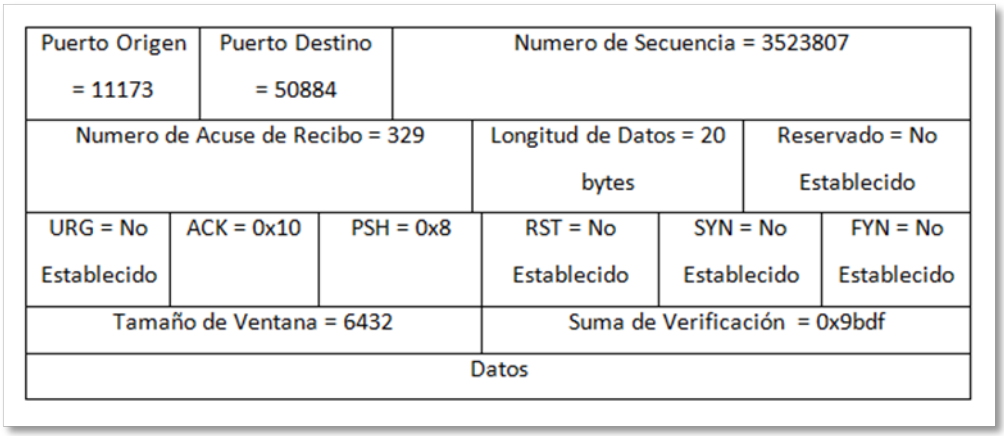


Figura 41. Cabecera TCP.

Fuente: Propia

La cabecera TCP muestra los puertos entre host origen y destino, acuse de recibo utlizados en la comunicación, en esta cabecera contiene banderas que son indicadores para la comunicación se realice de manera sincronizada, los campos de estas banderas que tienen valor de uno son ACK y PSH.

Bajo el modelo de referencia TCP/IP se desencapsula desde la capa acceso a la red hasta llegar al usuario final con la capa aplicación, cada cambio

se visualiza en todo el proceso anterior y el resultado se observa en la Figura 42.

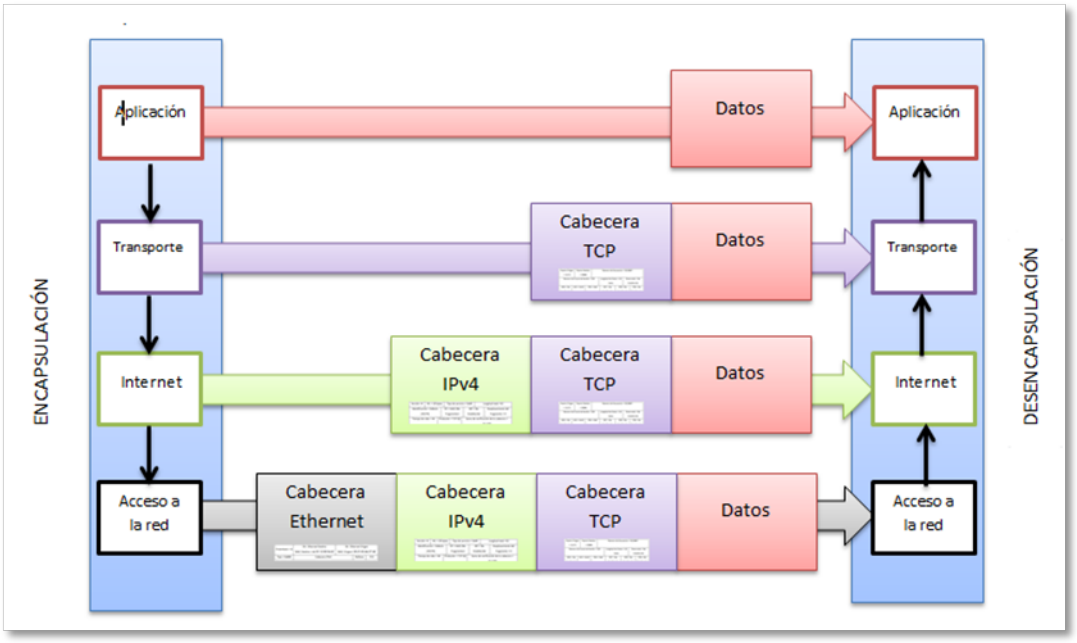


Figura 42. Encapsulación / Desencapsulación modelo TCP/IPv4.

Fuente: Propia

5.3.2. PAQUETE IPV6

El análisis en Wireshark describe los valores de cada campo de las capas: acceso a la red, internet y transporte, para capa aplicación los datos se transmiten bajos los mismos protocolos de usuario final (HTTP, DNS, FTP). La dirección IPv6 que se analiza es: 2800:68:c:8001::

- Capa Acceso a la Red - Cabecera Ethernet: la Figura 43 muestra la captura desde el programa Wireshark en la sección Ethernet II, con la información obtenida se establece la cabecera de la capa enlace de datos como muestra la Figura 44.

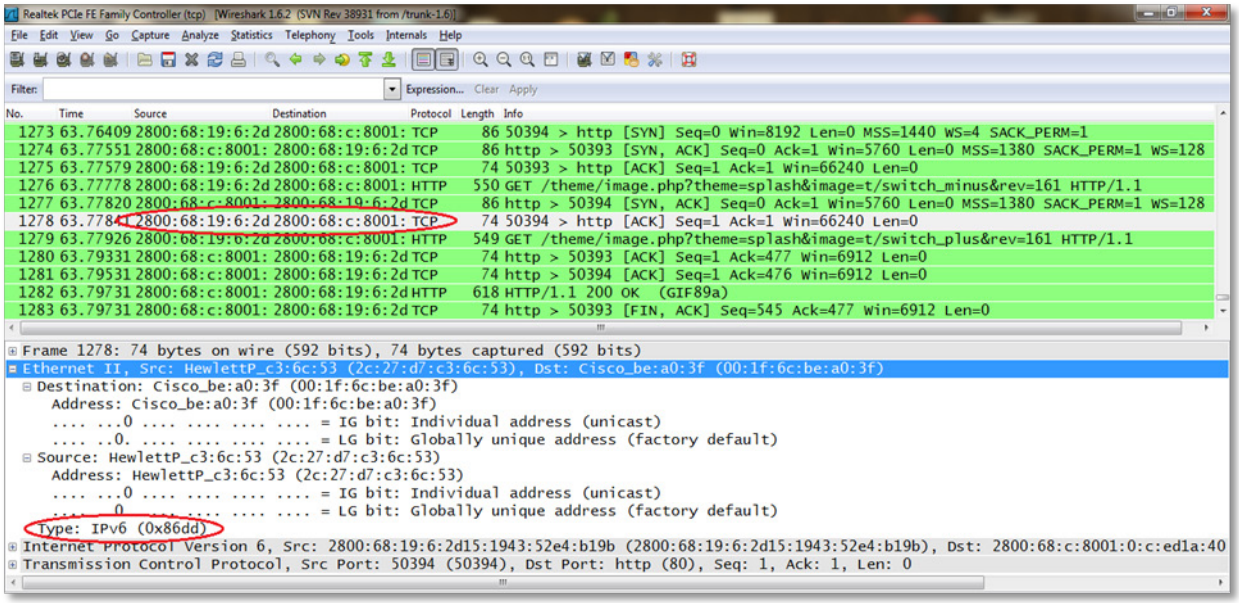


Figura 43. Wireshark cabecera Ethernet.

Fuente: Propia

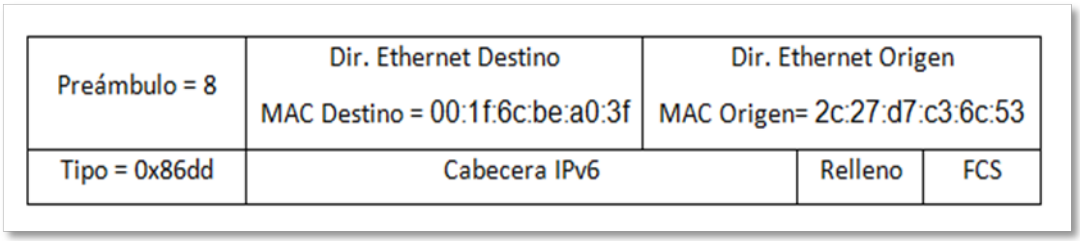


Figura 44. Cabecera Ethernet.

Fuente: Propia

En la cabecera Ethernet muestra direcciones MAC origen y destino (direcciones físicas de las tarjetas de host origen y destino), el campo preámbulo contiene el valor de ocho valor propio de la cabecera Ethernet, el campo tipo indica el valor del protocolo que se utiliza (IPv6), este valor se encuentra en formato de numeración hexadecimal.

Al identificarse el valor del campo tipo (0x86dd) de la cabecera indica bajo que protocolo va a trabajar y hacia dónde se dirige la información.

- Capa Internet - Cabecera IPv6: la Figura 45 muestra la captura desde el programa Wireshark en la sección Protocolo de Internet versión 6, con la información obtenida se establece la cabecera de la capa IP como muestra la Figura 46.

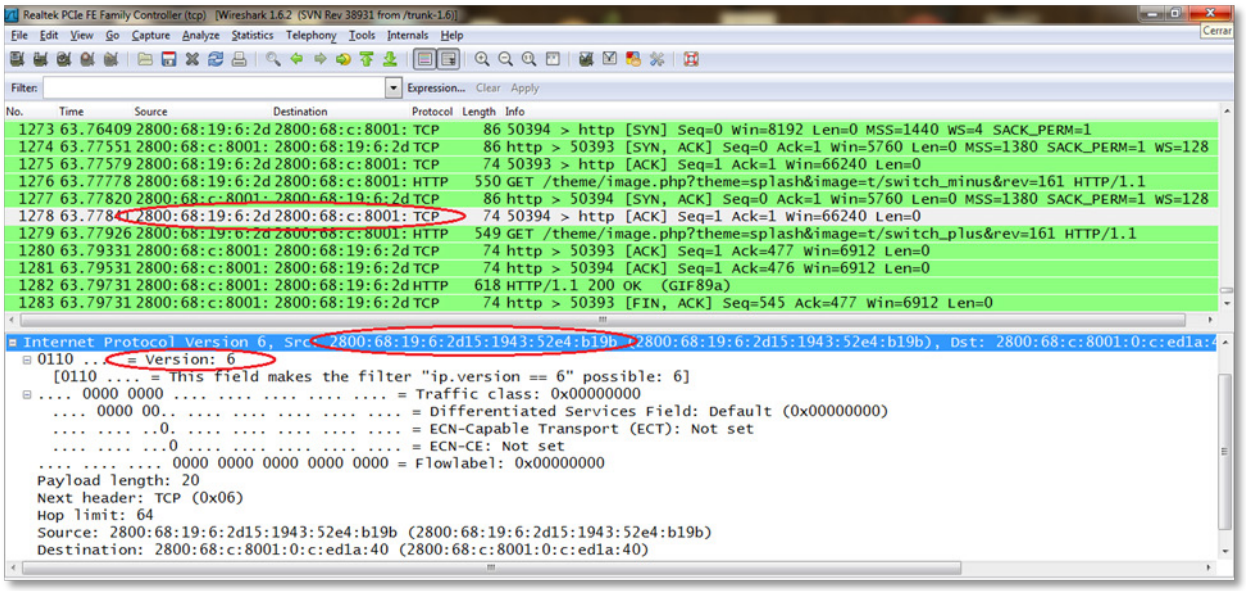


Figura 45. Wireshark cabecera IPv6.

Fuente: Propia

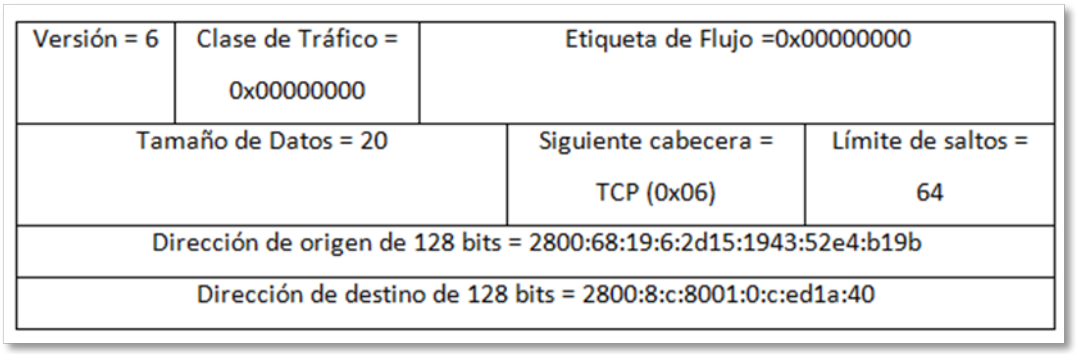


Figura 46. Cabecera IPv6.

Fuente: Propia

La cabecera IP muestra la versión del protocolo de Internet que se esta trabajando, tipo de tráfico, sino existen cabeceras de extensión el campo siguiente cabecera muestra la siguiente cabecera, en el caso de desencapsulación la siguiente cabecera se asigna a la capa transporte (TCP).

La información trasmitida es bajo el protocolo de Internet versión 6 como indica el campo versión, en base a esta versión se completa la cabecera con las direcciones origen y destino, direcciones en formato hexadecimal.

- Capa Transporte - Cabecera TCP: la Figura 47, 48 y 49 muestran las capturas desde el programa Wireshark en la sección Protocolo de Control de Transmisión, con la información obtenida de las capturas se establece la cabecera de la capa transporte como muestra la Figura 50.

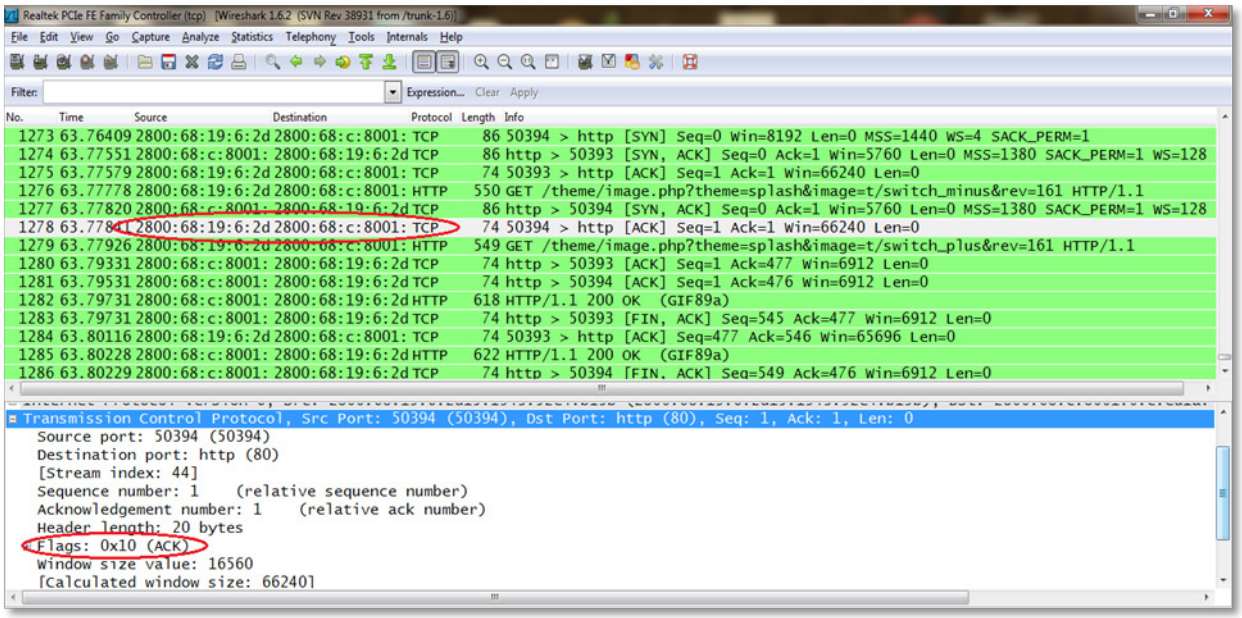


Figura 47. Wireshark cabecera TCP (1).

Fuente: Propia

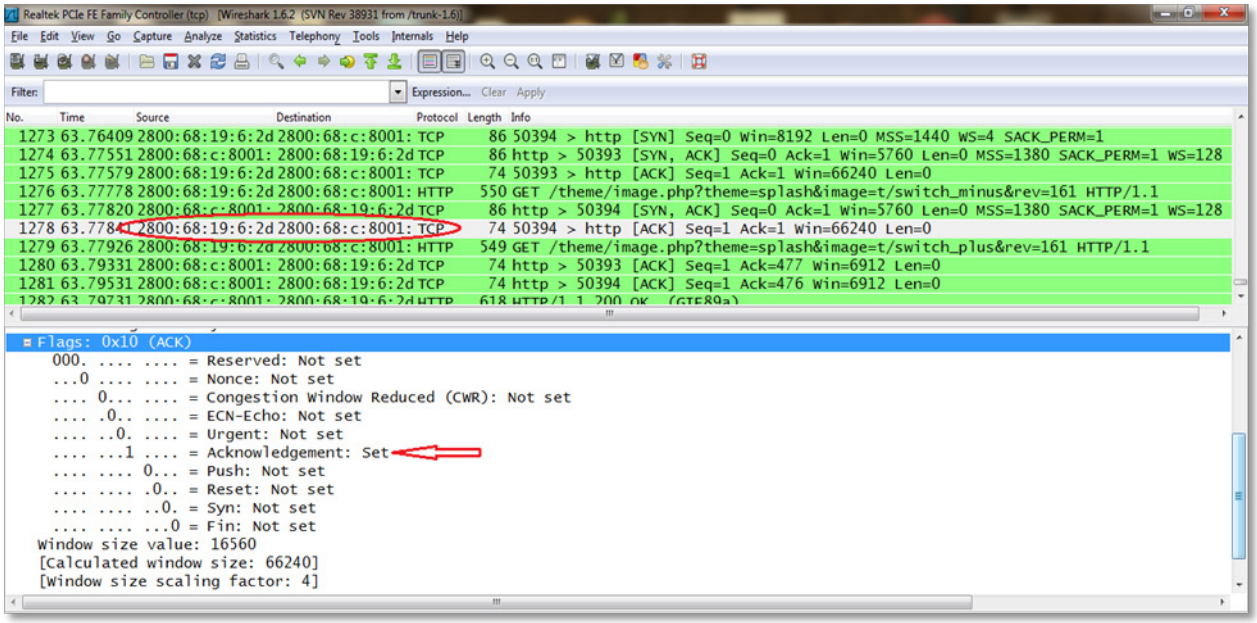


Figura 48. Wireshark cabecera TCP (2).

Fuente: Propia

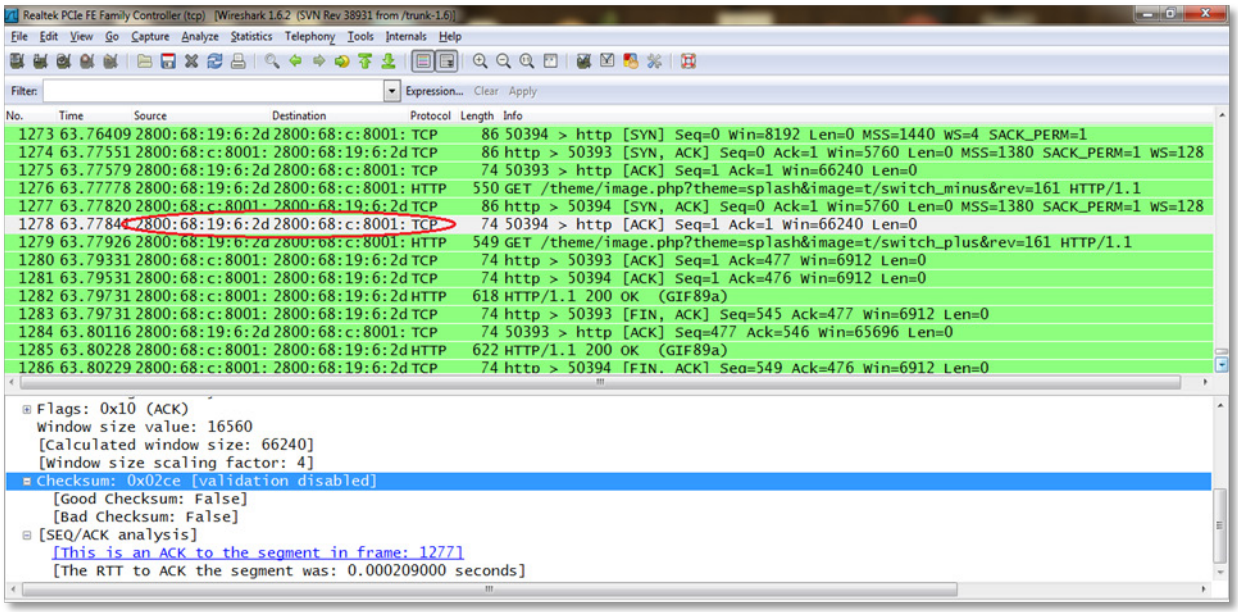


Figura 49. Wireshark cabecera TCP (3).

Fuente: Propia

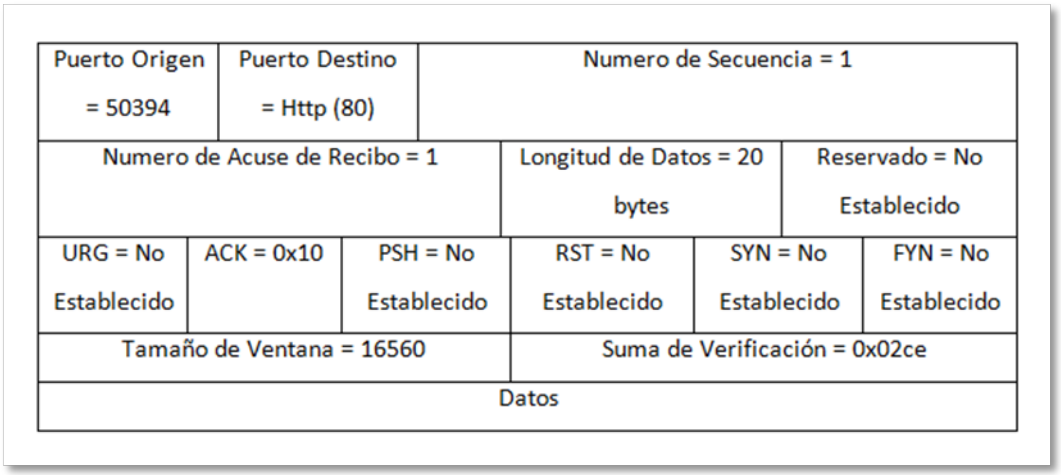


Figura 50. Cabecera TCP.

Fuente: Propia

La cabecera TCP muestra los puertos entre host origen y destino, acuse de recibo utlizados en la comunicación, en esta cabecera majera banderas que son indicadores para la sincronizacion de la comunicación se realice, el campo de esta bandera que tienen valor es ACK .

Bajo el modelo de referencia TCP/IP se desencapsula desde la capa acceso a la red hasta llegar al usuario final con la capa aplicación, cada cambio se visualiza en todo el proceso anterior y el resultado se observa en la Figura 51.

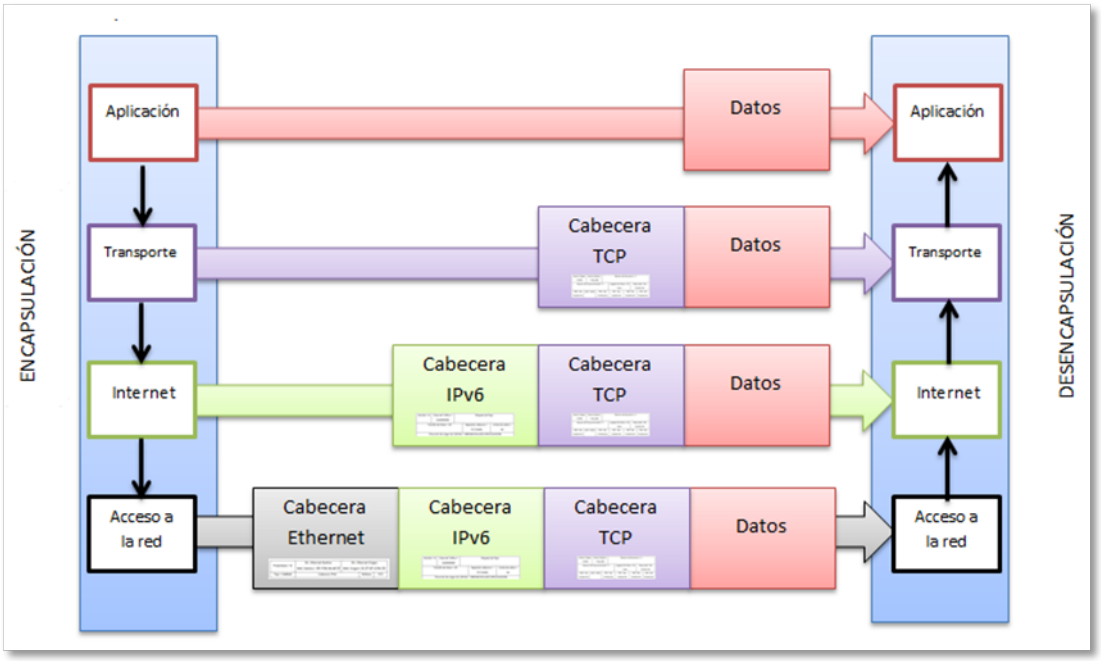


Figura 51. Encapsulación / Desencapsulación modelo TCP/IPv6.

Fuente: Propia

Al finalizar el análisis del detalle los campos de cada cabecera del modelo TCP/IP, se identifican las diferencias presentes de los dos protocolos como indica la Tabla 31.

Tabla 31

Comparación cabecera modelo TCP/IPv4 y TCP/IPv6

CAPA TCP/IP	IPv4	IPv6
Ethernet	Tipo = 0x800	Tipo = 0x86dd
Internet	Versión = 4	Versión = 6
	Dir. Origen = 69.175.21.99	Dir. Origen = 2800:68:19:6:2d15:1943:52e4:b19b
	Dir. Destino = 192.168.1.2	Dir. Destino = 2800:8:c:8001:0:c:ed1a:40

La red de datos UTN Dual Stack funciona correctamente y accede a páginas y sitios web que poseen de igual manera en la red Dual Stack.

5.4. APLICACIÓN EN SERVIDOR WEB

Un servidor web es una máquina configurada para que resuelva continuamente peticiones de otros dispositivos (clientes) y entrega como resultado a la solicitud una página web.

Una vez que se ha verificado el tráfico de paquetes IPv6 en UTN, se realiza la demostración de funcionamiento de un servidor web sobre IPv6, en el cual se configura en una máquina virtual sobre la plataforma Linux Ubuntu 12.04 incluye la instalación de Apache[30]. La versión del sistema operativo y Apache soportan el protocolo de Internet versión 6.

El inicio de la máquina virtual se indica en la Figura 52, que muestra también el programa *Terminal* donde se configuran las direcciones IPv4 e IPv6, este proceso es inicial para verificar si las aplicaciones que se ejecuten sobre IPv6 funcionan con normalidad y transparencia al usuario final.

[30] Apache: Software de aplicación de servidor web

Figura 52. Pantalla inicial de máquina virtual.

Fuente: Propia

Al dar click e ingresar al programa *Terminal* para realizar la configuración de la dirección del servidor bajo comandos, se escribe el comando *sudo gedit /etc/network/interfaces* (Figura 53) para agregar las direcciones IPv4 e IPv6 que se van a utilizar, al presionar Enter se abre una nueva ventana denominada *Interfaces* para editar las direcciones (Figura 54).

```
ubuntu@ubuntu-VirtualBox:~$ sudo gedit /etc/network7interfaces
[sudo] password for ubuntu:
ubuntu@ubuntu-VirtualBox:~$
```

Figura 53. Comando para editar interfaces.

Fuente: Propia

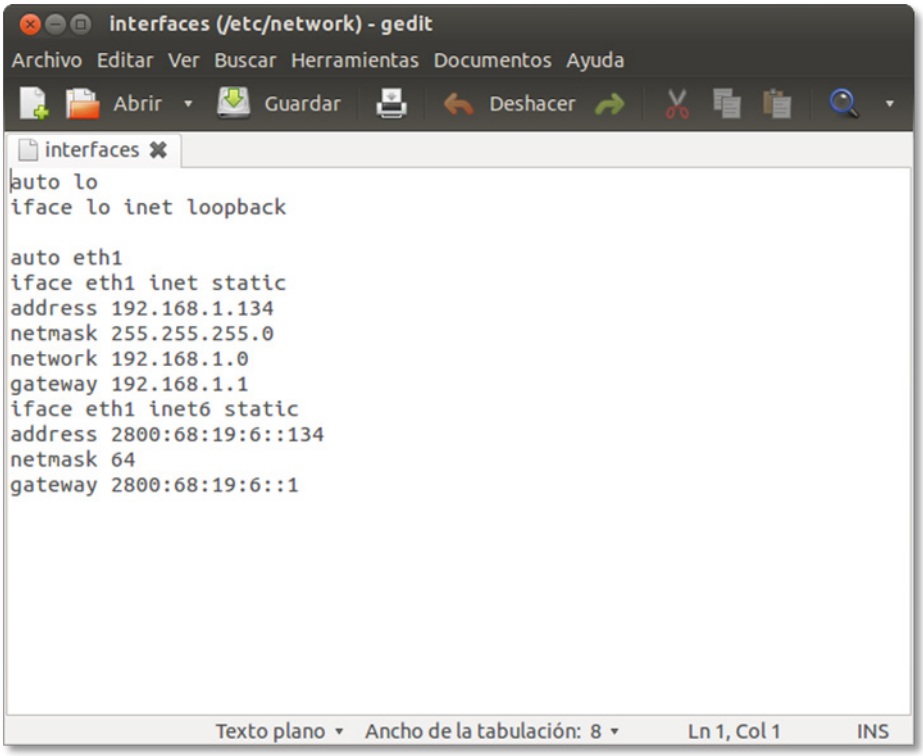


Figura 54. Agregando direcciones IPv4 e IPv6.

Fuente: Propia

De la Figura 54 se observa que la configuración se realiza en la interfaz *eth1* que posee conexión mediante cable UTP, para el protocolo de Internet versión 4 se agrega *iface eth1 inet static* (eth1= interfaz conectada, inet= IPv4, static= configuración de red estática); ahora para el protocolo de Internet versión 6 se agrega *iface eth1 inet6 static* (eth1= interfaz conectada, inet6= IPv6, static= configuración de red estática), guardamos las configuraciones realizadas y cerramos la ventana de interfaces, seguidamente se reinician las misma bajo el comando *sudo /etc/init.d/networking restart* como indica la Figura 55.

Figura 55. Reinicio de configuraciones de red

Fuente: Propia

Una vez establecidas las direcciones en IPv4 e IPv6 (Dual Stack), se instala Apache bajo el comando *sudo apt-get install apache2* al ejecutar este comando se descarga la aplicación desde la conexión a Internet como muestra la Figura 56.

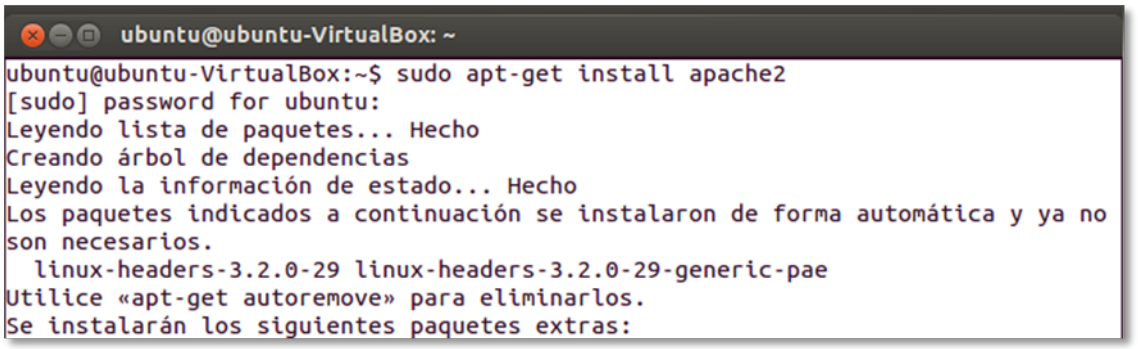


Figura 56. Instalación Apache

Fuente: Propia

Se verifica que la conexión IPv6 activa escuche por el puerto 80 (puerto utilizado para peticiones HTTP[31]) permitiendo recibir y enviar peticiones en el servidor web sobre IPv6, la acción se realiza bajo el comando *netstat –tan* en el programa Terminal como indica la Figura 57, en la que se observa la conexión activa de Internet se encuentra escucha por el puerto 80 en IPv6 (tcp6).

31

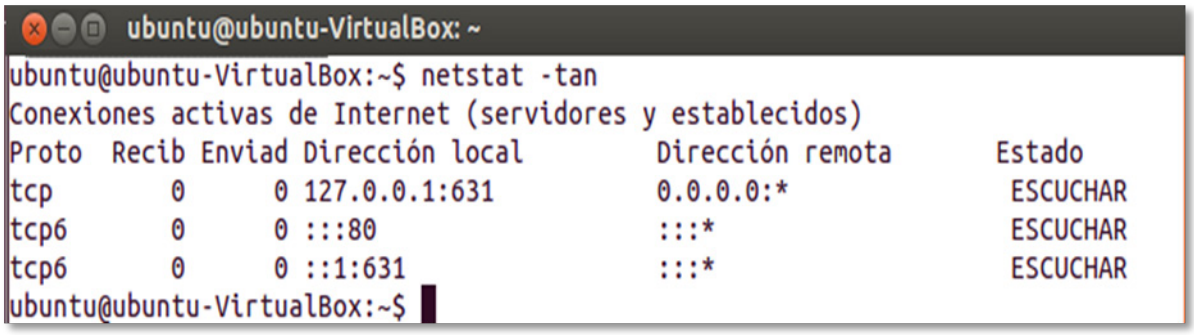


Figura 57. Verificación de IPv6 que escucha por el puerto 80

Fuente: Propia

En el navegador ingresamos la dirección IPv6 en URL entre corchetes como indica la Figura 58 y aparece el mensaje It works! indicando que se encuentra trabajando con normalidad con la dirección IPv6 establecida.

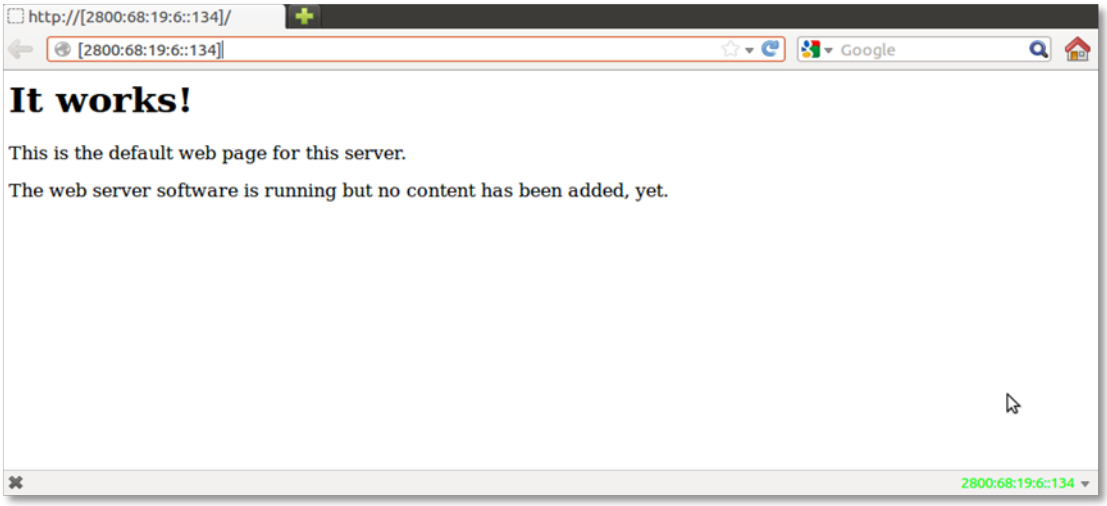


Figura 58. Verificación servicio web con dirección IPv6.
Fuente: Propia

Desde una máquina con sistema operativo Windows se realiza la prueba de funcionamiento del servidor web sobre IPv6, se abre un navegador y de la misma forma se ingresa la dirección IPv6 del servidor web en la URL y se obtiene el resultado que el servidor web sobre IPv6 trabaja correctamente.

Con la obtención del servidor web que trabaja sobre IPv6 se evidencia la transparencia de aplicaciones que puede beneficiarse el usuario final, sin la necesidad de que el usuario deba realizar nuevas configuraciones.

CONCLUSIONES

- La red de redes Internet opera actualmente bajo el protocolo de Internet versión 4 y su nueva versión 6 se despliega sobre la red existente, razón por la cual se basa en los mismos principios al utilizar el mismo medio de transmisión, aplica tecnología Ethernet, trabaja con protocolo TCP y los datos llegan al usuario bajo protocolos como HTTP, DNS, FTP.

- El principal motivo de crear una nueva versión de protocolo de Internet es la escasez de direcciones disponibles IPv4, en la cual la dirección de red se incrementa de 32 bits a 128 bits y al mismo tiempo se reduce su cabecera modificando algunos campos donde routers procesan rápidamente la información dando como resultado aplicaciones multimedia en tiempo real.

- La gran importancia que tiene el estudio de IPv6 ha ocasionado que más instituciones educativas, públicas y privadas decidan planificar su uso en las redes de datos preparándose hacia los nuevos retos tecnológicos ya que iniciar con el planeamiento de trabajar con IPv6 ahora permite que los administradores de red se familiaricen con IPv6 proporcionando una ventaja hacia un futuro cercano con usuarios, servicios y aplicaciones IPv6.

- Es importante diferenciar entre transición y migración; transición es un proceso donde el escenario de trabajo es compartido para IPv4 e IPv6 y migración es un proceso donde el escenario de trabajo es totalmente IPv6.

- Al finalizar la configuración de IPv6 con doble pila en equipos de red (router, switch, servidores), se concluye que las dos versiones de protocolos de Internet se encuentran en el mismo equipo pero trabajan independiente uno del otro, dando como resultado que todo este proceso sea transparente para el usuario final.

RECOMENDACIONES

- Aunque la selección del mecanismo de transición depende del administrador de red, se recomienda aplicar doble pila ya que se trabaja con los dos protocolos simultáneamente proporcionando ventaja a futuro al administrar la red simultáneamente con IPv6.

- IPSec en IPv6 es parte fundamental pero es necesario complementar la seguridad en la red de datos de una institución como se realiza con IPv4 en aplicar una buena política de seguridad como en la determinación de los servicios que son accesibles por tiempo completo, restricción de puertos, etc.

- En el diseño de la red IPv6 es recomendable que sea una configuración simple y adecuada documentación en la que se posea dominio total del protocolo de Internet versión 6, para que permita posteriormente el fácil crecimiento y/o activación en toda la institución.

- Es importante identificar cuales servicios van a trabajar bajo el protocolo de Internet versión 6 para configurar correctamente los servidores en base a los requerimientos necesarios, ya que algunos sistemas operativos y sus respectivas versiones no soportan IPv6 dificultando difundir el servicio sobre IPv6.

REFERENCIAS BIBLIOGRÁFICAS

Documentos en Internet

[1] CEDIA Red Nacional de Investigación y Educación del Ecuador. Recuperado de: www.cedia.org.ec.

[2] Red CLARA red + ciencia. Recuperado de: www.redclara.net.

[3] Red CLARA2 Comienza su instalación, *Memoria Anual CLARA 2009, núm 5, pág. 17. MEMORIA CLARA 2009.* Recuperado de: www.redclara.net.

[4] TELCONET La fibra del Ecuador, SOLUCIONES, Internet 2. Recuperado de: http://www.telconet.net/?lang=es&section=home.

[5] Nuevos miembros y ancho de banda, *Boletines CEDIA, núm 2, pág.1.* INFORME DE ACTIVIDES FEBRERO 2009. Recuperado de: http://www.cedia.org.ec/index.php.

[6] Nuevos miembros y ancho de banda, *Boletines CEDIA, núm 5, pág.1.* INFORME DE ACTIVIDES DICIEMBRE 2009. Recuperado de: http://www.cedia.org.ec/index.php.

[7] Organización Interna y Directorios, *Boletines CEDIA, núm 16, pág.1*. INFORME DE ACTIVIDES JUNIO 2010. Recuperado de: http://www.cedia.org.ec/index.php.

[8] Cursos y Capacitaciones Programadas, *Boletines CEDIA, núm 10, pág.2*. INFORME DE ACTIVIDES DICIEMBRE 2009. Recuperado de: http://www.cedia.org.ec/index.php.

[9] Estatutos de CEDIA. Recuperado de: http://www.cedia.org.ec/index.php.

[10] Curriculum CISCO Networking Academy Exploration v4.0. Capítulo 3: Protocolos y funcionalidad. Semestre nro. 1.

[11] RFC 791. Protocolo de Internet. Recuperado de: http://www.ietf.org/rfc/rfc791.txt.

[12] Curriculum CISCO Networking Academy Exploration v4.0. Capítulo 5: Capa de red de OSI. Semestre nro. 1.

[13] Curriculum CISCO Networking Academy Exploration v4.0. Capítulo 6: Direccionamiento de red IPv4. Semestre nro. 1.

[14] Technet Microsotf. Protocolo de resolución de direcciones (ARP, Address Resolution Protocol). Recuperado de: http://technet.microsoft.com/es-es/library/cc758357%28v=ws.10%29.aspx.

[15] RFC 903. Protocolo de resolución reversa de dirección. Recuperado de: http://tools.ietf.org/rfc/rfc903.txt.

[16] Tópicos Avanzados en Redes de Computadoras y Telecomunicaciones. Universidad Nacional de Asunción. Recuperado de: http://www.fdi.ucm.es/profesor/jcfabero/Asuncion09/ipv6.pdf.

[17] RFC 2460 Protocolo de Internet versión 6. Recuperado de: http://tools.ietf.org/html/rfc2460

[18] Características principales en IPv6, IPv6 Servicio de Información y Soporte, num 10, pág.3. EL PROTOCOLO IPV6. Recuperado de: http://www.6sos.org/glosario.php.

[19] Tutorial de IPv6. Consulintel. IPv6 Forum. Autor Jordi Palet, Director de Producto Consulintel, Presidente del Grupo de Trabajo de Educación Promoción y Relaciones Públicas del Foro IPv6. Recuperado de: http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf.

[20] RFC 2462 Autoconfiguracion en IPv6. Recuperado de: http://tools.ietf.org/html/rfc2462

[21] RFC 2463 Protocolo de mensajes de Internet para IPv6 (ICMPv6). Recuperado de: http://www.ietf.org/rfc/rfc2463.txt

[22] RFC 2461 descubrimiento del vecindario para IPv6 (Neighbor Discovery). Recuperado de: http://www.ietf.org/rfc/rfc2461.txt

[23] Librería de Microsoft. Características de IPv6. Recuperado de: http://technet.microsoft.com/es-es/library/cc780593%28v=ws.10%29.aspx.

[24] Glosario IPv6, IPv6 Servicio de Información y Soporte, num 12, pág.3. EL PROTOCOLO IPV6. Recuperado de: http://www.6sos.org/glosario.php.

[25] IPv6.br. La nueva generación del Protocolo de Internet. Núcleo de Información y Coordinación de BR. Movilidad IPv6 (pág. 123-130). Recuperado de:

[26] RFC 2080 RIPng. Recuperado de: http://tools.ietf.org/html/rfc2080.

[27] RFC 2740 OSPFv3. Recuperado de: http://tools.ietf.org/html/rfc5340.

[28] Gont F. (2011 Oct. 20). Campus Party *Implicancias en IPv6.* Recuperado de: http://www.youtube.com/watch?v=qyKLIogUrIo

[29] Grossetete Patrick (2011, Junio 07). The IPv6 Benefits in the Smart GRID World. Recuperado: Enero 132013 de: http://www.future-internet.uni.lu/images/stories/presentations/smart%20grid-

[30] Soporte de movilidad para IPv6. Recuperado de: http://tools.ietf.org/html/draft-ietf-mobileip-ipv6-12

[31] RFC 2893 Mecanismos de transición IPv6 para hosts y router. Recuperado de: http://www.ietf.org/rfc/rfc2893.txt.

[32] RFC 4213 Mecanismo de Transición Doble Pila. Recuperado de: http://tools.ietf.org/html/rfc4213.

[33] Enrutamiento IPv6. Núcleo de Informação e Coordenação do ponto BR - São Paulo. 2010. Recuperado de: http://www.6deploy.eu/workshops2/20111128_santo_domingo/TallerIPv6RepDominicana_Routing.pdf

[34] RFC 3056 Mecanismo de Transición – Túneles 6to4. Recuperado de: http://www.ietf.org/rfc/rfc3056.txt.

[35] RFC 2529 Mecanismo de Transición – Túneles 6over4. Recuperado de: http://www.ietf.org/rfc/rfc2529.txt.

[36] RFC 4380 Mecanismo de Transición – Túneles Teredo. Recuperado de: http://www.ietf.org/rfc/rfc4380.txt.

[37] RFC 3053 Mecanismo de Transición – Túneles Túnel Broker. Recuperado de: http://tools.ietf.org/html/rfc3053.

[38] RFC 2026 Mecanismo de Transición DSTM. Recuperado de: http://tools.ietf.org/html/draft-bound-dstm-exp-0.

[39] RFC 2765 Mecanismo de Transición – Traducción SIIT. Recuperado de: http://tools.ietf.org/html/rfc2765.

[40] RFC 2766 Mecanismo de Transición – Traducción NAT-PT. Recuperado de: http://www.ietf.org/rfc/rfc2766.txt.

[41] RFC 2767 Mecanismo de Transición – Traducción BIS. Recuperado de: https://tools.ietf.org/html/rfc2767.

[42] IPv6.br. La nueva generación del Protocolo de Internet. Núcleo de Informação e Coordenação do ponto BR - São Paulo. 2010. Autores: Rodrigo Regis dos Santos, Antônio M. Moreiras, Eduardo Ascenço Reis, Ailton Soares

da Rocha. Movilidad IPv6 (pág. 123-130). Recuperado de: http://ipv6.br/download/#TB_inline?height=350&width=300&inlineId=login-form.

[43] Redes de nueva generación (IPv6). Interconexiones de redes. Protocolos de comunicaciones. Área de Ingeniería Telemática. Departamento de Ingeniería Electrónica y Comunicaciones. Universidad de Zaragoza. 2009. Profesora María Canales. Recuperado de: http://155.210.158.52/docencia_it/Protocolos%20de%20Comunicaciones/TRANSPARENCIAS%20DE%20CLASE/B1T1.2_IPv6_0910.pdf.

Tesis

[44] Machado L. (2008). *Diseño de la infraestructura de red para un miembro tipo de CEDIA y planeamiento de una alternativa de conectividad entre dos miembros*. Tesis para obtención del título en Ingeniero en Electrónica y Redes de Información. Facultad de Ingeniería Eléctrica y Electrónica. Escuela Politécnica Nacional, Quito, Ecuador.

[45] Tesis Magister Redes de Datos. “QoS en redes wileres con IPv6”. Matías Robles. Facultad de Informática – Universidad Nacional de La Plata. 2008. acomodar

[46] Arias H. (2011). Estrategia de Migración de IPv4 a IPv6 para las Pymes en Colombia. Programa de Ingeniería de Sistemas y Telecomunicaciones. Universidad Católica de Pereira, Pereira, Colombia.

Libros

[47] Sector Público, Privado y Sociedad Civil (2009). *Libro Blanco Sociedad de la Información - Ecuador*. *Libro Blanco* (pp. 69-77).

[48] Tanenbaum, Andrew. (2007). Redes de Computadoras. México: Patti Guerrieri. (pp. 37-49).

[49] Josep M. Barcelo Odinas, Jordi Iñigo Griera, Jaume Abella Fuentes. Estructura de redes de computadores (2009). Editorial UOC. Capítulo V: Redes de gran alcance: Internet.

[50] Olifer, N., Olifer, V. (2009). Redes de computadoras. México: Litografía Ingramex.

[51] Francisconi, H. A. (2010). IPsec en Ambientes IPv4 e IPv6. Argentina: Carril Godoy Cruz.

[52] Posso A. (2011). *Tejiendo un Sueño. Apuntes para la historia de la Universidad Técnica del Norte.* Quito, Ecuador: Mariscal

[53] Todd Lammle (2007). *CCNA: Cisco Certified Network Associate. Study Guide.* Canadá. (pp. 740-772).

[54] Agbinya J. (2009). *IP Communications and Services for NGN*. Auerbach ISBN

GLOSARIO DE TÉRMINOS

PoP: Punto de Presencia. Punto geográfico, especialmente una ciudad, desde donde un Proveedor de Servicios Internet ofrece acceso a la red Internet.

NGN: Next Generation Network.

NTT: NipponTelegraph and Telephone Communications. NipponTelegraph and Telephone Communications, opera el mayor backbone IPv6 del mundo, que se extiende a lo largo de Asia, Europa, Norteamérica y Australia.

NREN: Red Nacional de Investigación y Educación.

VPN: Redes Privadas Virtuales.

Streaming. Es una tecnología que acelera la descarga de audio y video en la web.

TELCONET: Empresa privada operadora de comunicaciones corporativas y proveedora de servicios de Internet en Ecuador.

STM-1: (Synchronous Transport Module level 1) trama básica de Jerarquía Digital Síncrona con velocidades de 155 Mbps de fibra óptica.

LACNIC: Latin American and Caribbean Internet Addresses Registry – Registro de Direcciones de Internet para América Latina y el Caribe. Organización responsable de asignar y administrar direcciones IP.

OSI: Interconexión de Sistemas Abiertos.

TCP/IP: Protocolo de Control de Transmisión/Protocolo de Internet

IETF: Organización que por medio de ella estandarizan protocolos para la arquitectura de Internet, además de especificar normas y se visualizan mediante la representación de RFC.

ARPAnet: Proyecto de la Agencia de Programas Avanzados de Investigación (Advanced Research Projects Agency, ARPA) del Departamento de Defensa de los Estados Unidos, con el propósito de interconectar computadoras de distintas universidades e institutos de investigación.

RSVP: Resource Reservation Protocol, Protocolo de Reserva de Recursos, utilizan hosts como routers para pedir o entregar niveles específicos de calidad de servicio (QoS) para los flujos de datos de las aplicaciones.

NAT: (*Network Address Translation*) permite asignar una red completa o varias redes a una sola dirección IP.

DHCPv6: Protocolo de configuración dinámica de host para IPv6.

ICMPv6: Protocolo de mensajes de control de Internet para IPv6.

MIPv6: Mobile Internet Protocol version 6 Protocolo de Internet versión 6 móvil, protocolo creado para permitir conexiones móviles.

PDA's: Personal Digital Assistant Asistente Digital Personal, mini agenda electrónica personal.

Plug &Play: Término que se refiere a la capacidad de un sistema informático de configurar automáticamente los dispositivos al conectarlos.

Grid: Es una tecnología que permite utilizar de manera coordinado todo tipo de recurso como es computadores. Grid puede ser despachador de trabajos, manejador de colas o balanceador de carga.

Binding Updates: Enviado por el Nodo Móvil para notificar una nueva Dirección Remota al Agente de Origen o al Nodo Correspondiente.

Binding Acknowledgement: Enviado para confirmar la recepción de un mensaje Binding Update.

NDP: Neighbor Discovery Protocol.

TRT: Trasport Relay Trasnlator.

Medio de transmisión guiado: Hacen uso de medios físicos y solidos para la transmisión de datos.

Medio de transmisión no guiado: Hacen uso ondas electromagnéticas del medio (aire) para la transmisión de datos.

DMZ: Zona desmilitarizada es una red local que se sitúa entre la red interna y la red externa, con la finalidad de apartar a posibles intrusos de la red interna.

Apache: Software de aplicación de servidor web.

Apéndice A

INFORME DE ACTIVIDADES DICIEMBRE 2009

CONSORCIO ECUATORIANO PARA EL DESARROLLO
DE INTERNET AVANZADO

Informe de Actividades Diciembre
Villie Morocho Zurita, Ph.D., Director Ejecutivo

Organización Interna y Directorios

Se realizó con éxito el la Asamblea del CEDIA en la ESPE el día 4 de diciembre, se agradece la hospitalidad de la institución y de manera especial al Señor Rector Grab. Rubén Navia Loor y de la Ing. Lourdes De la Cruz. En la asamblea fue **presentado y aprobado el presupuesto para el 2010** y una de las resoluciones a destacar es la necesidad de **iniciar una licitación para la compra de nuevas capacidades de Internet** con otros proveedores. Para este último punto se ha solicitado ya la conformación de la comisión técnica.

Ilustración 1 Asamblea del CEDIA con la participación de 17 miembros

Problema de conectividad con las Universidades de Loja
Se mantiene seguimiento por parte de la comisión conformada para la instalación de la fibra óptica de TELCONET.

Calendarización de videoconferencias de CEDIA
El sistema de videoconferencias que está siendo desarrollado desde CEDIA se espera iniciar sus pruebas beta a en enero.

CEDIA El Concurso Ecuatoriano de Proyectos en Redes Avanzadas

Segunda convocatoria CEPRA'09
Los únicos proyectos que llegaron a presentar toda la documentación necesaria en la segunda convocatoria son:

1. Proyecto: "IMPLEMENTACIÓN DE UN LABORATORIO COMPUTACIONAL DE ALTO RENDIMIENTO PARA EL CÁLCULO DE PROPIEDADES FÍSICAS Y QUÍMICAS DE MATERIALES"
Área de Investigación:
- Comunidades científicas virtuales
- Laboratorios virtuales
- Computación distribuida

Institución: UTPL

2. "PROYECTO PLATAFORMA E-LEARNING PARA LA RED AVANZADA"
Institución: UNIVERSIDAD CENTRAL DEL ECUADOR

Dichos proyectos se encuentran en proceso de revisión por parte de los pares nacionales e internacionales y se espera la resolución para los primeros días de enero.

Nuevos Miembros y Ancho de Banda

Se ha solicitado la integración a CEDIA por parte de INDOAMERICA, el proceso se encuentra en estudio de factibilidad técnica debido a la ubicación de las instalaciones de la institución. Se espera los resultados del proveedor de servicios, TELCONET.

Se incrementa el ancho de banda de Internet Comercial, por pedido de la UPS.

Incremento de ancho de banda del anillo de Red Avanzada
Finalmente se cuenta con 1 Gbps de ancho de banda en Internet Avanzado para los miembros del CEDIA. Sin embargo, existen

actualizaciones no realizadas todavía a los equipos de los miembros integrados posteriores al contrato CEDIA TELCONET, dichas actualizaciones por contrato deben tardar mayor tiempo, por lo que se está trabajando para poder incrementar su ancho de banda.

Proyectos de Investigación

Ilustración 2 Reunión de trabajo WP6 de CLARA en Lima

Infraestructura de Datos Espaciales de RedCEDIA.

CEDIA presentó, en el WP6 de CLARA, llevado a cabo en LIMA, el proyecto sobre gestión de datos espaciales IDERedCEDIA (donde participan la UTPL, ESPOCH y UNIANDES), que realiza exitosamente y que está basado en el IDEUCuenca (http://ide.ucuenca.edu.ec).

Ilustración 3 Investigadores de la ESPOCH luego del Curso IDERedCEDIA

Esta IDE base, tiene el auspicio de la Agencia Española de Cooperación para el Desarrollo (AECID) en conjunto con la Universidad Politécnica de Cataluña (Centre de Política de Sòl i Valoracions) y la colaboración técnica de la IDE Cataluña. *La presentación fue recibida con interés por los miembros del WP6 que proponen incluirlo como un proyecto a extenderse a otros países de CLARA y a considerarse como una fuente para un servicio de información de CLARA.*

Por otra parte se llevó con éxito la capacitación al personal de la ESPOCH dentro del Proyecto IDERedCEDIA.

Proyectos presentados desde la presidencia del CEDIA

El Ing. Fabricio Echeverría presentó un informe del avance del proyecto en la asamblea del CEDIA, donde se dio a conocer los logros obtenidos y se llamó a la integración de otros miembros a dicho proyecto. Las Instituciones que forman parte actualmente del proyecto son 12: ESPOCH, UIDE, UCUENCA, UNL, UTA, UNACH, UTE, UNEMI, UEB, UCE, ESPOL, ESPE.

Relación con CLARA

Se organizó el taller de CLARA para el **ÁREA 2: Ciencias de la tierra y del mar (Ecología, Climatología, Oceanografía y Vulcanología)**, con la colaboración de la ESPE. Dicho evento contó con la participación de investigadores de diferentes países. Se presentó también el proyecto IDERedCEDIA el que fue bien recibido por los asistentes.

- Ángel Muñoz; agmunoz@cmc.org.ve; Venezuela
- Eric Chichaco; echichaco@yahoo.com; Panamá
- Gerardo Montoya Gaviria; gemonga@gmail.com; Colombia
- Alexander Caneva; alexander.caneva@uan.edu.co; Colombia
- Katiuska Briones; k.briones@cifen-int.org; Ecuador
- Mauro Mendoza Chacaltana; mmendoza@planbinacional.org.pe; Perú
- Miguel F. Acevedo; acevedo@unt.edu; USA
- Ana Cecilia Osorio; ana-cecilia.osorio@redclara.net; Chile

Cursos y Capacitaciones programadas

Se ha organizado los siguientes cursos para el mes de Enero y Febrero:

Temas: **IPv6 y Seguridades**
Fecha: 25, 26 y 27 de Enero
Lugar: Universidad de Cuenca
Contacto: Ing. Andrea Morales, Coordinadora General
e-mail: andrea.morales@ucuenca.edu.ec

CONSORCIO ECUATORIANO PARA EL DESARROLLO
DE INTERNET AVANZADO

Tutores: Ing. Claudio Chacón; Ing. Rosario Achig

Temas: **Tutorial GIRD para Usuarios y Administradores**
Fecha: 2 al 5 de Febrero
Lugar: Universidad de Cuenca
Contacto: Ing. Andrea Morales, Coordinadora General
e-mail: andrea.morales@ucuenca.edu.ec
Tutores:
1) Riccardo Bruno, de Italia y auspiciado por INFN/EPIHK
2) Jerome Verleyen, de México y auspiciado por EELA-2
3) Jesus De Oliveira, desde Venezuela y auspiciado por EELA-2

Sede actual en la Universidad de Cuenca

Fundación Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado - CEDIA
Dirección: Av. 12 de Abril y Agustín Cueva, Universidad de Cuenca. Edificio Laboratorios Tecnológicos, 3er. Piso. Cuenca-Ecuador.
Teléfono: (07) 4 051 000 ext. 4220

Dr. Moisés Tacle, Rector de la ESPOL, Presidente del CEDIA
Dr. Villie Morocho Zurita, Director Ejecutivo
vmorocho@cedia.org.ec
Ing. Andrea Morales, Coordinadora General
andrea.morales@cedia.org.ec
Ing. Claudio Chacón, Coordinador Técnico
claudio.chacon@cedia.org.ec
Celular: 097034418
Ing. Rosario Achig, Estadisticas y QoS
rosario.achig@cedia.org.ec
Cnt. Tania Washco, Coordinadora Financiera
tania.washco@cedia.org.ec
Información General:
Ing. Raquel Illescas
info@cedia.org.ec
http://www.cedia.org.ec

Apéndice B

ACTA DE COMPROMISO

ACTA DE COMPROMISO DE MIEMBROS ACADEMICOS, DE INVESTIGACION Y DE DESARROLLO CIENTIFICO DE LA FUNDACION CONSORCIO ECUATORIANO PARA EL DESARROLLO DE INTERNET AVANZADO-CEDIA

En la ciudad de Cuenca, a los tres días del mes de Enero del dos mil once, comparecen a la celebración del presente instrumento, por una parte la **Universidad Técnica del Norte, representada por el Doctor Antonio Posso Salgado, en su calidad de Rector,** a quien para los efectos de este contrato, se la denominará "UTN"; y, por otra, la **Fundación Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado (CEDIA), representada por el Dr. Moisés Tacle, en su calidad de Presidente,** que en adelante se llamará "CEDIA", al tenor de las siguientes cláusulas:

CLAUSULA PRIMERA: ANTECEDENTES .-

De conformidad al Informe presentado por la Comisión de Membresía del CEDIA, se procede a designar como Miembro Académico a la UTN, por cumplir con todos los requisitos de acuerdo al ESTATUTO DEL CONSORCIO ECUATORIANO PARA El DESARROLLO DE INTERNET AVANZADO (CEDIA)

CLAUSULA SEGUNDA: DEBERES Y OBLIGACIONES.-

La UTN se compromete, como Asociado Académico y de Investigación y Desarrollo Científico a lo siguiente:

a) Designar a una persona para formar parte del Consejo Directivo del Consorcio

b) Hacer uso de la red, de conformidad con las disposiciones que al efecto se establecen en la Normativa del CEDIA.

c) Consultar los reportes de investigación que deberán presentar los responsables de los proyectos que reciban aportaciones del CEDIA.

d) Asistir con hasta dos delegados a las reuniones semestrales en que se reporten los avances en los proyectos que reciban aportaciones del CEDIA.

e) Integrar las comisiones permanentes y de trabajo.

CLAUSULA TERCERA: DERECHOS.-

La UTN como miembro de CEDIA se podrá beneficiar de:

a) Participar en los proyectos conjuntos de nueva tecnología de información y comunicación que se realizarían con universidades o empresas de tecnología del exterior afiliada a Internet 2.

b) Tener prioridad en la selección de los proyectos que presenten las universidades ecuatorianas donde se privilegie la participación de dos o más instituciones y cuyos proyectos estén directamente relacionados con las áreas temáticas de los Asociados Institucionales.

c) Presentar candidatos para la selección de instructores de cursos formales de postgrado, seminarios o eventos de capacitación relacionados con la tecnología de comunicaciones y específicamente con Internet2.

d) Gozar de los descuentos que se otorgaran a los afiliados en los cursos formales o eventos de capacitación impartidos por el CEDIA.

e) Tener acceso a información de primera mano en el WEB de CEDIA, sobre el desarrollo de Internet2 en el país y de las noticias relevantes sobre Internet de la Nueva Generación a nivel mundial.

f) Participar en la selección de las instituciones que cumplan con los perfiles requeridos para interactuar en proyectos de nuevas tecnologías o innovadores con universidades del exterior.

g) Participar en los proyectos pilotos que se implementen sobre los nuevos procesos de enseñanza aplicados a la educación: virtual y a distancia.

h) Recomendar por parte del CEDIA a que las universidades nacionales puedan ser escogidas por parte de universidades del exterior para participar en proyectos conjuntos de interés común.

i) Hacer uso de la ley de propiedad intelectual, dentro de todos los productos desarrollados por las universidades que sean puestos a disposición para la red de Internet 2

j) Hacer uso de la ley de comercio electrónico donde se tomará en cuenta únicamente los aspectos de seguridad de datos, éticas de proyectos, buen uso de la información y firmas electrónicas.

k) De otros beneficios que puedan crearse en el futuro para sus asociados.

CLAUSULA CUARTA: MEMBRESIA ANUAL.-

La UTN pagará a CEDIA la cantidad anual de TRES MIL DOLARES AMERICANOS ($3.000,00), por concepto de membresía durante el año calendario 2011, que se lo hará en dos pagos iguales, previa presentación de las facturas respectivas, en las siguientes fechas: Primeros días de Enero del dos mil once MIL QUINIENTOS DOLARES AMERICANOS ($1.500,00); y, los primeros días del mes de Julio del dos mil once MIL QUINIENTOS DOLARES AMERICANOS ($1.500,00). A estos valores se les sumarán los impuestos de ley.

CLAUSULA QUINTA: RATIFICACION.-

Las partes declaran expresamente que se ratifican en lo estipulado en el presente instrumento para constancia de lo cual firman en dos ejemplares de igual tenor y valor en la ciudad de Cuenca a los tres días del mes de Enero del dos mil diez.

Universidad Técnica del Norte
UTN

Dr. Antonio Posso Salgado
Rector

UNIVERSIDAD TÉCNICA DEL NORTE
RECTORADO
IBARRA - ECUADOR

Fundación Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado
CEDIA

Dr. Moisés Tacle
Presidente

Apéndice C

ESTATUTO DEL CONSORCIO ECUATORIANO PARA EL DESARROLLO DE INTERNET AVANZADO (CEDIA)

CAPÍTULO I

DE LA CONSTITUCIÓN, FINES, MISIÓN, ESTRATÉGIAS, DOMICILIO Y PLAZO

Artículo 1.- Se constituye el Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado (CEDIA) para estimular promover y coordinar el desarrollo de las tecnologías de información, las redes de telecomunicaciones e informática, enfocadas al desarrollo científico, tecnológico, innovador y educativo en el Ecuador.

Artículo 2.- El CEDIA es una persona jurídica de derecho privado, sin fines de lucro, que se rige por las disposiciones del Título XXIX del Libro Primero del Código Civil, de otras disposiciones legales pertinentes, de este Estatuto, y de las disposiciones reglamentarias que se expidan, por ello gozará de todos los privilegios y derechos que le confieren las leyes.

Artículo 3.- Son fines del CEDIA:

(i) Fomentar y coordinar proyectos de investigación para el desarrollo de aplicaciones de tecnología avanzada en las áreas de aplicación de las TI, redes de telecomunicaciones e informática enfocadas al desarrollo científico y educativo de la sociedad ecuatoriana.

(ii) Promover el desarrollo de habilidades y formación de recursos humanos capacitados para la innovación y desarrollo de aplicaciones educativas y de tecnología avanzada en las áreas de las tecnologías de información, redes de telecomunicaciones e informática.

(iii) Promover la interconexión e interoperabilidad de las redes de las Instituciones Asociadas y de los Afiliados al CEDIA.

(iv) Promover el desarrollo de nuevas aplicaciones entre sus miembros.

(v) Difundir entre sus miembros todos los desarrollos que se realicen.

(vi) Relevar y determinar las necesidades de desarrollo de Tecnología de Información, Telecomunicaciones e informática de la red avanzada

(vii) Responsable de la administración, control y gestión del punto de conexión en el Ecuador

Artículo 4.- La misión del CEDIA es:

"Promover y coordinar el desarrollo de redes avanzadas de informática y telecomunicaciones, enfocadas al desarrollo científico, tecnológico, innovador y educativo en el Ecuador".

Artículo 5.- Para el cumplimiento de sus fines y misión, el CEDIA podrá:

(i) Realizar todos los actos y contratos lícitos, con personas naturales o jurídicas, públicas o privadas, nacionales o extranjeras, que sean

necesarios o convenientes, o que de una u otra manera se relacionen directamente con su finalidad.

(ii) Recibir asignaciones, legados y donaciones.

(iii) Celebrar convenios de colaboración recíproca.

(iv) Realizar actividades lícitas que produzcan bienes y servicios concordantes con sus fines.

(v) Participar en actividades comerciales y financieras

Artículo 6.- El domicilio del CEDIA será la ciudad de domicilio del Director Ejecutivo, pudiendo establecer representaciones en otros lugares.

Artículo 7.- Las actividades del Consorcio serán las que determinen ser o no sujeto de obligaciones tributarias directas o indirectas.

Artículo 8.- El CEDIA como persona jurídica legalmente constituida es un ente distinto a sus asociados, miembros o integrantes. Sus miembros, donantes y participantes, no adquieren personal, directa, indirecta, subsidiaria ni en forma solidaria, las obligaciones del CEDIA.

Artículo 9.- El tiempo de duración del CEDIA será indefinido, pero podrá disolverse por los casos previstos en la ley, el presente Estatuto y el Reglamento General.

CAPÍTULO II

DE LOS MIEMBROS

Artículo 10.- Los miembros del CEDIA tendrán el carácter de:

a) Asociados Académicos, de Investigación y Desarrollo Científico

b) Asociados Estratégicos

c) Adherentes

d) Honorarios

Artículo 11.- Son **Asociados Académicos** las Universidades y Escuelas Politécnicas, los centros de investigación y de desarrollo científico que suscriban el Acta de Constitución del CEDIA y los que en el futuro cumplan con los requisitos siguientes:

(i) Ser aprobados por el directorio, previo informe favorable de la Comisión de Membresía.

(ii) Suscribir con el CEDIA un Memorando de Compromisos en el que constan los derechos y obligaciones como miembro del CEDIA.

(iii) Contar con un nodo de computación con alta capacidad de transmisión.

(iv) Promover la instalación y operación de la red de transmisión de alta velocidad entre dichos nodos y la extensión de la conectividad de la red con otras redes similares en otros países, conforme al diseño de la red.

(v) Desarrollar y utilizar aplicaciones educativas en las áreas de Tecnología de Información, Telecomunicaciones e Informática.

(vi) Destinar recursos humanos y financieros para llevar a cabo las actividades anteriores.

Artículo 12.- Son **Miembros Estratégicos** los entes establecidos conforme a las leyes del Ecuador que están comprometidos con el desarrollo, evolución y utilización de aplicaciones educativas y de tecnología avanzada, redes de telecomunicaciones e informática, que cumplan con los requisitos siguientes:

(i) Ser aprobados por la Comisión de Membresías de acuerdo a los Estatutos.

(ii) Suscribir con la Asociación un documento, previamente aprobado por el Consejo Directivo, en el que se establezcan los derechos y obligaciones que contrae.

(iii) Aportar al patrimonio de la Asociación fondos por el importe que determine el Consejo Directivo y que serán destinados al desarrollo de aplicaciones educativas y/o de tecnología avanzada, redes de telecomunicaciones e informática, así como aportación de infraestructura, equipos y/o servicios que se consideren esenciales para el desarrollo de la red.

Artículo 13.- Son **Miembros Adherentes** las Universidades, Escuelas Politécnicas e Institutos de Investigación del país que, aun cuando no cuenten con un nodo de computación de alta capacidad de transmisión digital de datos, estén comprometidas con el desarrollo, evolución y utilización de aplicaciones educativas y de tecnología avanzada, redes de telecomunicaciones e informática. También son Miembros Adherentes las Universidades e instituciones de educación del país, las Sociedades Mercantiles, Instituciones de los sectores público, privado o social de nacionalidad ecuatoriana y de instituciones extranjeras, que reúnan los siguientes requisitos:

(i) Ser aprobados por el Comité de Membresías de acuerdo a lo establecido en los Estatutos.

(ii) Presentar un proyecto de documento por suscribir con la Asociación, que establezca derechos y obligaciones, incluyendo el cumplimiento de los requisitos aplicables, previamente aprobado por el Consejo Directivo de conformidad con los Estatutos.

(iii) La presentación de un documento suscrito con un Asociado Académico, mediante el cual se establezca la obligación de destinar coordinadamente con dicho Asociado Académico, recursos académicos adicionales, destinados al desarrollo de aplicaciones educativas y/o de tecnología tecnologías de información, telecomunicaciones e informática.

(iv) Demostrar haber realizado la instalación de los enlaces y las adecuaciones necesarias para su conexión al nodo de computación con alta capacidad de transmisión digital de datos del Asociado Académico, de acuerdo a los estándares técnicos establecidos por la Comisión Técnica de Desarrollo de la Red.

Artículo 14.- Son **Miembros Honorarios** las personas naturales o jurídicas que han prestado servicios relevantes al CEDIA y serán designados como tales por el

Directorio con los votos de por lo menos las tres cuartas partes de sus integrantes.

Artículo 15.- La calidad de miembro del CEDIA se pierde por:

a) Renuncia expresa.

b) Exclusión resuelta por el Directorio de acuerdo con la Reglamentación respectiva.

c) Disolución de la Institución miembro.

Artículo 16.- Son atribuciones y deberes de los Asociados Académicos y de Investigación y Desarrollo Científico los siguientes:

a) Designar a una persona para formar parte del Consejo Directivo del Consorcio

b) Hacer uso de la red, de conformidad con las disposiciones que al efecto se establecen el la Normativa del CEDIA

c) Consultar los reportes de investigación que deberán presentar los responsables de los proyectos que reciban aportaciones del CEDIA

d) Asistir con hasta dos delegados a las reuniones semestrales en que se reporten los avances en los proyectos que reciban aportaciones del CEDIA

e) Integrar las comisiones permanentes y de trabajo.

Artículo 17.- Son atribuciones y deberes de los Miembros Estratégicos:

a) Designar a una persona para formar parte del Consejo Directivo del Consorcio.

b) Consultar los reportes de investigación que deberán presentar los responsables de los proyectos que reciban aportaciones del CEDIA

c) Asistir con hasta dos delegados a las reuniones semestrales en que se reporten los avances en los proyectos que reciban aportaciones del CEDIA

d) Realizar propuestas de proyectos asociados con un miembro académico

e) Integrar las comisiones permanentes y de trabajo.

Artículo 18.- Son atribuciones y deberes de los Miembros Adherentes:

a) Acceder a los beneficios de la red a través del socio que lo patrocina.

b) Ser miembros de las comisiones de trabajo

c) Integrar las comisiones permanentes.

Artículo 19.- De las atribuciones y deberes de los Miembros Honorarios

a) Asesorar al Directorio, al Presidente y al Director Ejecutivo en la búsqueda de recursos y en el fortalecimiento de la cooperación interinstitucional.

b) Integrar las comisiones permanentes y de trabajo.

CAPÍTULO III
DE LA ORGANIZACIÓN

Artículo 20.- El Gobierno del CEDIA será ejercido por:

a) El Directorio
b) El Presidente
c) El Director Ejecutivo
d) Las Comisiones Permanentes

Artículo 21.- El Directorio lo integran sendos delegados de los miembros Académicos y de Investigación y Desarrollo Científico, que tendrán voz y voto.

Participarán con voz sendos delegados de los socios estratégicos.

Artículo 22.- Son atribuciones del directorio:

a) Diseñar y evaluar las políticas institucionales del CEDIA
b) Designar al Presidente, al Director Ejecutivo, y al Asesor Jurídico y Jefe Financiero.
c) Aprobar las estrategias que presente el Director Ejecutivo relacionadas con el cumplimiento de la misión y los fines del CEDIA.
d) Aprobar los Planes Estratégicos y Planes Operativos Anuales que deberá presentar el Director Ejecutivo.
e) Aprobar el ingreso de nuevos miembros.
f) Designar a los Socios Honorarios.
g) Reformar e interpretar el Estatuto.
h) Designar a los miembros de las comisiones permanentes.
i) Crear Comisiones de Trabajo
j) Autorizar al Director Ejecutivo la celebración de convenios, contratos y operaciones económicas que comprometan al CEDIA en montos máximos de acuerdo a la Normativa del CEDIA
k) Dictar los Reglamentos del Consorcio; y,
l) Las demás que señale en el Estatuto y en los Reglamentos.

Artículo 23.- Las sesiones de convocatoria del Directorio deben de hacerse con 15 días de anticipación e incluyendo la agenda. Las sesiones de convocatoria son ordinarias y extraordinarias. Las ordinarias se realizarán cada tres meses. Las extraordinarias cuando fueren convocadas por el Presidente o a petición de por lo menos el 40% de los miembros Académicos y de Investigación y Desarrollo Científico.

Artículo 24.- Para las sesiones del Directorio el quórum se establece con más de la mitad de los miembros Académicos y de Investigación y Desarrollo Científico. Toda

decisión contará con los votos a favor de la mayoría de los miembros presentes. En caso de empate, el Presidente tendrá voto dirimente.

Artículo 25.- De cada sesión del Directorio se dejará constancia en Acta, que será autenticada por el Presidente y por el Secretario que actuó.

En las actas constarán exclusivamente los nombres de los asistentes, las resoluciones tomadas y el número de votos a favor que tuvieron. No se dejará constancia de ninguna intervención personal, pero sí podrá solicitar cualquier miembro, que se agregue como documento anexo su opinión, que obligatoriamente entregará por escrito.

Artículo 26.- Del Presidente: será designado por el Directorios para un periodo de dos años y podrá ser reelegido una vez que todos los miembros del directorio hayan ocupado la presidencia

Artículo 27.- Son deberes y atribuciones del Presidente:

a) Convocar y presidir las reuniones del Directorio,

b) Convocar a los miembros del Directorio a sesión extraordinaria cuando lo estime conveniente o cuando lo soliciten por escrito el Directorio o cuando menos la tercera parte de los Miembros del Directorio

c) Asumir o encargar las funciones del Director Ejecutivo mientras dure la ausencia temporal del mismo o cuando lo considere necesario, con obligación de convocar, en este último caso, de inmediato al Directorio;

d) Promover el cumplimiento de los fines y misión del CEDIA.

e) Gestionar recursos financieros y tecnológicos, a favor del CEDIA

f) Promover las Comisiones permanentes del CEDIA.

g) Las demás que se señale en la Normativa del CEDIA.

Artículo 28.- Del Director Ejecutivo será designado por el Directorios para un periodo de dos años y podrá ser reelegido indefinidamente o removido de su cargo, si su desenvolvimiento así lo amerita.

Artículo 29.- Son deberes y atribuciones del Director Ejecutivo:

a) Representar legalmente al Consorcio en todo lo que haga relación con el cumplimiento a sus funciones.

b) Presentar a la aprobación del Directorio los Planes Estratégicos y Operativos Anuales y el presupuesto anual.

c) Presentar a la aprobación del Directorio las políticas financieras y presupuestarias del Consorcio, el informe de labores y los estados financieros

d) Abrir cuentas corrientes en los bancos y registrar las firmas conjuntamente con el Jefe Financiero.

e) Coordinar el ajuste de los planes estratégicos y operativos.

f) Tener a su cargo la administración del personal incluida su selección, contratación, remoción, fijación de remuneraciones y todos los demás aspectos relacionados con ella, debiendo someter al Directorio las políticas sobre esta materia.

g) Ejecutar el plan Estratégico Operativo.

h) Cumplir, hacer cumplir y coordinar las acciones entre los diferentes miembros del CEDIA para el cumplimiento de su misión, fines y ejecución de los reglamentos que le encomiende el Directorio.

i) Gestionar la obtención de recursos económicos ante personas naturales y jurídicas nacionales y extranjeras.

j) Presentar al Directorio las gestiones realizadas.

k) Ser miembro nato de las comisiones permanentes.

h) Presentar informes anuales al Directorio.

i) Las demás que se señale en la Normativa del CEDIA.

Artículo 30: El CEDIA tendrá tres comisiones permanentes:

a) La Comisión de membresías.

b) La Comisión para el Desarrollo de Aplicaciones

c) La Comisión Técnica para el desarrollo de la red.

La integración, funciones y más aspectos operativos de las comisiones constarán en el Reglamento que expida el Directorio.

CAPÍTULO IV

DEL PATRIMONIO

Artículo 31 .- El patrimonio del CEDIA estará integrado por:

(i) El fondo inicial equivalente a la cuota de inscripción de cada miembro, cuotas de membresía, y las cuotas anuales tanto de Miembros fundadores como de miembros estratégicos, las mismas establecidas en los reglamentos del CEDIA

(ii) Las donaciones, contribuciones, legados de personas naturales y jurídicas o privadas, sean éstas nacionales o internacionales;

(iii) Los bienes que en el futuro adquiera, a cualquier título;

(iv) Las asignaciones que recibiere del Estado y otros organismos de derecho público o privado, sean nacionales o extranjeros; y,

(v) El producto que obtuviere de sus actividades.

(vi) El fondo total que se constituirá con un aporte específico de sus miembros y que se nutrirá con recursos externos y con los excedentes de las actividades que ejecuta el CEDIA

Los bienes de la entidad no pertenecen en todo ni en parte a los miembros que

la componen.

Artículo 32.- Los recursos del CEDIA y los beneficios que se obtengan de su manejo financiero servirán para cubrir sus costos operacionales y sus inversiones en desarrollo. En caso de haber excedente pasarán al fondo total.

CAPÍTULO V

DE LA DISOLUCIÓN Y LIQUIDACIÓN

Artículo 33.- El CEDIA solamente podrá disolverse por decisión del Directorio, con el voto favorable del 80% de sus miembros, tomada en dos sesiones convocadas para el efecto, por no cumplir con sus finalidades y por las causas señaladas en la Ley.

Acordada la disolución del Consorcio, el Directorio procederá a nombrar un Comité de Liquidación compuesto de tres personas que elegirán un Presidente.

En caso de disolución, los bienes del CEDIA se distribuirá de manera igualitaria entre sus miembros académicos y de investigación y desarrollo.

Artículo 34.- Y todos los indicados en el Capítulo V de la Disolución y Liquidación del Reglamento de Personas jurídicas sin fines de Lucro, Acuerdo Ministerial N°608 / 86 de 29 de mayo del 2000

CAPÍTULO VI

DISPOSICIONES TRANSITORIAS

Artículo 35.- El CEDIA expedirá su reglamentación después del primer año de haberse aprobado sus Estatutos; en consecuencia, en su primer año de funciones, todos los aspectos no contemplado en el Estatuto serán normados por el Directorio mediante resoluciones e instructivos.

Artículo 36.- Se establece un monto de inscripción para todos los miembros fundadores de $3000,00 dólares, y a los miembros estratégicos un monto de $5000,00. Las Cuotas mensuales de membresías serán de XXXX,00 dólares.

Artículo 37.- El Directorio del CEDIA delega a la ESPOL la tramitación de todos los requisitos iniciales de conformación, así como la representación legal y el manejo de fondos hasta que el Directorio este conformado y sea capaz de elegir al Directorio inicial.

Artículo 38.- El Directorio del CEDIA podrá tomar resoluciones mediante consultas utilizando como medio las herramientas de tecnologías de la información.

DISPOSICIÓN GENERAL

Los miembros del CEDIA se podrán beneficiar de:

a) Participar en los proyectos conjuntos de nueva tecnología de información y

comunicación que se realizarían con universidades o empresas de tecnología del exterior afiliada a Internet2.

b) Tener prioridad en la selección de los proyectos que presenten las universidades ecuatorianas donde se privilegie la participación de dos o más instituciones y cuyos proyectos estén directamente relaciones con las áreas temáticas de los Asociados Institucionales.

c) Presentar candidatos para la selección de instructores de cursos formales de postgrado, seminarios o eventos de capacitación relacionados con la tecnología de comunicaciones y específicamente con Internet2.

d) Gozar de los descuentos que se otorgarán a los afiliados en los cursos formales o eventos de capacitación impartidos por el CEDIA.

e) Tener acceso a información de primera mano en el WEB que construirá el CEDIA, sobre el desarrollo de Internet2 en el país y de las noticias relevantes sobre Internet de la Nueva Generación a nivel mundial.

f) Participar en la selección de las instituciones que cumplan con los perfiles requeridos para interactuar en proyectos de nuevas tecnologías o innovadores con universidades del exterior.

g) Participar en los proyectos pilotos que se implementen sobre los nuevos procesos de enseñanza aplicados a la educación: virtual y a distancia.

h) Recomendar por parte del CEDIA a que las universidades nacionales puedan ser escogidas por parte de universidades del exterior para participar en proyectos conjuntos de interés común.

i) Hacer uso de la ley de propiedad intelectual, dentro de todos los productos desarrollados por las universidades que sean puestos a disposición para la red de Internet 2

j) Hacer uso de la ley de comercio electrónico, donde se tomará en cuenta únicamente los aspectos de seguridad de datos, éticas de proyectos, buen uso de la información y firmas electrónicas.

k) De otros beneficios que puedan crearse en el futuro para sus asociados.

La reforma aquí propuesta fue aceptada por unanimidad en reunión de directorio realizada en las instalaciones de la Universidad de Cuenca a los 23 días del mes de abril de 2009.

Para constancia firma.

Dr. Carlos Villie Morocho Zurita
Secretario
CEDIA

ASESORIA JURIDICA
CERTIFICO
Que esta copia
es igual a su Original
Quito, de 09 JUL. 2009 del 2.00

Apéndice D

TIA/EIA 568 B.3: NORMA DE FIBRA ÓPTICA

- INTRODUCCIÓN

La norma TIA/EIA B.3 especifica los requerimientos de fibra óptica usados en el cableado estructurado de telecomunicaciones en instituciones educativas, privadas y estatales.

TIA/EIA B.3 es una norma que se encuentra en constante revisión y actualización garantizando avances en la construcción de tecnologías de las telecomunicaciones.

- TERMINOLOGÍA

La terminología utilizada se detalla en la Tabla D1

Tabla D 1.

Terminología TIA/EIA-568-B.3

ÍTEM	SIGNIFICADO
Adaptador dúplex de fibra óptica	Dispositivo mecánico diseñado para alinear y unir dos fibras ópticas
Cable	Conjunto de uno o más conductores aislados o fibras ópticas, dentro de una envoltura o revestimiento
Envoltura del cable	Cubierta sobre la fibra óptica o conjunto conductor que puede incluir elementos metálicos
Punto de consolidación	Lugar para la interconexión entre los cables horizontales
Conector cruzado	Instalación que permite la terminación de elementos de cable y su interconexión
Conexión cruzada	Esquema de conexión entre tendido del cableado, subsistemas y equipo que utilizan cables o conectores que se conectan al hardware de conexión en cada extremo
Cable híbrido de fibra	Cable de fibra óptica que contiene dos o más

óptica	tipos de fibra (multimodo y monomodo)
Interconexión	Esquema que emplea la conexión de hardware para la conexión directa de un cable a otro cable
Incrustación	Es una característica mecánica de un sistema conector que garantiza la correcta orientación de una conexión, o impide la conexión a un conector, o para un adaptador de fibra óptica del mismo tipo utilizado para otro propósito
Link	Vía de transmisión entre dos puntos, sin incluir equipos terminales, cables de área de trabajo y cables de los equipos
Modo	Camino de luz en una fibra óptica
Fibra óptica	Cualquier filamento fabricado de materiales dieléctricos que la luz guías

- FIBRA OPTICA

La norma TIA/EIA B.3 contiene especificaciones de rendimiento del cable de fibra óptica que deben cumplir según la Tabla D2

Tabla D2.

Especificaciones de rendimiento

TIPO DE CABLE DE FIBRA ÓPTICA	LONGITUD DE ONDA	MÁXIMA ATENUACIÓN (DB/KM)	MÍNIMA INFORMACIÓN DEL LIMITE EN CAPACIDAD DE TRANSMISIÓN
50/125 µm multimodo	850	3.5	500
	1300	1.5	500
62.5/125 µm multimodo	850	3.5	160
	1300	1.5	500
Base interna cable monomodo	1310	1.0	N/A
	1550	1.0	N/A
Base externa cable monomodo	1310	0.5	N/A
	1550	0.5	N/A

Un cable de fibra óptica esta formado por 50/125 mm 0 62.5/125 mm hilos de fibra óptica monomodo, multimodo o en combinación de ambos. Las fibras ópticas antes mencionadas deben estar identificadas de acuerdo a ANSI/TIA/EIA-598-A.

- CABLE INTERNO DE FIBRA ÓPTICA

Las especificaciones del cable interno de fibra óptica se encuentran bajo la norma ANSI/ICEA S-83-596. Los cables 2 y 4 de fibra óptica destinados a poseer un radio de curvatura de 25 mm para el cableado horizontal. Los demás cables tendrán un radio de curvatura 10 veces el diámetro del cable exterior cuando no posea dependencia de carga de tensión y 15 veces el diámetro del cable exterior cuando posea dependencia de carga de tensión.

- CABLE EXTERNO DE FIBRA ÓPTICA

Las especificaciones del cable externo de fibra óptica se encuentran bajo la norma ANSI/ICEA S-87-640. A diferencia del cable interno de fibra óptica, el cable externo de fibra óptica debe cumplir con requerimientos de protección en el medio donde se encuentra. El cable expuesto requiere de una resistencia a la tracción mínima de 2670 (600 lb). Estos cables también poseen un radio de curvatura de 10 veces el diámetro del cable exterior cuando no posea dependencia de carga de tensión y 20 veces el diámetro del cable exterior cuando posea dependencia de carga de tensión.

- HARDWARE DE CONEXIÓN

El hardware de conexión usado son conectores de fibra óptica y empalmes, aplicados a conexiones: cruzada principal, cruzada intermedia,

cruzada horizontal y área de trabajo. Existen variedad de conectores ópticos que se utilizan de acuerdo a los requerimientos básicos del cableado estructurado de fibra óptica.

El hardware de conexión es diseñado para proporcionar flexibilidad en el montaje en paredes y racks. Además de brindar facilidad en gestión del cable durante la instalación.

Para el cableado centralizado el hardware de conexión de fibra óptica utilizado para unir cables horizontales esta diseñado para:

→ Proporcionar un medio de unión entre las fibras del backbone y cables horizontales

→ Proporcionar tecnología de unión para gestionar fibras individuales como pares de fibra

→ Proporcionar un medio para almacenamiento e identificación a fibras no conectadas dentro del backbone

→ Permitir eliminar las actuales conexiones horizontales y añadir nuevas conexiones horizontales

→ Proporcionar un medio de acceso para pruebas del cableado de fibra óptica

→ Proporcionar protección a las conexiones apropiada contra el contacto accidental de objetos extraños.

- CONECTOR IDENTIFICATIVO

El conector monomodo posee un identificativo (una parte visible del conector) de color azul y para el conector multimodo posee un identificativo (una parte visible del conector) de color beige.

- ETQUETADO

El etiquetado en el cableado de fibra óptica se muestra en la Figura C.1 en donde indica la ubicación de un conector 568Sc y el adaptador 568SC el cual realiza un cruce por pares entre los conectores.

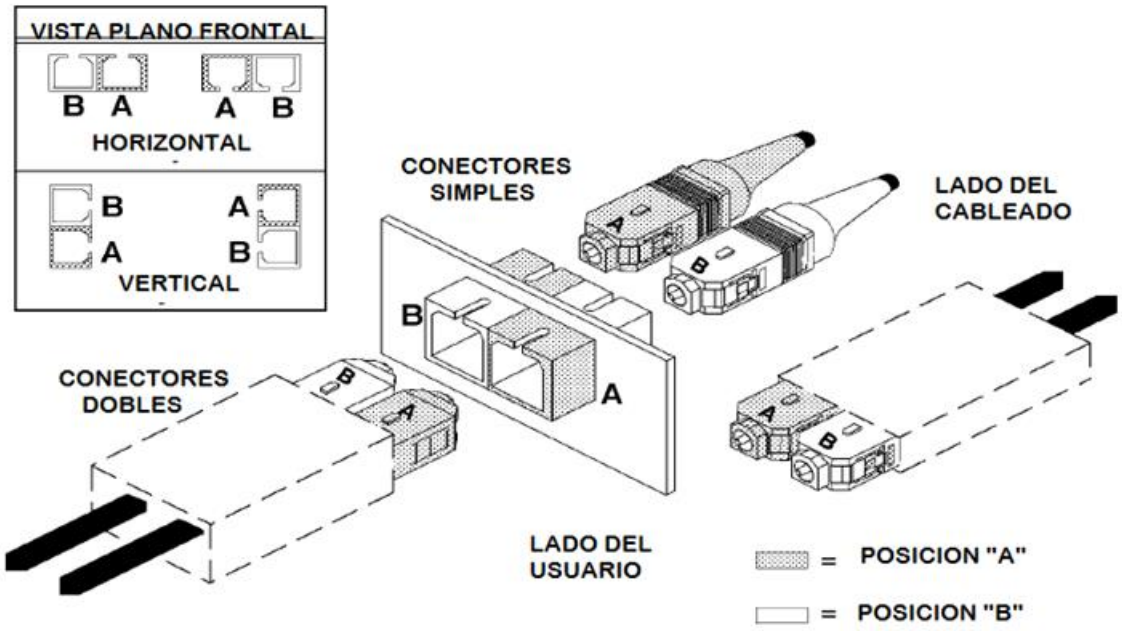


Figura D 1. Configuración de conector y adaptador 568SC.

Fuente: http://www.docstoc.com/documents/most-recent

En el diseño del panel de fibra óptica se considera lo siguiente:

→ Medios de conexión cruzada de cableado

→ Medios para interconectar equipos en las instalaciones del cableado de fibra óptica

→ Medios para identificar el cableado para administración conforme a la norma ANSI/TIA/EIA-606

→ Medios de manipulación de cables de fibra óptica y cables de red promoviendo una gestión adecuada

→ Medios de acceso para monitorear el cableado de fibra óptica, instalaciones y equipos

→ Medios de protección adecuados para conectores y adaptadores dentro del cableado contra el contacto accidental con objetos que degraden temporal o permanente.

La caja de salida de telecomunicaciones debe tener la capacidad de brindar alojamiento a terminaciones en fibra óptica, proporcionando una curvatura para la fibra óptica mínima de 25 mm.

- PATCH CORDS

Patch cords son cables de conexión utilizados para conectar enlaces de fibra óptica como equipos de trabajo, conexiones cruzadas y para conectar equipos dentro del backbone; aplicando la configuración de conectores como indicia la Figura D1.

Apéndice E

SOPORTE DE IPv6 EN EQUIPOS DE RED DE FACULTADES UTN

Tabla E1

Características Switch 4566-E

EQUIPO	CARACTERÍSTICAS
Switch 4566-E	Nuevas funciones del software: IPv6 software de conmutación Comunidad VLAN privada (PVLAN) Switched Puerto Analyzer (SPAN) lista de control de acceso filtrado (ACL) DHCP configuración automática del cliente Mejorado Protocolo Simple de Administrador de Red (SNMP) MIB

Tabla E2

Características Switch 3COM 5500G

EQUIPO	CARACTERÍSTICAS
Switch 3COM 5500G	Basado en estándares de conmutación y funciones de administración para proporcionar una solución de red que maximiza la inversión y apoya las nuevas normas. Integra funciones de administración de IPv6, así como IPv6 filtrado de tráfico y la clasificación, prepara la red para el próximo generación de la versión IPv6, manteniendo la plena compatibilidad con hoy en día es más común IPv4.

Tabla E3

Características Swicth LINSYS SRW2048

EQUIPO	CARACTERÍSTICAS
Swicth LINSYS SRW2048	Calidad de servicio mediante las siguientes clases de servicios: 802.1p VLAN VLAN ID Direcciones MAC Direcciones IP Tipo de Servicio Trafico IPv6 basado en clases de servicio

Apéndice F

MANUAL DE ADMINISTRADOR CONFIGURACIÓN IPv6 EN RED DE DATOS UTN

Manual de Administrador Configuración DUAL STACK en UTN

Sayra Espinosa

Contenido

Índice de Figuras

1. Introducción

El presente manual de administrador expone el proceso de configuración del protocolo de Internet versión 6 (IPv6) orientado al entorno externo que posee la red de datos de la Universidad Técnica del Norte.

La red de datos UTN actualmente opera sobre el protocolo de Internet versión 4 (IPv4), para llegar a trabajar con IPv6 es necesario que exista un proceso denominado transición que indica el mecanismo utilizado para que los dos protocolos funcionen adecuadamente.

2. Dual Stack Mecanismo de Transición

Dual Stack o Doble Pila es el mecanismo de transición en el cual cada versión de protocolo de Internet funciona independientemente dentro de la red, llegando a ser transparente para el usuario final.

La configuración de Dual Stack aplicado en la red UTN se realiza en los siguientes equipos de red: routers, switchs y hosts (configuración en hosts opcional por la ventaja de autoconfiguración de dirección en IPv6).

3. Metodología utilizada

La metodología utilizada hacia la transición al protocolo de Internet versión 6 se basa desde el punto de vista de red y en conjunto con el mecanismo de transición seleccionado se configura siguiendo el proceso jerárquico que se encuentran los equipos en UTN:

a) Router 7304 (TELCONET)
b) Firewall CISCO ASA 5520
c) Siwtchs CISCO 3750
d) Host (opcional)

4. Descripción de configuraciones del entorno externo con IPv4 en UTN

La red de datos del entorno externo que posee la UTN esta conformada de los siguientes equipos: Router 7604, Firewall CISCO ASA 5520, Switch CISCO 3750.

4.1. Configuraciones Router 7604

Las configuraciones existentes en el router 7604 de la institución son realizadas por parte del personal técnico de TELCONET y no se tiene acceso a las mismas.

4.2. Configuraciones Firewall CISCO ASA 5520

Las configuraciones que se muestran a continuación fueron realizadas bajo líneas de consola (comandos), ingresados desde el software ZOC, el acceso en base a SSH como indica la Figura 1.

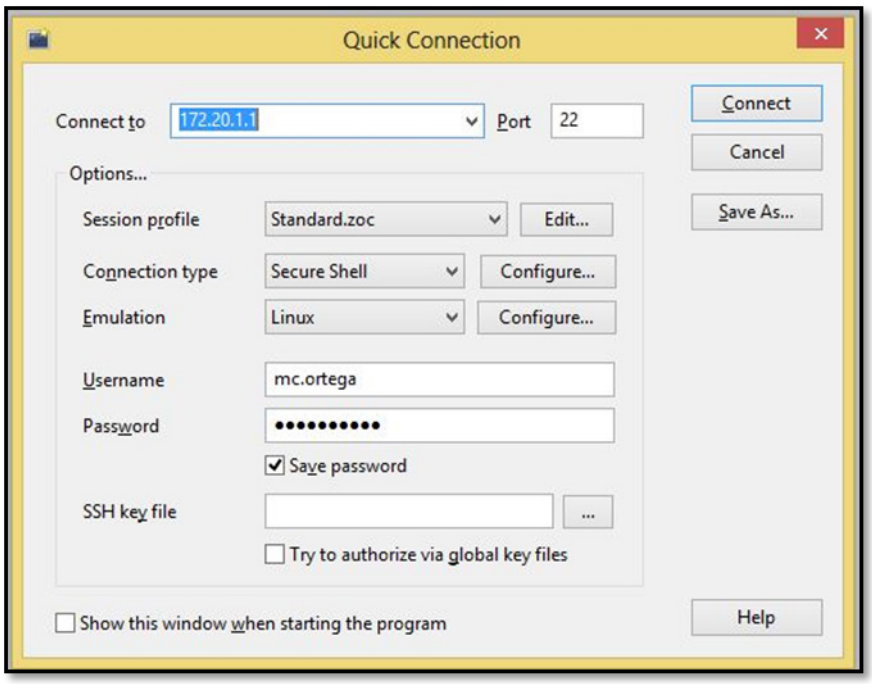


Figura1. Acceso a Firewall ASA 5520

Al dar click en connect, aparece la pantalla de configuración de firewall, se necesita ingresar el usuario y contraseña
firewall>

Se sitúa en modo de configuración privilegiado para pasar a modo de configuración global se escribe
firewall>enable

Solicita nuevamente contraseña y se tiene la siguiente línea de comando
firewall#

En este modo de configuración global se pueden realizar las configuraciones referentes a interfaces.

firewall#configure terminal

La interfaz del firewall que se configura es GigabitEthernet0/0 interfaz de salida en el mismo modo de configuración global se escribe:
firewall(config)#interface GigabitEthernet0/0

Para la configuración en IPv6 es necesario activar con el siguiente comando
firewall(config-if)#ipv6 enable

Se ingresa a la interfaz y se puede establecer la dirección IPv4 e IPv6
firewall(config-if)#ip address 190.95.196.194 255.255.255.224
firewall(config-if)#ipv6 address 2800:68:19::2/64
firewall(config-if)#exit

Se realiza la misma configuración para la interfaz GigabitEthernet0/1 interfaz de entrada
firewall#configure terminal
firewall(config)#interface GigabitEthernet0/1
firewall(config-if)#ipv6 enable
firewall(config-if)#ip address 172.20.1.1 255.255.255.0
firewall(config-if)#ipv6 address 2800:68:19:1::2/64
firewall(config-if)#exit

De igual manera la configuración para la interfaz GigabitEthernet0/1 interfaz DMZ
firewall#configure terminal
firewall(config)#interface GigabitEthernet0/2
firewall(config-if)#ipv6 enable
firewall(config-if)#ip address 10.24.8.1 255.255.255.0
firewall(config-if)#ipv6 address 2800:68:19:2408::6/64
firewall(config-if)#exit

4.3. Switch CISCO 3750

Las configuraciones que se muestran a continuación fueron realizadas bajo líneas de consola (comandos). El ingreso se realiza remotamente desde el programa Putty con la dirección del Switch CISCO 3750 por el puerto 23 Telnet (Figura 2).

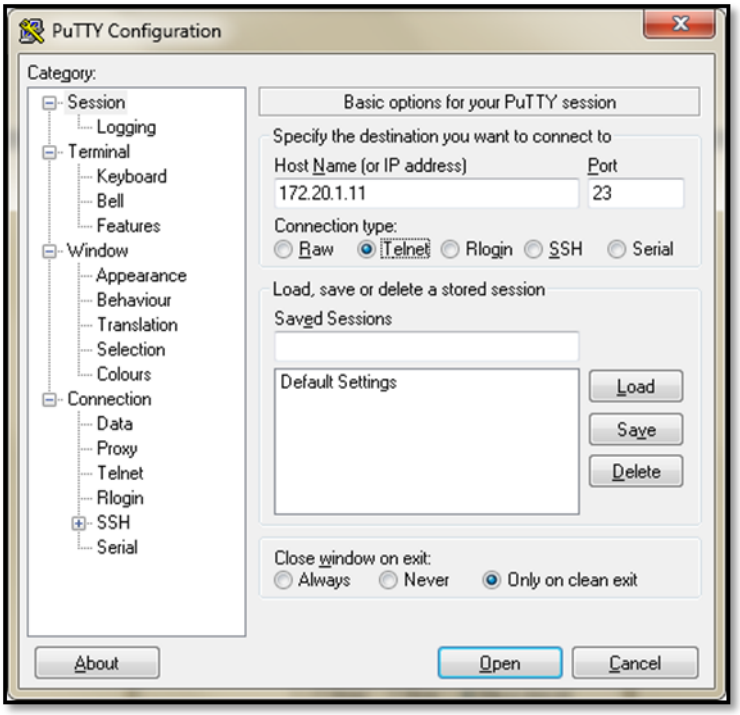


Figura2. Acceso a switch por Telnet

Aparece la pantalla inicial de switch, se necesita ingresar el usuario y contraseña (Figura 3)

Figura3. Interfaz en línea de comandos en switch

Se sitúa en modo de configuración privilegiado para pasar a modo de configuración global se escribe
SW_CORECENTRAL>enable

Solicita nuevamente contraseña y se tiene la siguiente línea de comando (configuración global)
SW_CORECENTRAL#

En este modo de configuración global se pueden realizar las configuraciones referentes a VLANs:
SW_CORECENTRAL#configure terminal

Para la configuración en IPv6 es necesario activar con el siguiente comando
SW_CORECENTRAL(config)#ipv6 enable

Como las VLANs IPv4 ya están creadas y asignadas a sus respectivos puertos, accedemos a la VLANs para configurar la dirección en IPv6, la VLAN 1 corresponde a Servidores:
SW_CORECENTRAL(config)#interface vlan 1
SW_CORECENTRAL(config-if)#ip address 172.20.1.11 255.255.255.0

En la misma interfaz se escribe la dirección IPv6:

SW_CORECENTRAL(config-if)#ipv6 address 2800:68:19:1::1/64
SW_CORECENTRAL(config-if)#exit

Para la VLAN 6 que corresponde al Departamento de Informática, es el siguiente proceso:

En este modo de configuración global se pueden realizar las configuraciones referentes a VLANs:
SW_CORECENTRAL#configure terminal

Para la configuración en IPv6 es necesario activar con el siguiente comando
SW_CORECENTRAL(config)#ipv6 enable

Como las VLANs IPv4 ya están creadas y asignadas a sus respectivos puertos, accedemos a la VLANs para configurar la dirección en IPv6, la VLAN 6:
SW_CORECENTRAL(config)#interface vlan 6
SW_CORECENTRAL(config-if)#ip address 172.20.6.2 255.255.255.0

En la misma interfaz se escribe la dirección IPv6:

SW_CORECENTRAL(config-if)#ipv6 address 2800:68:19:6::1/64
SW_CORECENTRAL(config-if)#exit

5. Pruebas de conectividad

Se realizan pruebas de conectividad en cada equipo para verificar que las configuraciones se realizaron correctamente en base al protocolo de control de mensajes de Internet ICMP, este protocolo responderá con un mensaje informando el estado de conectividad, las direcciones de cada interfaz se observa en la Figura 4. Como la red actual funciona con normalidad sobre IPv4, las pruebas se centran solo en IPv6.

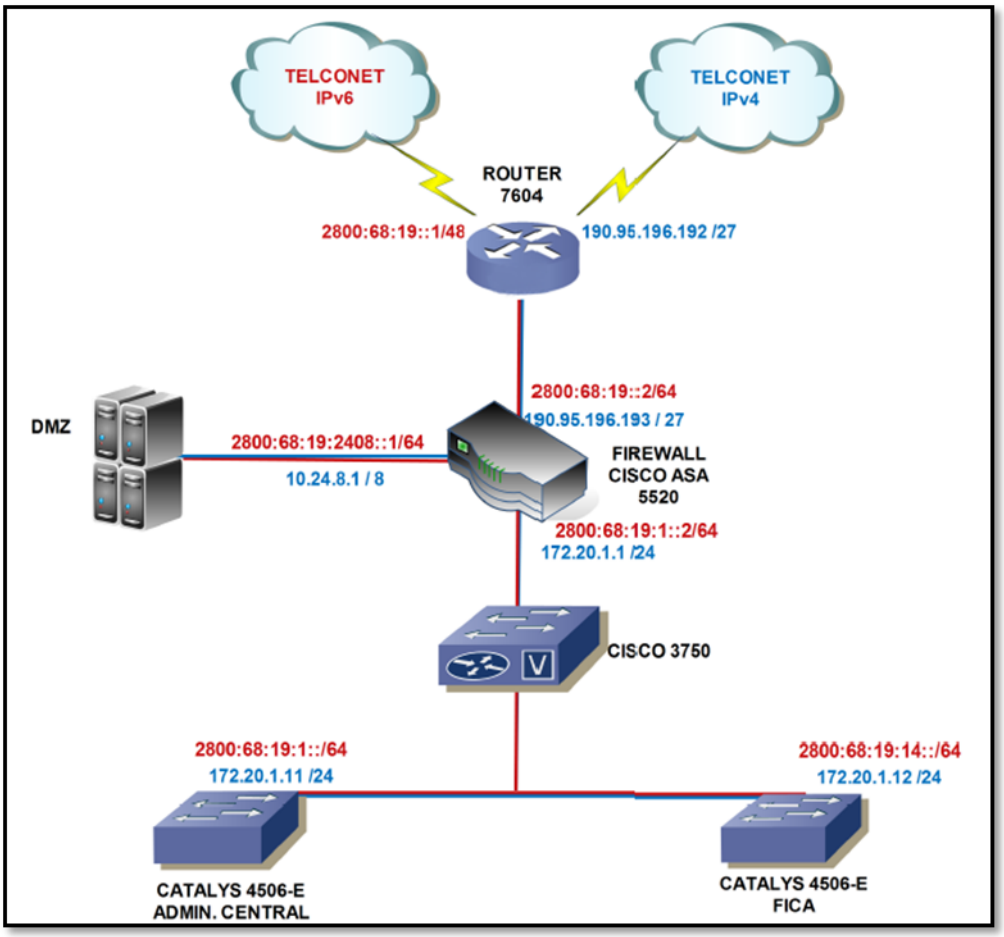


Figura4. Red Dual Stack UTN

→ Prueba de conectividad desde Firewall hacia interfaz de entrada Firewall dirección IPv6 2800:68:19:1::2.

firewall# ping 2800:68:19:1::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:19:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

→ Prueba de conectividad desde Firewall hacia interfaz de salida Firewall dirección IPv6 2800:68:19::2.

firewall# ping 2800:68:19::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:19::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

→ Prueba de conectividad desde Firewall hacia puerta de enlace de router 7604 dirección IPv6 2800:68:19::1.

firewall# ping 2800:68:19::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:68:19::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

Las pruebas a continuación son realizadas desde un host situado en el Departamento de Informática, el host tiene configurado la dirección estática IPv6 2800:68:19:6::136 y se basan en accesos a sitios web que poseen IPv6, este acceso se puede verificar en el navegador Mozilla Firefox al ejecutar el complemento “show ip” este complemento muestra la respuesta de dirección que el sitio esta trabajando. La dirección se sitúa en el inferior derecho del navegador en color verde.

→ Prueba de conectividad desde host situado en el Departamento de Informática hacia pagina inicial de Google en IPv6 ipv6.google.com (Figura 5).

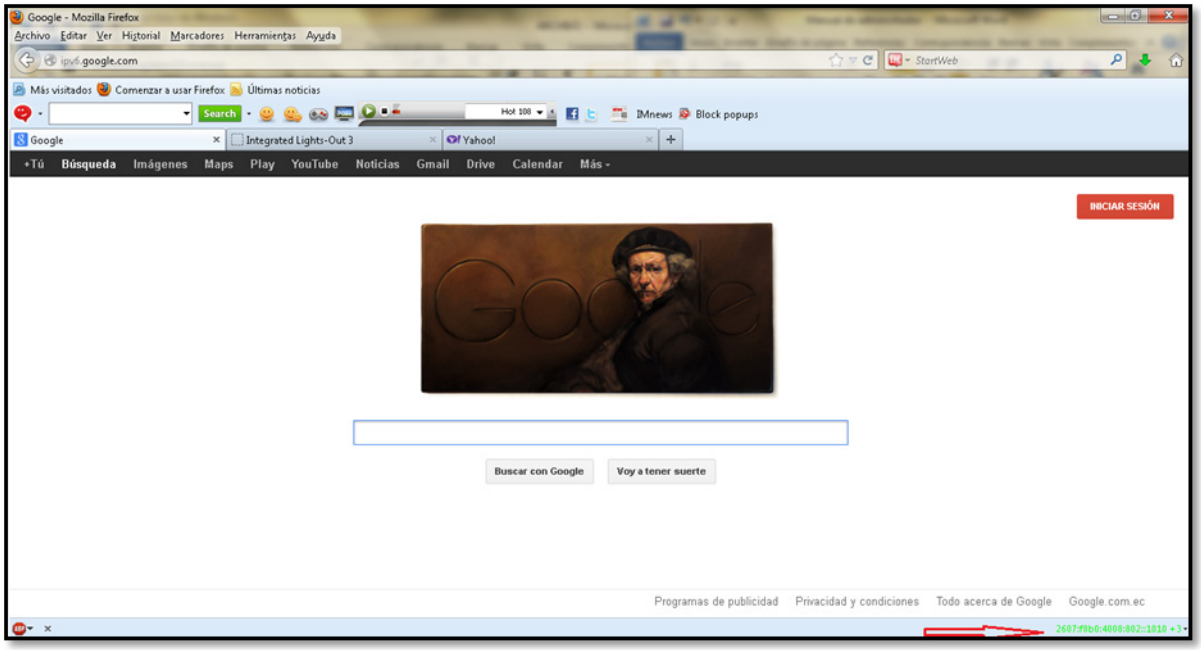


Figura5. Página google con IPv6

→ Prueba de conectividad desde host situado en el Departamento de Informática hacia página inicial www.facebook.com (Figura 6).

Figura6. Página facebook con IPv6

→ Prueba de conectividad desde host situado en el Departamento de Informática hacia pagina inicial www.yahoo.com (Figura 7).

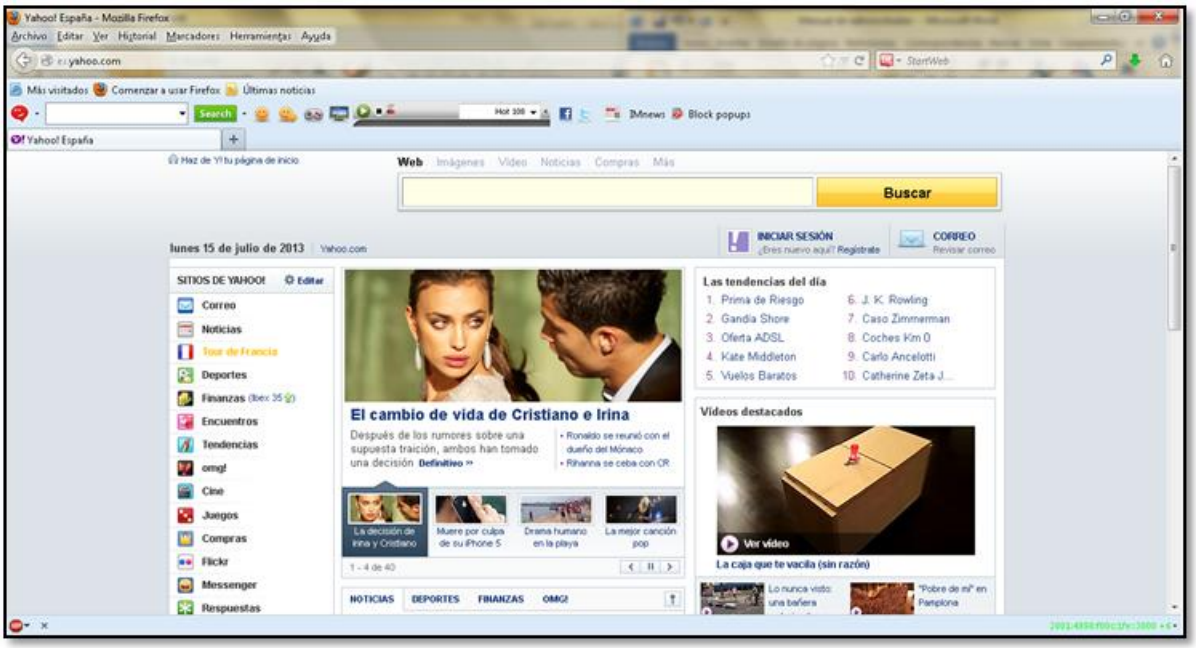


Figura7. Página facebook con IPv6

6. Resultados de configuraciones

Desde una maquina situado en el Departamento de Informática UTN se realiza un test para verificación de conectividad de IPv6, ingresando en la URL: *http://test-ipv6.com/* (Figura 8 y 9).

Figura8. Conectividad IPv6