UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE

DEPARTAMENTO DE INGENIERIA Y ARQUITECTURA

TRABAJO DE GRADO

"DISEÑO DE UN PROTOTIPO DE IMPLEMENTACIÓN DEL PROTOCOLO IPv6 EN LA RED DE LA UNIVERSIDAD DE EL SALVADOR FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE"

PRESENTADO POR:

FIGUEROA JIMÉNEZ, CARLOS ENRIQUE
MARROQUÍN ARGUETA, HÉCTOR OSWALDO
MARTÍNEZ MONTERROSA, RICARDO ENRIQUE

PARA OPTAR AL GRADO DE:

INGENIERO DE SISTEMAS INFORMATICOS

DOCENTE DIRECTOR:

ING. JUAN CARLOS PEÑA MORAN

11 DE OCTUBRE DE 2011

SANTA ANA EL SALVADOR CENTROAMERICA

UNIVERSIDAD DE EL SALVADOR

AUTORIDADES

RECTOR

INGENIERO Y MASTER RUFINO ANTONIO QUEZADA SÁNCHEZ

VICE-RECTOR ACADÉMICO

MASTER MIGUEL ÁNGEL PÉREZ RAMOS

VICE-RECTOR ADMINISTRATIVO

MASTER ÓSCAR NOÉ NAVARRETE

SECRETARIO GENERAL

LICENCIADO DOUGLAS VLADIMIR ALFARO CHÁVEZ

FISCAL GENERAL

LICENCIADO RENE MADECADEL PERLA JIMÉNEZ

UNIVERSIDAD DE EL SALVADOR

FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE

AUTORIDADES

DECANO

LICENCIADO JORGE MAURICIO RIVERA

VICE-DECANO

MASTER ELADIO EFRAÍN ZACARÍAS ORTEZ

SECRETARIO

LICENCIADO VÍCTOR HUGO MERINO QUEZADA

Agradecimientos

A Dios todo poderoso, por darnos la sabiduría necesaria para tomar las decisiones correctas, por darnos fuerzas para afrontar los problemas, por las bendiciones derramadas sobre nosotros y por estar a nuestro lado en todo momento.

A nuestras familias:
FIGUEROA JIMÉNEZ, MARROQUÍN ARGUETA Y MARTÍNEZ MONTERROSA; por habernos motivado y apoyado durante el transcurso de toda la carrera, por todo el amor y confianza depositado en nosotros.

A nuestro director de tesis:
Ing. Juan Carlos Peña Moran; Por toda su ayuda, consejos y observaciones en el transcurso de este proyecto y por motivarnos a superarnos personal y académicamente.

A todos nuestros amigos:
Que nos acompañaron en el desarrollo de toda nuestra carrera, por su apoyo, amistad y momentos compartidos que brindaron las fuerzas en los momentos necesarios.

Nuestros más sinceros agradecimientos:

Carlos Figueroa, Héctor Marroquín y Ricardo Martínez.

Índice General

Índice de Figuras

Índice de Tablas

Introducción

Los protocolos son una parte fundamental del software en la telecomunicación a través de Internet, éstos hacen posible que las aplicaciones instaladas en los dispositivos puedan comunicarse con otras en la red. En el mundo del internet se utiliza el conjunto de protocolos TCP/IP, dentro de este grupo de protocolos se encuentra uno en específico denominado Protocolo de Internet (IP por sus siglas en inglés), utilizado ampliamente entre los dispositivos de origen y destino de la red.

En la actualidad la versión comúnmente utilizada del protocolo IP es la versión cuatro (IPv4), sin embargo, recientemente se ha dado a conocer que las direcciones generadas mediante el protocolo IPv4 están por agotarse, considerando la demanda actual de los usuarios del internet que sigue creciendo constantemente. Por ello desde hace algún tiempo se vienen estudiando diversas soluciones al problema de agotamiento propiciado por la versión 4 de IP, una de las soluciones que se viene desarrollando es la creación de una versión más avanzada, es decir el Protocolo de Internet

versión 6 (IPv6), que dará solución al problema de la cantidad disponible de direcciones IP públicas y otras deficiencias de la versión 4.

Puesto que es inminente la necesidad de iniciar la utilización del protocolo IPv6 para la comunicación entre los usuarios de la red y considerando que las dos versiones mencionadas no son compatibles entre sí, la Universidad de El Salvador Facultad Multidisciplinaria de Occidente tendrá que adaptar tarde o temprano su tecnología a dicha situación, por lo que se desarrolla el proyecto "DISEÑO DE UN PROTOTIPO DE IMPLEMENTACIÓN DEL PROTOCOLO IPv6 EN LA RED DE LA UNIVERSIDAD DE EL SALVADOR FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE", como un aporte a esta institución, otorgándole una guía previa y sugerencias concretas que sean de utilidad al momento de dar el paso hacia la nueva versión de IP.

En el presente documento se explica brevemente las causas y necesidades de desarrollar el proyecto mencionado, los objetivos que se persigue alcanzar mediante el mismo, así como los alcances y limitantes dentro de los cuales se realizó este estudio. Puede encontrarse también el detalle de

la metodología utilizada durante la ejecución del proyecto, que permitió de una manera sistemática obtener los objetivos previamente establecidos. Además, se detalla la metodología diseñada para la evaluación y selección de la técnica de transición que mejor se apegue a las necesidades de una empresa o institución en particular y la forma de cómo ejecutarla.

Objetivos

General

Diseñar una metodología que permita elegir entre las técnicas conocidas y recomendadas de implementación del protocolo IPv6 en la infraestructura de red de la Universidad de El Salvador Facultad Multidisciplinaria de Occidente, de tal manera que la institución pueda aprovechar dicha metodología para escoger la mejor opción que permita la convergencia entre los protocolos IPv6 e IPv4, mientras se lleve a cabo la implementación del protocolo IPv6.

Específicos:

- Identificar los requerimientos de hardware y software necesarios para que la institución pueda implementar el protocolo IPv6 mediante el análisis del equipo con que cuenta actualmente la Universidad de El Salvador Facultad Multidisciplinaria de Occidente.

- Examinar las técnicas de transición entre los protocolos IPv4 e IPv6, mediante el estudio de un grupo de indicadores cualitativos que serán determinados en base a los requerimientos y capacidades de la entidad a la cual se le esté realizando dicho estudio.

- Diseñar prototipos en base a los resultados arrojados por la metodología de selección de técnicas de transición, que permitan verificar la fiabilidad de dichos resultados mostrando la técnica de transición entre los protocolos IPv4 e IPv6 de mayor factibilidad, para que pueda ser utilizado por la Universidad de El Salvador Facultad Multidisciplinaria de Occidente, en el momento que ésta lo necesite.

- Establecer información que sea de utilidad para la implementación del protocolo IPv6 en la Universidad de El Salvador Facultad Multidisciplinaria de Occidente, mediante la documentación de los procesos de selección que ayuden a la implementación de dicho protocolo (IPv6).

Justificación

Poco a poco, la necesidad por adentrarse al mundo de IPv6 se está volviendo mayor, esto no viene de un par de años atrás sino ya más de una década, sin embargo el poco interés por parte de las instituciones, ha hecho que esta realidad no haya sido tomada con la importancia adecuada.

El agotamiento de las reservas de direcciones IP en los Proveedores de Servicio de Internet (ISP por sus siglas en inglés) es evidente, para contrarrestarlo dichas instituciones han pensado respaldarse en tecnologías como NAT (Traducción de Direcciones de Red), pero expertos en el tema recomiendan el uso de medidas a largo plazo. Las organizaciones dedicadas a la enseñanza, desarrollo e investigación, se caracterizan por explorar y experimentar con los nuevos protocolos y tecnologías de red, tanto en su calidad de promotoras de ciencia y desarrollo educativo, como en su calidad de usuaria directa de esta tecnología, tal es el caso de la Universidad de El Salvador Facultad Multidisciplinaria de Occidente.

Reconociendo que las nuevas tecnologías de redes serán orientadas a IPv6, la Universidad de El Salvador Facultad Multidisciplinaria de Occidente, debe prever esto y anticiparse para no quedar desfasada y perder las mejoras y nuevos servicios que IPv6 brinda, esto ofrece la ventaja de poder trabajar en el cambio de sus servicios que no soporten IPv6 evitando interrupciones de los mismos. También le evita el tener que comprar equipos y servicios apresuradamente de una forma obligatoria al tener la necesidad de desplegar IPv6 en la red de la institución.

Es así como se desarrolla el proyecto denominado "DISEÑO DE UN PROTOTIPO DE IMPLEMENTACIÓN DEL PROTOCOLO IPv6 EN LA RED DE LA UNIVERSIDAD DE EL SALVADOR FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE". Dicho proyecto se enfoca en la manera de lograr una comunicación entre los protocolos IPv4 e IPv6, contando con servicios desplegados para clientes de ambos protocolos y a la vez, tener acceso tanto a sitios externos desplegados en cualquiera de los protocolos mencionados anteriormente (considerando que la institución brinda el servicio de acceso a Internet a todos sus clientes, estudiantes y personal universitario) mientras el resto del

mundo va migrándose a la nueva tecnología y así no carecer de los servicios que ambas implementaciones ofrecen.

Durante el desarrollo del proyecto se estudia a detalle las técnicas de transición existentes más conocidas y recomendadas para llevar a cabo la implementación del protocolo IPv6, identificando el más adecuado para aplicar en la Universidad de El Salvador Facultad Multidisciplinaria de Occidente, de acuerdo a los factores considerados en este proyecto.

Llegará el momento en el que el avance tecnológico obligue a las instituciones y usuarios particulares a migrar a IPv6, para poder tener acceso a sus servicios. Al realizar este proyecto se pretende preparar a la Universidad de El Salvador Facultad Multidisciplinaria de Occidente, de manera oportuna para esa necesidad ya prevista.

Alcances

- El desarrollo de este proyecto consta de una investigación documental en la que se detallan las características y funciones de los protocolos de Internet (IP) en sus versiones 4 y 6, comparándolos y resaltando las ventajas y desventajas entre ellos.

- Analizar la infraestructura de red con que cuenta la Universidad de El Salvador Facultad Multidisciplinaria de Occidente, comprendido en esto su topología, protocolos utilizados, servicios desplegados y equipo, con el fin de identificar la capacidad de los mismos para el soporte y la implementación del protocolo IPv6, presentando propuestas de cambios en la infraestructura en caso sean necesarios.

- Elaboración de una metodología que detalle los requerimientos, procesos y recomendaciones para la implementación del nuevo protocolo de comunicación en la red de la institución.

- Diseño de prototipos que permitan seleccionar mediante una comparación basada en indicadores cualitativos previamente definidos, la técnica de transición óptima para que la Universidad de El Salvador Facultad Multidisciplinaria de Occidente pueda implementar el protocolo IPv6.

Limitantes

- La dificultad que representa el alto costo de acceder a equipo de red que proporcione el soporte necesario para realizar las pruebas de desarrollo de los prototipos sobre el protocolo IPv6.

- Acceso limitado a información sobre despliegues IPv6 por parte de los proveedores de servicios de internet.

- Dada la naturaleza del proyecto, la cual es de carácter investigativo y con el cual se crean prototipos a escala y no una implementación del protocolo IPv6 en la red de la institución, no se realiza una Factibilidad Económica para dicho fin.

Capítulo I

Antecedentes

El Internet hoy en día se ha vuelto más que un lujo, una necesidad, llegando a tener una demanda tan grande que probablemente ni sus mismos creadores tuvieron la visión para anticipar su gigantesco crecimiento o darle la importancia debida al tema.

Los protocolos son una parte fundamental del software en la telecomunicación a través de Internet, éstos hacen posible que las aplicaciones instaladas en los dispositivos puedan comunicarse con otras a través de la red.

En el mundo del Internet se utiliza el conjunto de protocolos TCP/IP, que hacen posible la comunicación entre equipos (computadoras, celulares, etc.) a través de la red, aun sin importar la arquitectura interna de los mismos.

Dentro de este grupo de protocolos se encuentra uno denominado Protocolo de Internet (IP por sus siglas en

inglés) que es utilizado, tanto por el equipo origen y el equipo destino en una red, para la comunicación de los datos.

Actualmente la versión del protocolo IP comúnmente utilizada es la versión cuatro (IPv4), siendo una de sus características la creación de direcciones con un tamaño de 32bits, aproximadamente unos cuatro mil millones de direcciones. Aun siendo este un número alto, con las exigencias del mercado actual no son suficientes.

Con anticipación se predijo el suceso de agotamiento de las direcciones IP, de esta manera el Grupo de Tareas sobre Ingeniería de Internet (IETF por sus siglas en inglés) comenzó con la tarea de darle seguimiento a esta situación, resultando la creación de un equipo de trabajo enfocado en la creación del nuevo protocolo denominado IPv6, el cual corrige la mayoría de problemas que posee IPv4 y aumenta el tamaño de las direcciones IP a un espacio de 128 bits teniendo la capacidad de crear un numero de direcciones IP igual a 2 elevado a la 128 (RFC 2460).

Esta tecnología (IPv6) lleva muchos años de desarrollo y estudio (desde principios de los 90´s), lastimosamente aunque muchas autoridades e instituciones reguladoras como la Corporación para Números y Nombres Asignados (ICANN por sus siglas en inglés) lo han advertido y recomendado en base a estudios que se debe comenzar con un proceso de migración de IPv4 a IPv6, pocas organizaciones lo están haciendo, al igual que pocas personas se están preparando para el soporte e implementación de esta nueva tecnología.

Cabe mencionar que ambos protocolos no son compatibles entre sí, no puede comunicarse directamente un equipo que maneje IPv4 con uno sobre IPv6, por ello la necesidad de realizar una migración de protocolos o en todo caso, un medio de intercomunicación para que ambos puedan comunicarse.

Dentro de la Universidad de El Salvador, el estudio sobre el protocolo IPv6 ha sido poco desarrollado, los antecedentes encontrados son los siguientes:

- El 14 de diciembre de 2005, justo diez años después de que El Salvador se conectara en forma directa a

Internet, se logró la conexión a la Red Avanzada Mundial, conocida en algunos países como Internet 2. La Universidad de El Salvador es miembro de RAICES (por sus siglas: Red Avanzada de Investigación, Ciencia y Educación Salvadoreña) que es la organización que da apoyo a las actividades de educación, investigación e innovación en el área de tecnologías de comunicación mediante el uso de Internet 2. Para tener acceso a dicha red, la institución miembro de RAICES debe cumplir con ciertos requisitos: se debe tener una conexión a redClara (Cooperación Latinoamericana de Redes Avanzadas), además debe utilizarse el protocolo IPv6 para la comunicación con Internet 2; la Universidad de El Salvador siendo una de las instituciones de educación superior con mayor importancia en el país y siendo miembro de la organización RAICES, tuvo que realizar cambios en su infraestructura de red incluyendo la implementación de una red IPv6 para dar soporte a las conexiones con Internet 2, además de la contratación de servicios avanzados de redes como lo son el Clear Channel para lograr la conexión por IPv6 (Anexo 1).

- (Barrera Mancía, Henríquez Campos, & Tutila Hernández, 2007) Este trabajo de grado se enfoca en las diferentes técnicas de ruteo que pueden ser utilizadas con el protocolo en estudio y las configuraciones necesarias para su implementación.

Planteamiento del Problema

La Universidad de El Salvador cuenta con muchos servicios, desplegados tanto en el Internet como en la red interna de la institución, con el objetivo de que estén a disposición de la comunidad universitaria y de los empleados que laboran en la Universidad.

En el protocolo IPv4 se han encontrado muchos problemas, como por ejemplo la forma en que procesa los datos sobrecargando los equipos de la red, la dificultad en la implementación de mecanismos de seguridad en la conectividad, entre otros, pero el más destacado de ellos es que las direcciones IP son limitadas, hay un número máximo que puede ser asignado dada la naturaleza con que se pensó en sus inicios.

Ya hace varios meses se viene especulando a nivel mundial sobre la asignación total de direcciones IP públicas, de lo cual se encarga ICANN, y justamente el 2 de Febrero de 2011 fueron asignados los últimos bloques de direcciones a los cinco Registros Regionales de Internet (RIR por sus siglas en inglés) en que se divide la red (África, América Anglosajona,

América Latina y el Caribe, Asia, Europa), es decir, ya solo falta que los ISP (Proveedores de Servicios de Internet) asignen estas direcciones en su región respectiva para que se acaben las direcciones restantes. Pero esto no significa que el Internet va a colapsar, simplemente no habrá más espacios de direcciones para todos los nuevos dispositivos y usuarios que las necesiten. Como respuesta a esta situación y otras deficiencias de IPv4 hace varios años se viene desarrollando otro protocolo llamado IPv6, el cual incorpora muchas mejoras y cambios comparado con su predecesor IPv4. Dentro de estas mejoras, se encuentra el límite de direcciones IP que el protocolo permite asignar, el cual es aproximadamente de 340 sextillones de direcciones (muy superior a los 4,294 millones de direcciones de IPv4).

A mediano o largo plazo, cuando los ISP agoten su reserva de direcciones IPv4 disponibles, los nuevos usuarios de Internet tendrían que empezar a utilizar el nuevo protocolo IPv6, lo que los dejaría incomunicados con los que aún tienen desplegado IPv4, siempre y cuando no posean un medio de traducción.

De forma particular, la Universidad de El Salvador también necesita de estos protocolos para mantener sus servicios funcionando en la red. Considerando todo lo anterior resulta de suma importancia proveer anticipadamente a la Universidad de El Salvador Facultad Multidisciplinaria de Occidente, de un estudio en el cual se analicen alternativas y sugiera una técnica de transición entre los protocolos IPv4 e IPv6 que sirvan para que los usuarios de ambos protocolos puedan acceder a los servicios de la institución mientras todos los usuarios se migran totalmente al protocolo IPv6.

Metodología de la Investigación

El desarrollo del proyecto denominado "DISEÑO DE UN PROTOTIPO DE IMPLEMENTACIÓN DEL PROTOCOLO IPv6 EN LA RED DE LA UNIVERSIDAD DE EL SALVADOR FACULTAD MULTIDISCIPLINARIA DE OCCIDENTE" se basó en la realización de un estudio comparativo entre diferentes técnicas de transición del protocolo IPv4 a IPv6 aplicables a la institución, dicho estudio pretende como resultado sugerir la mejor técnica que se adapte a la realidad y necesidades de la misma.

Metodológicamente, la ejecución del proyecto puede resumirse en cuatro grandes etapas, desarrolladas sistemáticamente para alcanzar los objetivos deseados, dichas etapas son las siguientes:

1. Etapa de Investigación Documental o Bibliográfica: Inicialmente se desarrolla la investigación documental, que representa la base sobre la cual se sustenta todo el marco teórico del proyecto, esto incluye antecedentes de los protocolos de comunicación objeto de estudio, actualidad y demás información relevante sobre los

mismos, así como aquella relativa a las técnicas de transición a comparar y la descripción de ellas. Toda la información obtenida durante esta etapa de desarrollo del proyecto representan también la base para las comparaciones realizadas entre las alternativas seleccionadas y las conclusiones finales. La información documental que sustenta el proyecto es obtenida a través de revisiones a la bibliografía relacionada disponible, información disponible en internet y otras fuentes documental relevantes como revistas, artículos especializados, etc.

2. Etapa de Investigación de Campo: Otra de las etapas de desarrollo en la ejecución del proyecto es la investigación de campo, en la cual es obtenida toda la información acerca de las condiciones o situación actual del protocolo de comunicación utilizado en la Universidad de El Salvador Facultad Multidisciplinaria de Occidente, desde su infraestructura, topología y equipo, hasta las variables de mayor prioridad a la hora de evaluar las técnicas de transición comparadas y el nuevo equipo sugerido de ser necesario. En esta fase

también se debe investigar diferentes proveedores de equipo y servicios tecnológicos, con el fin de conocer las ofertas disponibles en el país y sus respectivas cotizaciones, lo cual ayudará a comparar las técnicas y sugerir una propuesta.

La información de campo es obtenida principalmente mediante la utilización de los siguientes métodos e instrumentos:

- Entrevista; utilizada para recolectar la información obtenida de diferentes entidades o personas que se contacten en el desarrollo de este proyecto. Las entrevistas son de tipo semi-estructuradas, con las cuales se logra obtener información muy específica por parte de los entrevistados, también se realizan a contactos electrónicos con entidades de otros países que permitan captar aspectos más generales como opiniones, descripciones narrativas de la situación actual de actividades realizadas o problemas

existentes e incluso ideas y sugerencias valiosas para este estudio.

- Cuestionario; sirve para poder capturar información relevante mediante preguntas que requieran de respuestas puntuales, así como de aquellas en las que deba profundizarse para obtener el mayor volumen de información relevante para el desarrollo del proyecto.

- Inspección; este método es utilizado sobre todo al evaluar las condiciones o recursos actuales con que cuenta la Universidad de El Salvador Facultad Multidisciplinaria de Occidente, mediante éste se determinan las necesidades actuales para el desarrollo de un proyecto a escala real y las sugerencias a proponer que ayuden al cambio a la versión 6 de IP.

3. Etapa de Comparación: Ésta se refiere a la comparación propiamente dicha entre las técnicas de transición seleccionadas, para las cuales se desarrollan prototipos

de implementación que permitan analizar la idoneidad o mejor adaptación de cada técnica a las condiciones de la Universidad de El Salvador Facultad Multidisciplinaria de Occidente. De esta etapa se obtiene la información necesaria para elaborar la propuesta de migración al IPv6. Esta fase es de mucha utilidad para la obtención de datos, el método de observación, puesto que se experimenta con los prototipos de implementación y se presencian las condiciones, dificultades y facilidades mostradas por cada una de las técnicas de transición a comparar.

4. Etapa de Definición de una Propuesta: Inmediatamente después de la etapa de Comparación, se genera como consecuencia aquella en la que se define la propuesta de la técnica de transición de IPv4 a IPv6 que mejor se adapte a las condiciones y necesidades de la Universidad de El Salvador Facultad Multidisciplinaria de Occidente, todo esto producto de interpretar los resultados obtenidos en la comparación previa. En esta etapa se define las principales conclusiones y recomendaciones finales del proyecto.

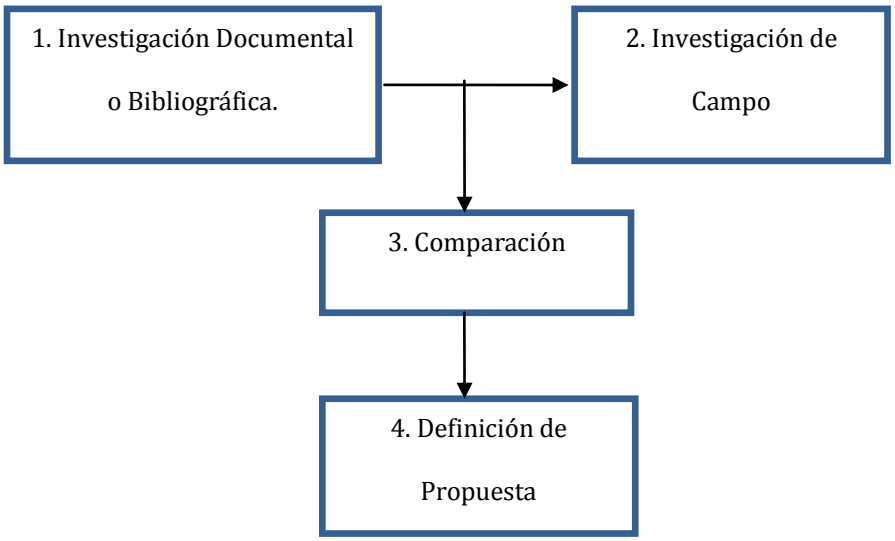


Figura 1.1 – Metodología de Investigación

Capítulo II

Protocolo IPv4

IPv4 es la versión 4 del Protocolo de Internet (IP por sus siglas en inglés) y constituye la primera versión de éste último que es implementada de forma extensiva. IPv4 es el principal protocolo utilizado en el nivel red del Modelo TCP/IP para Internet. Fue descrito inicialmente en el RFC 791 elaborado por la Fuerza de Trabajo en Ingeniería de Internet (IETF por sus siglas en inglés) en Septiembre de 1981, documento que dejó obsoleto al RFC 760 de Enero de 1980, el cual define al protocolo IP como tal. Tiene las siguientes características:

- Sin conexión: No establece conexión antes de enviar los paquetes de datos. De este problema se preocuparán los protocolos de nivel superior.

- Máximo esfuerzo (no confiable): No se usan encabezados para garantizar la entrega de paquetes. Esto permite que los paquetes sean más pequeños y sobrecarguen menos la

red. De la recuperación de paquetes perdidos o corruptos se encargarán los protocolos de nivel superior.

- Medios independientes: Operan independientemente del medio que lleva los datos. Es responsabilidad de los protocolos de nivel inferior esta tarea. Existe, no obstante, una característica principal de los medios que la capa de red: el tamaño máximo de la PDU que cada medio puede transportar. A esta característica se le denomina Unidad máxima de transmisión (MTU). Parte de la comunicación de control entre la capa de Enlace de datos y la capa de red es establecer un tamaño máximo para el paquete. La capa de Enlace de datos pasa la MTU hacia arriba hasta la capa de red.

El propósito principal de IP es proveer una dirección única a cada sistema para asegurar que una computadora en Internet pueda identificar a otra (RFC 791).

Formato del Paquete IPv4

Un paquete IP contiene varios tipos de información, que se detallan a continuación:

Figura 2.1 - Cabecera IPv4

- Versión: Indica la versión de IP que se está usando. En este caso siempre será 4.

- Ancho de cabecera IP (ILH): Indica el ancho de cabecera del datagrama en palabras de 32 bits.

- Tipo de servicio: Especifica la manera en que un protocolo de capa superior preferiría que fuese tratado el datagrama, y asigna al datagrama distintos niveles de importancia. Este campo normalmente alberga lo que en las configuraciones de los routers se conoce como peso relativo o métricas.

- Tamaño total: Especifica el tamaño total en bytes, del paquete IP entero, incluyendo los datos y la cabecera.

- Identificación: Contiene un entero que identifica al datagrama. Este campo es utilizado para ayudar a reconfigurar los datagramas fragmentados.

- Flags: Consiste en un campo de 3 bits de los cuales los dos menos significativos controlan la fragmentación. El bit menos significativo indica si el paquete puede ser fragmentado. El bit de en medio, indica si el paquete es el último de una serie de paquetes, y el tercer bit no es usado.

- Disposición del fragmento: Indica la posición relativa de los datos del fragmento con respecto al inicio de los datos en el datagrama original, lo que le permite al proceso IP destino, reconstruir apropiadamente el datagrama original.

- Tiempo de vida (TTL): Mantiene un contador que gradualmente decrementa hasta cero cada vez que atraviesa algún router, en cuyo momento el datagrama es descartado. Esto permite a los paquetes el evitar circular eternamente.

- Protocolo: Indica el protocolo de nivel superior que recibe el paquete luego de que el procesamiento IP termine.

- Comprobación de cabecera: Ayuda a asegurar la integridad de la cabecera IP.

- Dirección Origen: Especifica el nodo de origen.

- Dirección de Destino: Especifica el nodo de destino.

- Opciones: Permite a IP agregar varias opciones, por ejemplo seguridad, aunque este elemento es externo a la definición de IP.

Así como cualquier protocolo de capa de red, el esquema de direccionamiento IP es integral para el proceso de enrutamiento de datagramas IP a través de varias redes. Cada dirección IP tiene componentes específicos y sigue un formato básico. Estas direcciones pueden ser subdivididas y usadas para crear direcciones para subredes.

Cada cliente en una red TCP/IPv4 tiene asignada una dirección lógica única de 32 bits, la cual está dividida en dos partes principales: el número de red, y el número de cliente (host).

Direccionamiento IPv4

Para poder comunicarse en una red, cada equipo debe tener una dirección IP exclusiva. En el direccionamiento IP en clases, existen tres clases de dirección que se utilizan para asignar direcciones IP a los equipos. El tamaño y tipo de la red

determinará la clase de dirección IP aplicada a los equipos y otros hosts de la red.

La dirección IP es un identificador que diferencia un equipo de otro en una red y ayuda a localizar dónde reside ese equipo. Se necesita una dirección IP para cada equipo y componente de red, como un router, que se comunique mediante TCP/IP.

La dirección IP identifica la ubicación de un equipo en la red, debe ser exclusiva pero conforme a un formato estándar. Una dirección IP está formada por un conjunto de cuatro números, cada uno de los cuales puede oscilar entre 0 y 255. Obtenido el 4 de mayo de 2011, de (Urueña León, 2005).

Componentes de una Dirección IPv4

Una dirección IPv4 consta de dos partes: el ID de host y el ID de red.

ID de red: La primera parte de una dirección IP es el ID de red, que identifica el segmento de red en el que está ubicado

el equipo. Todos los equipos del mismo segmento deben tener el mismo ID de red.

ID de host: La segunda parte de una dirección IP es el ID de host, que identifica un equipo, un router u otro dispositivo de un segmento. El ID de cada host debe ser exclusivo en el ID de red.

Es importante observar que dos equipos con diferentes IDs de red pueden tener el mismo ID de host. Sin embargo, la combinación del ID de red y el ID de host debe ser exclusivo para todos los equipos que se comuniquen entre sí. Obtenido el 4 de mayo de 2011, de (Urueña León, 2005).

Clases de Direcciones

Las clases de direcciones se utilizan para asignar IDs de red a organizaciones para que los equipos de sus redes puedan comunicarse en Internet. Las clases de direcciones también se utilizan para definir el punto de división entre el ID de red y el ID de host.

Se asigna a una organización un bloque de direcciones IP, que tienen como referencia el ID de red de las direcciones y que dependen del tamaño de la organización. Por ejemplo, se asignará un ID de red de clase C a una organización con 200 hosts, y un ID de red de clase B a una organización con 20,000 hosts.

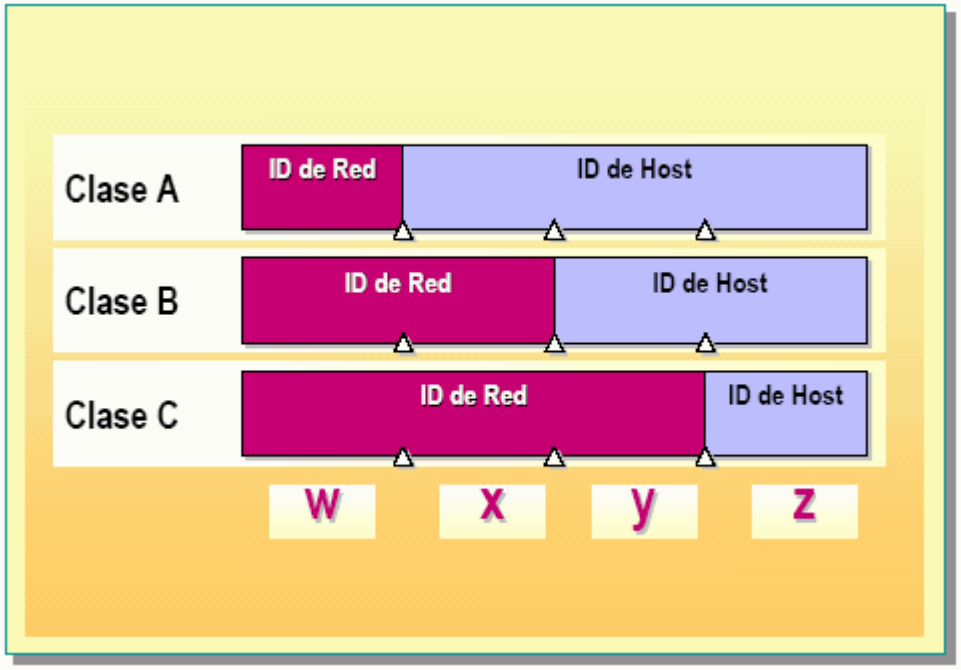


Figura 2.2 - Clases de Direcciones (Urueña León, 2005)

Clase A: Las direcciones de clase A se asignan a redes con un número muy grande de hosts. Esta clase permite 126 redes, utilizando el primer número para el ID de red. Los tres números restantes se utilizan para el ID de host, permitiendo 16,777,214 hosts por red.

Clase B: Las direcciones de clase B se asignan a redes de tamaño mediano a grande. Esta clase permite 16,384 redes, utilizando los dos primeros números para el ID de red. Los dos números restantes se utilizan para el ID de host, permitiendo 65,534 hosts por red.

Clase C: Las direcciones de clase C se utilizan para redes de área local (LANs) pequeñas. Esta clase permite aproximadamente 2,097,152 redes utilizando los tres primeros números para el ID de red. El número restante se utiliza para el ID de host, permitiendo 254 hosts por red.

Clases D y E: Las clases D y E no se asignan a hosts. Las direcciones de clase D se utilizan para la multidifusión, y las direcciones de clase E se reservan para uso futuro.

Obtenido el 4 de mayo de 2011, de (Urueña León, 2005).

Formato de Direcciones IPv4

La dirección IP de 32 bits es agrupado en bloques de ocho bits, separados por puntos, y representados en formato decimal (conocido como notación decimal puntuada. DDN por sus siglas en inglés). Cada bit en el octeto tiene un peso binario, donde el valor mínimo es 0 y el máximo es 255.

Cuando se escribe una dirección IPv4 en cadenas, la notación más común es en decimal con puntos. Hay otras notaciones basadas sobre los valores de los octetos de la dirección IP.

Notación	Valor	Conversión desde decimal con puntos
Decimal con puntos	201.161.1.226	-
Hexadecimal con puntos	0xC9.0xA1.0x01.0xE2	Cada octeto de la dirección es convertido individualmente a hexadecimal.
Octal con puntos	0311.0241.0001.0342	Cada octeto es convertido individualmente a octal.
Binario con puntos	11001001.10100001.00000001.11100010	Cada octeto es convertido individualmente a binario
Hexadecimal	0xC9A101E2	Concatenación de los octetos de hexadecimal con puntos.

Decimal	3382772194	La forma hexadecimal convertida a decimal.
Octal	31150200742	La forma hexadecimal convertida a octal.
Binario	11001001101000010000000111100010	La forma hexadecimal convertida a binario.

Tabla 2.1 - Notación de Direcciones IPv4 (Barrios Dueñas, 2009)

Teóricamente, todos estos formatos mencionados deberían ser reconocidos por los navegadores (sin combinar). Además, en las formas con puntos, cada octeto puede ser representado en combinación de diferentes bases. Ejemplo: 201.0241.0x01.226.

Asignación de Direcciones IPv4

Desde 1993 rige el esquema CIDR (Classless Inter-Domain Routing o Encaminamiento Inter-Dominios sin Clases) cuya principal ventaja es permitir la subdivisión de redes y permitir a las entidades sub-asignar direcciones IP, como haría un ISP con un cliente.

El principio fundamental del encaminamiento (routing) es que la dirección codifica información acerca de localización de un dispositivo dentro de una red. Esto implica que una

dirección asignada a una parte de una red no funcionará en otra parte de ella. Existe una estructura jerárquica que se encarga de la asignación de direcciones de Internet alrededor del mundo. Esta estructura fue creada para el CIDR, y hasta 1998 fue supervisada por IANA (Internet Assigned Numbers Authority o Agencia de Asignación de Números Internet) y sus RIR (Regional Internet Registries o Registros Regionales de Internet). Desde el 18 de Septiembre de 1998 la supervisión está a cargo de la ICANN (Internet Corporation for Assigned Names and Numbers o Corporación de Internet para los Nombres y Números Asignados). Cada RIR mantiene una base de datos WHOIS (Quien es) disponible al público y que permite hacer búsquedas que proveen información acerca de las asignaciones de direcciones IP. La información obtenida a partir de estas búsquedas juega un papel central en numerosas herramientas las cuales se utilizan para localizar direcciones IP geográficamente (RFC 791).

Bloques reservados: Existe una serie de bloques de direcciones IP reservadas que no pueden ser asignadas a ningún cliente. Dichos bloques son los siguientes:

Bloque de direcciones CIDR	Descripción	Referencia
0.0.0.0/8	Red actual (solo válido como dirección origen)	RFC 1700
10.0.0.0/8	Red Privada	RFC 1918
14.0.0.0/8	Red de datos públicos	RFC 1700
39.0.0.0/8	Reservado	RFC 1797
127.0.0.0/8	Anfitrión local (localhost)	RFC 1700
128.0.0.0/16	Reservado	
169.254.0.0/16	Red Privada (Zeroconf)	RFC 3927
172.16.0.0/12	Red Privada	RFC 1918
191.255.0.0/16		
192.0.0.0/24		
192.0.2.0/24	Red de pruebas	RFC 3330
192.88.99.0/24	Retransmisión desde IPv6 hacia IPv4	RFC 3068
192.168.0.0/16	Red Privada	RFC 1918
198.18.0.0/15	Pruebas de desempeño de red	RFC 2544
223.255.255.0/24	Reservado	RFC 3330
224.0.0.0/4	Multidifusión (Multicast, antes red Clase D)	RFC 3171
240.0.0.0/4	Reservado (Antes red Clase E)	RFC 1700
255.255.255.255	Difusiones (Broadcast)	

Tabla 2.2 - Bloques Reservados de Direcciones IPv4 (Barrios Dueñas, 2009)

Redes Privadas: De los más de cuatro mil millones de direcciones permitidas por IPv4, tres rangos están especialmente reservados para utilizarse solamente en redes privadas. Estos rangos no tienen encaminamiento fuera de una red privada y las máquinas dentro de estas redes privadas no pueden comunicarse directamente con las redes públicas. Sin embargo, pueden comunicarse hacia redes públicas a través de

la Traducción de Direcciones de Red o NAT (Network Address Translation).

Nombre	Rango de direcciones IP	Numero de direcciones IP	Tipo de clase	Bloque CIDR mayor
Bloque de 24bits	10.0.0.0 – 10.255.255.255	16,777,215	Única clase A	10.0.0.0/8
Bloque de 20bits	172.16.0.0 – 172.31.255.255	1,048,576	16 clases B contiguas	172.16.0.0/12
Bloque de 16bits	192.168.0.0 – 192.168.255.255	65,535	256 clases C contiguas	192.168.0.0/16

Tabla 2.3 – Bloques Reservados para Redes Privadas (Barrios Dueñas, 2009)

Anfitrión local (Localhost): Además de las redes privadas, el rango 127.0.0.0 – 127.255.255.255, o 127.0.0.0/8 en la notación CIDR, están reservados para la comunicación del anfitrión local (localhost). Ninguna dirección de este rango deberá aparecer en una red, sea pública o privada, y cualquier paquete enviado hacia cualquier dirección de este rango deberá regresar como un paquete entrante hacia la misma máquina.

Obtenido el 4 de mayo de 2011, de (Barrios Dueñas, 2009).

Direccionamiento IP de Subred

Las redes IP pueden ser divididas en redes más pequeñas llamadas subredes (subnets). El subneteo le brinda a un administrador de red múltiples beneficios, incluyendo flexibilidad extra, un uso más eficiente de las direcciones de red, seguridad y la capacidad de contener el tráfico de broadcast (un broadcast no atraviesa un router).

Las subredes como se mencionó son responsabilidad de los administradores locales. Con esta técnica, los medios externos observan la organización como una sola red, y no tienen conocimiento detallado de la estructura interna de dicha organización.

Una dirección de red puede ser separada en muchas subredes. Por ejemplo, 172.16.1.0, 172.16.2.0 y 172.16.3.0 son subredes dentro de la red 172.16.0.0 (cuando se especifican solo ceros en el espacio de la dirección de host, se hace referencia a toda la red).

Máscara de Subred IP: Una dirección de subred es tomando bits del campo del host y asignándolos como campo de subred. El número de bits prestados varía y es especificado por la máscara de subred.

Las máscaras de subred hacen uso del mismo formato y técnica de representación de las direcciones IP. Además, las máscaras de subred deben provenir de los bits más significativos del campo de host.

La máscara por defecto para una dirección clase B que no ha sido subneteada es 255.255.0.0, mientras que por ejemplo, la máscara de subred para una dirección clase B 171.16.0.0 que especifique ocho bits para subred sería 255.255.255.0.

La razón para esto es que ocho bits para subredes o 2^8-2 (una dirección para la red y otra para el broadcast) proporcionan 254 subredes posibles, con 2^8-2=254 host para cada subred.

La máscara de subred para una dirección clase C 192.168.3.0 que especifique 5 bits para subredes es 255.255.255.248, con

lo cual se dispondría de 2^5-2 = 30 subredes disponibles, con 2^3-2=6 host por cada subred.

Ruteo entre Redes

Los dispositivos de ruteo han sido llamados gateways tradicionalmente, sin embargo este término en la actualidad se refiere específicamente a routers, dispositivos que realiza las funciones de ruteo entre máquinas o redes bajo el mismo control administrativo o autoridad, como la red interna de una corporación.

Ruteo IPv4

Los protocolos de ruteo IP son dinámicos, lo que significa que las rutas usadas son calculadas automáticamente en intervalos regulares por el software contenido en los dispositivos de ruteo. Esto contrasta con el ruteo estático, donde las rutas son establecidas por el administrador de red y no cambian a menos que dicho administrador las cambie.

Una tabla de ruteo IP, la cual consta de pares de direcciones/próximos saltos, es usada para permitir el ruteo dinámico. Una entrada en dicha tabla, por ejemplo, se interpreta así: para llegar a la red 172.35.0.0, es necesario mandar el paquete a la dirección 190.10.0.2 por la interfaz Ethernet 0 (eth0 por ejemplo).

La participación de cada nodo en el proceso de ruteo se limita a enviar el paquete recibido, basándose en información interna. Al nodo no le interesa si el paquete llega hasta el destino final, así como IP tampoco proporciona un método para reportar los errores causados por anomalías de ruteo hasta la fuente. Esta tarea es delegada a otro protocolo, el Protocolo de Mensajes de Control de Internet (ICMP por sus siglas en inglés).

Protocolos Complementarios para IPv4

El Protocolo ICMP: El Protocolo de Mensajes de Control y Error de Internet o ICMP, es de características similares a UDP, pero con un formato mucho más simple, y su utilidad no está en el transporte de datos de usuario, sino en controlar

si un paquete no puede alcanzar su destino, si su vida ha expirado, si el encabezamiento lleva un valor no permitido, si es un paquete de eco, etc. Es decir, se usa para manejar mensajes de error y de control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado. ICMP proporciona así una comunicación entre el software IP de una máquina y el mismo software en otra.

El protocolo ICMP solamente informa de incidencias en la entrega de paquetes o de errores en la red en general, pero no toma decisión alguna al respecto. Esto es tarea de los protocolos de capas superiores.

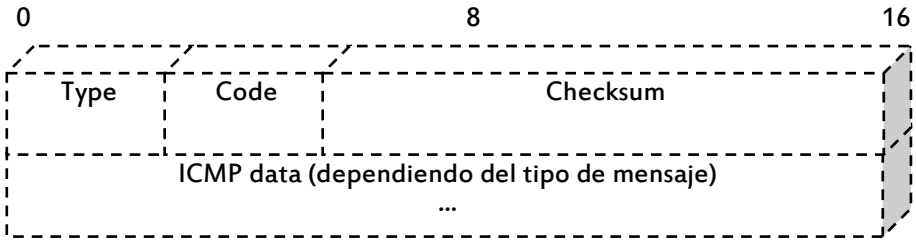


Figura 2.3 - Datagrama ICMP (Universidad de Malaga, 2002)

Los mensajes ICMP se transmiten como datagramas IP normales (ver figura 2.3), con el campo de cabecera "protocolo" con un valor 1, y comienzan con un campo de 8 bits que define el tipo de mensaje de que se trata. A continuación viene un

campo código, de 8 bits, que a veces ofrece una descripción del error concreto que se ha producido y después un campo suma de control, de 16 bits, que incluye una suma de verificación de errores de transmisión. Tras estos campos viene el cuerpo del mensaje, determinado por el contenido del campo "tipo". Contienen además los 8 primeros bytes del datagrama que ocasionó el error.

Los principales tipos de mensaje ICMP son los siguientes:

Mensajes informativos:

Tipo de mensaje	Descripción	Referencia
0	Echo Reply (respuesta de eco)	RFC792
3	Destination Unreacheable(destino inaccesible)	RFC792
4	Source Quench (disminución del tráfico desde el origen)	RFC792
5	Redirect (redireccionar - cambio de ruta)	RFC792
6	Alternate Host Address	JBP
8	Echo (solicitud de eco)	RFC792
9	Router Advertisement	RFC1256
10	Router Solicitation	RFC1256
11	Time Exceeded (tiempo excedido para un datagrama)	RFC792
12	Parameter Problem(problema de parámetros	RFC792
13	Timestamp (solicitud de marca de tiempo)	RFC792
14	Timestamp Reply (respuesta de marca de tiempo)	RFC792
15	Information Request(solicitud de información) - obsoleto-	RFC792
16	Information Reply (respuesta de información) - obsoleto-	RFC792
17	Addressmask (solicitud de máscara de dirección)	RFC792
18	Addressmask Reply(respuesta de máscara de dirección	RFC792

19	Reservado	
20-29	Reservado	ZSu
30	Traceroute	RFC1393
31	Datagram Conversion Error	RFC1475
32	Mobile Host Redirect	David Johnson
33	IPv6 Where-Are-You	Bill Simpson
34	IPv6 I-Am-Here	Bill Simpson
35	Mobile Registration Request	Bill Simpson
36	Mobile Registration Reply	Bill Simpson
37	Domain Name Request	RFC1788
38	Domain Name Reply	RFC1788
39	SKIP	Markson
40	Photuris	RFC2521
41	ICMP messages utilized by experimental	RFC4065
1,2,7,42-255	Reservados	JBP

Tabla 2.4 - Mensaje informativos ICMP (Universidad de Malaga, 2002)

Entre estos mensajes hay algunos de suma importancia, como los mensajes de petición de ECO (tipo 8) y los de respuesta de Eco (tipo 0). Las peticiones y respuestas de eco se usan en redes para comprobar si existe una comunicación entre dos host a nivel de capa de red, por lo que nos pueden servir para identificar fallos en este nivel, ya que verifican si las capas física (cableado), de enlace de datos (tarjeta de red) y red (configuración IP) se encuentran en buen estado y configuración.

Mensajes de Error: En el caso de obtener un mensaje ICMP de destino inalcanzable, con campo "tipo" de valor 3, el error concreto que se ha producido vendrá dado por el valor del campo "código", pudiendo presentar los siguientes valores:

Código de Error	Descripción	Referencia
0	No se puede llegar a la red	RFC792
1	No se puede llegar al host o aplicación de destino	RFC792
2	El destino no dispone del protocolo solicitado	RFC792
3	No se puede llegar al puerto destino o la aplicación destino no está libre	RFC792
4	Se necesita aplicar fragmentación, pero el flag correspondiente indica lo contrario	RFC792
5	La ruta de origen no es correcta	RFC792
6	No se conoce la red destino	RFC1122
7	No se conoce el host destino	RFC1122
8	El host origen está aislado	RFC1122
9	La comunicación con la red destino está prohibida por razones administrativas	RFC1122
10	La comunicación con el host destino está prohibida por razones administrativas	RFC1122
11	No se puede llegar a la red destino debido al Tipo de servicio	RFC1122
12	No se puede llegar al host destino debido al Tipo de servicio	RFC1122
13	Communication Administratively Prohibited	RFC1812
14	Host Precedence Violation	RFC1812
15	Precedence cutoff in effect	RFC1812

Tabla 2.5 - Mensajes de error ICMP (IANA, 2010)

Este tipo de mensajes se generan cuando el tiempo de vida del datagrama ha llegado a cero mientras se encontraba en

tránsito hacia el host destino (código=0), o porque, habiendo llegado al destino, el tiempo de reensamblado de los diferentes fragmentos expira antes de que lleguen todos los necesarios (código=1).

Los mensajes ICMP de tipo 12 (problemas de parámetros) se originan por ejemplo cuando existe información inconsistente en alguno de los campos del datagrama, que hace que sea imposible procesar el mismo correctamente, cuando se envían datagramas de tamaño incorrecto o cuando falta algún campo obligatorio.

Por su parte, los mensajes de tipo 5 (mensajes de redirección) se suelen enviar cuando, existiendo dos o más routers diferentes en la misma red, el paquete se envía al router equivocado. En este caso, el router receptor devuelve el datagrama al host origen junto con un mensaje ICMP de redirección, lo que hará que éste actualice su tabla de enrutamiento y envíe el paquete al siguiente router.

El Protocolo de Resolución de Direcciones ARP (Plummer, 1982): Para que dos máquinas en determinada red puedan

comunicarse, deben conocer entre sí la dirección MAC. Al enviar un broadcast de ARP, un cliente puede descubrir automáticamente la dirección de la subcapa MAC que corresponde a determinada dirección IP.

Luego de recibir una dirección MAC, los dispositivos IP crean una caché de ARP para almacenar las correspondencias IP-MAC recientemente adquiridas, y así evitar tener que hacer múltiples broadcast de ARP cuando quieran recontactar con un dispositivo. Si el dispositivo no responde dentro de un tiempo determinado, entonces la entrada de la caché es eliminada.

Existe también el caso contrario, en que se conozca la MAC y se desea saber la dirección IP correspondiente, en cuyo caso se utiliza el protocolo RARP (Protocolo de Resolución de Dirección Inversa).

ARP es responsable de convertir las direcciones de protocolo de alto nivel (direcciones IP) a direcciones de red físicas.

Dicho de otra manera, es un protocolo de nivel de enlace responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de difusión de la red (Broadcast, MAC = FF FF FF FF FF FF) que contiene la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto sólo funciona si todas las máquinas lo soportan.

En Ethernet, la capa de enlace trabaja con direcciones físicas. El protocolo ARP se encarga de traducir las direcciones IP a direcciones MAC (direcciones físicas).Para realizar ésta conversión, el nivel de enlace utiliza las tablas ARP, cada interfaz tiene tanto una dirección IP como una dirección física MAC.

ARP se utiliza en 4 casos referentes a la comunicación entre 2 hosts:

1. Cuando 2 hosts están en la misma red y uno quiere enviar un paquete a otro.

2. Cuando 2 host están sobre redes diferentes y deben usar un gateway/router para alcanzar otro host.

3. Cuando un router necesita enviar un paquete a un host a través de otro router.

4. Cuando un router necesita enviar un paquete a un host de la misma red.

Tabla ARP (caché ARP): Cada ordenador almacena una tabla de direcciones IP y direcciones físicas. Cada vez que formula una pregunta ARP y le responden, inserta una nueva entrada en su tabla. Sin embargo, para evitar incongruencias en la red debido a posibles cambios de direcciones IP o adaptadores de red, se asigna un tiempo de vida de cierto número de segundos a cada entrada de la tabla. Cuando se agote el tiempo de vida de una entrada, ésta será eliminada de la tabla. Obtenido el 4 de mayo de 2011, de (Curso de protocolos TCP/IP, 2001).

El Protocolo de Resolución de Direcciones Inverso RARP: Algunos hosts de red, tales como estaciones de trabajo sin disco, no saben su propia dirección IP cuando se resetean. Para determinar su propia dirección IP, usaron un mecanismo similar para ARP (Protocolo de Resolución de Direcciones), pero ahora la dirección hardware del host es el parámetro conocido, y la dirección IP el parámetro requerido. Esto difiere fundamentalmente de ARP en el hecho de que un servidor RARP debe existir en la red que mantiene una base de datos de correspondencia de direcciones hardware a direcciones de protocolo. Obtenido el 4 de mayo de 2011, de (Finlayson, 1984).

Protocolo IPSec: IPSec (abreviatura de Internet Protocol Security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet autenticando y/o cifrando cada paquete IP en un flujo de datos. IPSec también incluye protocolos para el establecimiento de claves de cifrado.

Los Protocolos de IPSec actúan en la capa de red, la capa 3 del modelo OSI. Otros protocolos de seguridad para Internet de uso extendido, como SSL, TLS y SSH operan de la capa de transporte (capas modelo OSI 4 a 7) hacia arriba. Esto hace que IPSec sea más flexible, ya que puede ser utilizado para proteger Protocolos de la capa 4, incluyendo TCP y UDP, los Protocolos de capa de transporte más usados. IPSec tiene una ventaja sobre SSL y otros métodos que operan en capas superiores, para que una aplicación pueda usar IPSec no hay que hacer ningún cambio, mientras que para usar SSL y otros Protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

IPSec está implementado por un conjunto de Protocolos criptográficos para asegurar el flujo de paquetes, garantizar la autenticación mutua y establecer parámetros criptográficos. Obtenido el 4 de mayo de 2011, de (Universidad Politécnica de Madrid, 2010).

Protocolo IPv6

IPv6 (Internet Protocol Version 6) o IPng (Next Generation Internet Protocol) es la nueva versión del protocolo IP (Internet Protocol). Ha sido diseñado por el IETF para reemplazar en forma gradual a la versión actual, el protocolo IPv4.

En esta versión se mantuvieron las funciones de IPv4 que son utilizadas, las que no son utilizadas o se usan con poca frecuencia, fueron removidas o se hicieron opcionales, agregándose nuevas características.

El motivo básico para crear un nuevo protocolo fue la falta de direcciones. IPv4 tiene un espacio de direcciones de 32 bits, en cambio IPv6 ofrece un espacio de 128 bits. El reducido espacio de direcciones de IPv4, junto al hecho de falta de coordinación para su asignación durante la década de los 80s, sin ningún tipo de optimización, dejando incluso espacios de direcciones discontinuos que generan en la actualidad dificultades no previstas en aquel momento.

Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, aspectos que no fueron contemplados en su análisis inicial, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades. Entre las más conocidas se pueden mencionar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPSec) y movilidad.

Formato del paquete IPv6

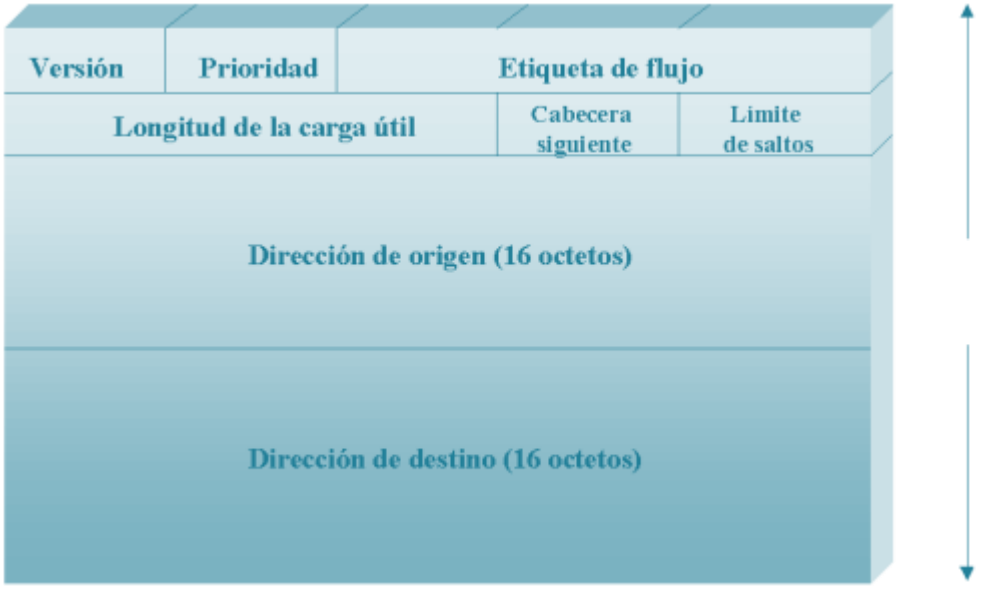


Figura 2.4 – Cabecera IPv6

Descripción de la Cabecera:

- Versión: Indica la versión del protocolo IP, en este caso su valor es igual a 6.

- Prioridad (Clase de tráfico "Traffic Class"): Incluye información que permite a los "routers" clasificar el tipo de tráfico al que el paquete pertenece, aplicando distintas políticas de enrutamiento según sea el caso. Realiza la misma función que el campo "Type of Service" de IPv4.

- Etiqueta de flujo ("Flow Label"): Identifica a un flujo determinado de paquetes, permitiendo a los "routers" identificar rápidamente paquetes que deben ser tratados de la misma manera.

- Longitud de Carga Útil ("Payload Length"): Indica cuantos bytes siguen en la cabecera de 40 bytes (es lo que en IPv4 era la Longitud Total).

- Siguiente Cabecera ("Next Header"): Indica cuales de las cabeceras de extensión, de haberlas, sigue a ésta. De no

haber apunta a la cabecera del protocolo capa 4 utilizado.

- Límite de saltos (“Hop Limit”): Indica el máximo número de saltos que puede realizar el paquete. Este valor es disminuido en uno por cada “router” que reenvía el paquete. Si el valor llega a cero, el paquete es descartado.

- Dirección de Origen (“Source Destination Address”): Indica la dirección IPv6 del nodo que generó el paquete.

- Dirección de Destino (“Source Destination Address”): Indica la dirección de destino final del paquete.

Características Principales

- Mayor espacio de direcciones: El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar más niveles de jerarquías de direccionamiento y más nodos direccionables.

- Simplificación del formato del Header: Algunos campos del header IPv4 se quitan o se hacen opcionales.

- Paquetes IP eficientes y extensibles: sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del router.

- Posibilidad de paquetes con carga útil (datos) de más de 65,355 bytes.

- Seguridad en el núcleo del protocolo (IPSec): El soporte de IPSec es un requerimiento del protocolo IPv6.

- Capacidad de etiquetas de flujo: Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) de tráfico particular, que requieren manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real. Por ejemplo video conferencia.

- Autoconfiguración: La autoconfiguración de direcciones es más simple. Especialmente en direcciones Aggregatable Global Unicast, los 64 bits superiores son seteados por un mensaje desde el router (Router Advertisement) y los 64 bits más bajos son seteados con la dirección MAC (en formato EUI-64). En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red. Además el largo del prefijo no depende en el número de los hosts por lo tanto la asignación es más simple.

- Renumeración y "multihoming": facilitando el cambio de proveedor de servicios o pudiendo utilizar 2 ISP al mismo tiempo.

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

- Ruteo más eficiente en el backbone de la red: debido a la jerarquía de direccionamiento basada en agregación.

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

- Capacidades de autenticación y privacidad: incorporación de encriptación y autenticación en la capa IP.

Cabeceras de Extensión

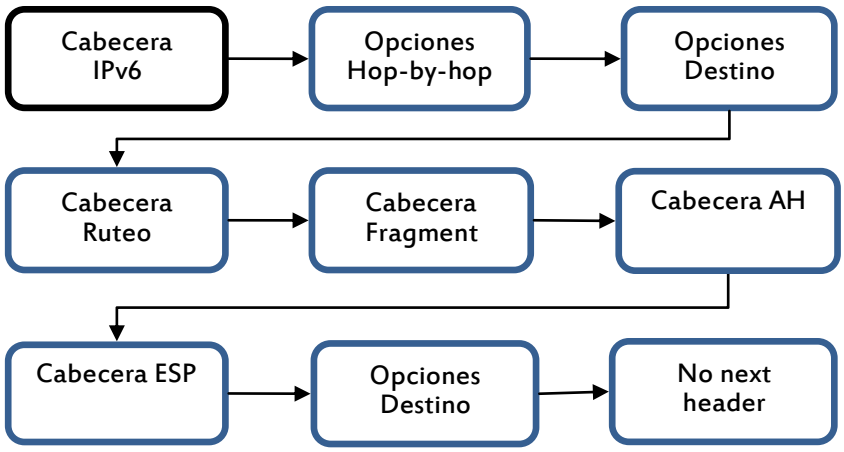


Figura 2.5 - Cabeceras de extensión IPv6

Tipos de Cabeceras de Extensión: Las cabeceras de extensión que se encuentran definidas en este momento (y deben usarse en este orden) son:

- *Opciones Hop-by-Hop (next header=0)*: Contiene datos que deben ser examinados por cada nodo a través de la ruta de envío de un paquete (RFC 2460).

- *Opciones de Ruteo (next header=43)*: Contiene métodos para especificar la forma de rutear un datagrama (RFC 2460, 3775, 5095).

- *Cabecera de Fragmentación o Fragment (next header=44)*: Contiene parámetros para la fragmentación de los datagramas (RFC 2460).

- *Cabecera de Autenticación o AH (next header=51)*: Contiene información para verificar la autenticación de la mayor parte de los datos del paquete (RFC 4302).

- *Encapsulado de Seguridad para Carga Útil o ESP (next header=50)*: Lleva la información cifrada para comunicación segura (RFC 4303).

- *Opciones de Destino (next header=60)*: Información que necesita ser examinada solamente por los nodos de destino del paquete (RFC 2460).

- *No Next Header (next header=59)*: Indica que no hay más cabeceras (RFC 2460).

Cada cabecera de extensión debe aparecer como mucho una sola vez, salvo la cabecera de opción destino, que puede aparecer como mucho dos veces, una antes de la cabecera ruteo y otra antes de la cabecera de la capa superior.

Ventajas de las Cabeceras de Extensión:

- Son procesadas solo por los nodos destinos y no por los nodos intermedios, excepto cuando la cabecera de opción hop-by-hop está activada.

- Se recomienda el uso de las cabeceras en el orden de la figura 2.5.

- El paquete se descarta si cualquier cabecera de extensión no es reconocida.

- Deja de existir la limitación de 40 bytes para las opciones planteadas en IPv4.

Fragmentación de Paquetes IPv6

Cabecera de Fragmentación: Se emplea cuando el paquete que se desea transmitir es mayor que el Path MTU existente hacia el destino. Es importante señalar que la fragmentación en IPv6 se realiza en el origen y nunca en los nodos intermedios, cosa que sí podía suceder en IPv4, con lo que se alivia muchos problemas de seguridad.

Paquete Original (no fragmentado):

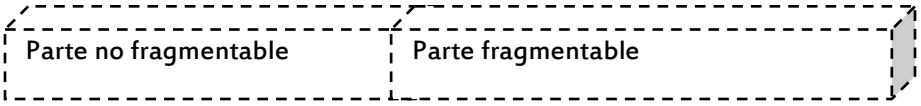


Figura 2.6 – Paquete Original IPv6 No Fragmentado

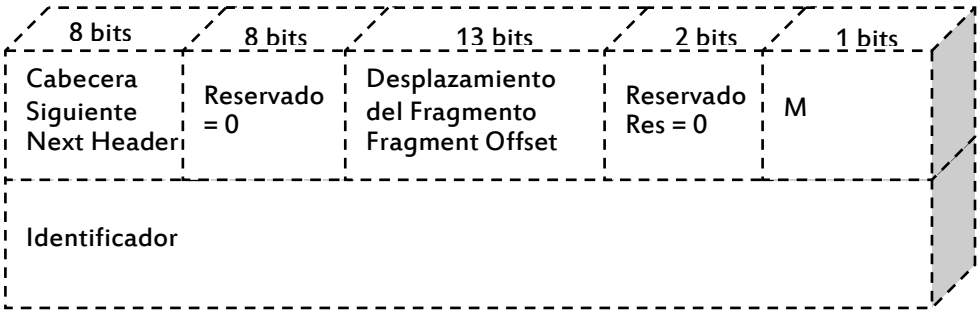


Figura 2.7 – Fragmento de Paquete IPv6

- Cabecera siguiente (8 bits).

- Reservado (8 bits): Uso futuro.

- Desplazamiento del fragmento (13 bits): Número de bloques de 8 octetos contenidos en el campo de datos de fragmentos anteriores.

- Reservado (2 bits): Uso futuro.

- Indicador M (1 bit): Indica si a continuación vienen más fragmentos pertenecientes al mismo Datagrama.

- Identificador (32 bits): Identifica a los fragmentos pertenecientes a un mismo datagrama.

Proceso de Fragmentación: La parte fragmentable del paquete original se divide en fragmentos de tamaño múltiplo de 8 bytes, excepto el último. Cada fragmento se envía en paquetes separados.

Paquete original:

Figura 2.8 – Paquete Original IPv6 Fragmentado

Paquetes fragmentados:

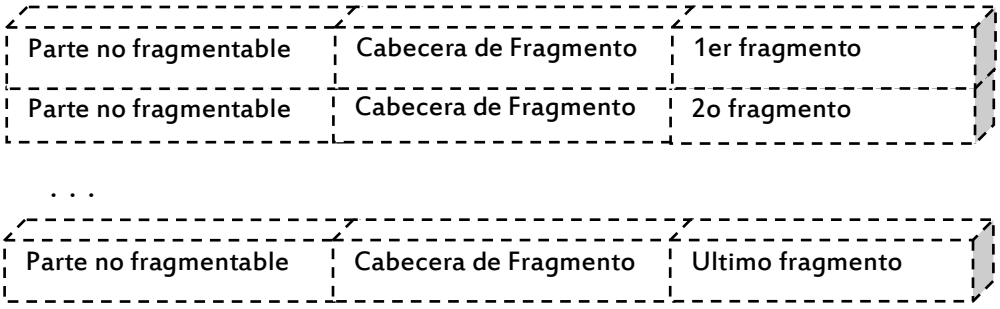


Figura 2.9 – Fragmentos de Paquete IPv6

Detalle del Proceso de Fragmentación: Suponiendo que el Host A (A) desea comunicarse con el Host B (B), y para hacerlo debe atravesar cuatro routers (R1 a R4). Todos los MTU son de 1500, excepto el del segmento que conecta a R2 con R3 el cual posee un MTU de 500. Para el ejemplo en el caso que A envía un paquete IPv6 de tamaño 1500 hacia B, el paquete avanza sin problemas por los enlaces entre A y R1, R1 y R2, pero cuando alcanza el segmento R2 y R3, R2 notifica a A que el paquete

es demasiado grande. Esta notificación se realiza a través de un mensaje ICMPv6 (Packet Too Big), el cual entre otra información, incluye el MTU que debería utilizar para fragmentar el paquete. Entonces A realiza el proceso de fragmentación y envía uno a uno los fragmentos, los cuales serán recompuestos al llegar a B.

MTU Mínimo: El link MTU es el máximo MTU del link o enlace, es decir, el tamaño máximo del paquete IP que puede transmitirse sobre el link. Por su parte, el Path MTU es el MTU mínimo de todos los links en la ruta desde el nodo origen hasta el nodo destino.

El link MTU mínimo para IPv6 es de 1280 bytes, en lugar de los 68 bytes que solía recomendar IPv4. Esto obliga entonces, a que los links donde el Path MTU sea menor que 1280 utilicen fragmentación y reensamblado en el nivel de enlace. Además, en los links donde fuese posible configurar el MTU, IPv6 recomienda usar un valor de 1500 bytes.

Descubrimiento del Path MTU (RFC1981): Las implementaciones deben realizar el descubrimiento del Path MTU enviando

paquetes mayores a 1280 bytes. Para cada destino, se comienza asumiendo el MTU del primer salto; luego, si un paquete llega a un link en el que el MTU es menor que su tamaño, se envía al nodo origen un paquete ICMPv6 "Packet Too Big", informando del MTU de ese link, el cual se guarda para ese destino específico. Ocasionalmente se descartan los valores almacenados de MTU para detectar posibles aumentos del MTU para los diversos destinos.

Las implementaciones minimalistas pueden omitir todo el proceso de descubrimiento de MTU si observan que los paquetes de 1280 bytes pueden llegar al destino. Esto es útil en implementaciones livianas, por ejemplo las que residen en sistemas operativos mínimos como en el caso de teléfonos celulares, etc.

Representación de Direcciones IPv6

Las representaciones de las direcciones IPv6 tienen las siguientes formas:

a) x:x:x:x:x:x:x:x, donde "x" es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. No es preciso escribir los ceros a la izquierda de cada campo. Ejemplos:

   1080:0000:0000:0000:0008:0800:200C:417A (impreciso)

   1080:0:0:0:8:800:200C:417A (preciso)

b) Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits "cero", se permite la abreviación de su escritura mediante el uso de "::", el cual sólo puede aparecer una vez en la dirección. Ejemplos:

   1080:0:0:0:8:800:200C:417A=1080::8:800:200C:417A

   FF01:0:0:0:0:0:0:101=F01::101

   0:0:0:0:0:0:0:1=::1

   0:0:0:0:0:0:0:0 = ::

c) La tercera optimización surge del problema que no se puede simplemente cambiar el protocolo sobre el cual está corriendo internet, por eso IPv6 tiene que poder convivir con IPv4 por años hasta que la transición termine e internet sea totalmente IPv6, así que se

inventó una forma de escribir IPv4 en IPv6 y se utiliza la segunda optimización que es la reducción de la cadena de 16 ceros por lo que si nuestra dirección IPv4 es 192.168.1.11 nuestro IPv6 será: ::192.168.1.11 lo que en realidad es: 0000:0000:0000:0000:0192:0168:0001:0011.

Normas para Direcciones IPv6

a) Una dirección IPv6 consta de 8 grupos de 16 bits separados por ":".

b) Se utiliza notación hexadecimal de cada medio octeto.

c) Se pueden eliminar los ceros a la izquierda dentro de cada grupo.

d) Se pueden sustituir uno o más grupos que contengan solamente ceros, por "::", pero esta sustitución solo puede hacerse una vez. Por ejemplo, suponga una dirección IPv6 2001:0DB8:3003:0001:0000:0000:6543:017A, podría comprimirse hasta 2001:DB8:3003:1::6453:17A.

Tipos de Direcciones IPv6

- Unicast: identifican a una sola interfaz. Un paquete enviado a una dirección Unicast es entregado sólo a la interfaz identificada con dicha dirección (uno a uno).

- Multicast: identifican un grupo de interfaces. Cuando un paquete es enviado a una dirección multicast es entregado a todos las interfaces del grupo identificadas con esa dirección (uno a muchas).

- Anycast (RFC 2526): identifican a un conjunto de interfaces. Un paquete enviado a una dirección anycast, será entregado a alguna de las interfaces identificadas con la dirección del conjunto al cual pertenece esa dirección anycast (a la más cercana).
    - Dirección para un conjunto de interfaces
    - Entrega a una única interfaz del conjunto

- No hay dirección de broadcast.

Unicast: Las direcciones "Unicast" cumplen la función de individualizar a cada nodo conectado a una red. Esto permite otorgar conectividad punto a punto entre los nodos pertenecientes a ella.

Uno de los nuevos aspectos introducidos en IPv6 es el uso de contextos en las direcciones "Unicast". Los contextos definen el dominio de una red, ya sea lógico o físico. El poder reconocer el contexto al que pertenece una determinada dirección permite realizar un manejo óptimo de los recursos de la red, optimizando su desempeño.

En IPv6, las direcciones Unicast pueden pertenecer a uno de los tres contextos existentes:

- Local al enlace ("link-local"): Identifica a todos los nodos dentro de un enlace (capa 2).

- Local único ("unique-local"): Identifica a todos los dispositivos dentro de una red interna o sitio, compuesta por varios enlaces o dominios capa 2.

- Global: Identifica a todos los dispositivos ubicables a través de Internet.

Direcciones "Unicast" Locales al Enlace: Las direcciones "Unicast" locales al enlace son aquellas que permiten la comunicación entre los distintos nodos conectados a un mismo enlace capa 2 del modelo ISO/OSI. Estas direcciones no pueden ser enrutadas y sólo son válidas al interior del enlace. Cada vez que un nodo IPv6 se conecta a una red, adquiere automáticamente una dirección local al enlace, sin ser necesaria la intervención del usuario o de otros dispositivos.

La estructura de una dirección local al enlace es "fe80:0:0:0:<identificador de interfaz>". El identificador de interfaz se genera automáticamente a partir de su dirección MAC, siguiendo el formato EUI-64. En la figura 2.10 se detalla cómo se construye el identificador de interfaz IPv6 a partir de la dirección MAC.

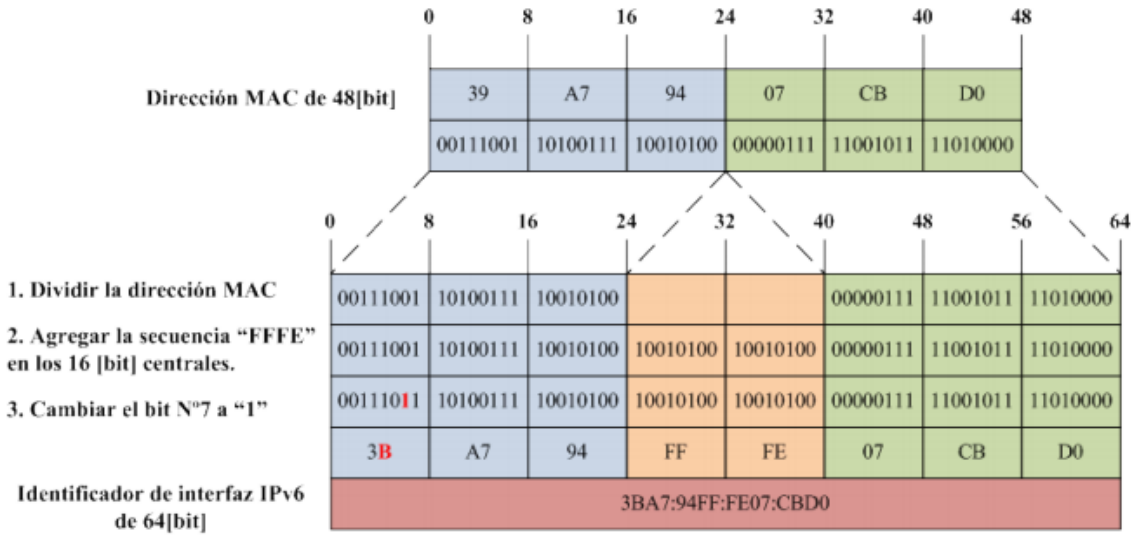


Figura 2.10 - Creación del Identificador de Interfaz (UTFSM (FELIPE ERNESTO JARA SABA), 2009)

Direcciones "Unicast" Locales Únicas: Las direcciones locales únicas son direcciones que permiten la comunicación de nodos al interior de un sitio.

Se entiende por sitio a toda red organizacional, de prefijo /48, compuesta por 1 o más subredes. Son el equivalente a las direcciones privadas en IPv4, cumpliendo la misma función: proveer conectividad entre los nodos de un sitio o "intranet".

Al igual que las direcciones locales al enlace, no pueden ser enrutadas hacia Internet. Su estructura se detalla en la figura 2.11.

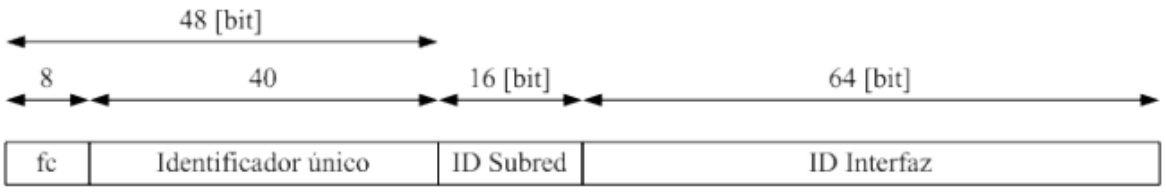


Figura 2.11 - Estructura de una Dirección Local Única

Todas las direcciones locales únicas se encuentran dentro del rango dado por el prefijo fc00::/7. Los campos de una dirección "Unicast" local única son:

- Identificador único: Es un valor de 40 bits que identifica a un sitio en particular. Dado que este tipo de direcciones no son publicadas en Internet, pueden existir distintos sitios con el mismo identificador.

- Identificador subred: Permite crear un plan de direccionamiento jerárquico, identificando a cada una de las 2^{16} posibles subredes en un sitio.

- Identificador de interfaz (IID): Individualiza a una interfaz presente en una determinada subred del sitio. A diferencia de las direcciones locales al enlace, este identificador no se genera automáticamente.

Los 64 bits de menor peso de las direcciones Unicast pueden ser asignados mediante diferentes métodos:

- Auto configuración a partir de una dirección MAC de 64 bits, como las que usa FireWire.

- Auto configuración a partir de una dirección MAC de 48 bits, como las que usa Ethernet, y expandida a un formato EUI-64 de 64 bits.

- DHCPv6.

- Configuradas manualmente.

- Auto generado pseudo-aleatoriamente (como medida de protección de seguridad).

- Además, se deja abierta la posibilidad para otros métodos en el futuro.

Direcciones "Unicast" Globales: Las direcciones Unicast globales son usadas para comunicar 2 nodos a través de Internet. Son el equivalente a las direcciones públicas en IPv4. Son el único tipo de direcciones que pueden ser enrutadas a través de Internet. El espacio reservado actualmente para este tipo de direcciones es de 2001:: a 3fff:ffff:ffff:ffff:ffff:ffff:ffff (2001::/3).

Todas las subredes en el espacio de direccionamiento Unicast global tienen un prefijo de red fijo e igual a /64. Esto implica que los primeros 64 bits (los primeros 4 campos en formato hexadecimal) corresponden al identificador de red, y los siguientes corresponden a la identificación de la interfaz de un determinado nodo. En la figura 2.12 se observa la estructura de una dirección Unicast global.

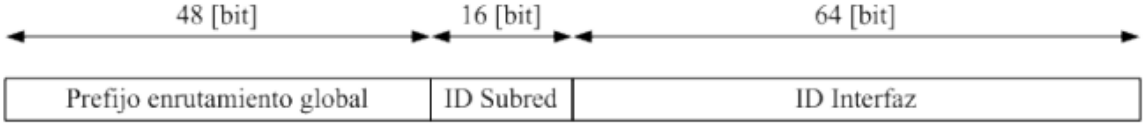


Figura 2.12 – Estructura de una Dirección "Unicast" Global

Unicast para Servicios en Producción: Actualmente, los ISPs toman prefijos /32, por lo que las direcciones IPv6 actuales empiezan por 2001, 2003, 2400, 2800, etc. Esta estructuración jerárquica se realiza por el ISP de acuerdo a su uso interno, hasta alcanzar los bloques /48. Desde los bloques /48 hasta los bloques /128 se delega a los usuarios, aunque existen algunas recomendaciones para la delegación de direcciones (RFC3177):

- Se debe asignar bloques /48 en casos generales.

- Se deben asignar bloques /64 si se sabe que una y solo una única red es necesaria.

- Se asignarán bloques /128 si es absolutamente seguro que se va a conectar uno y solo un dispositivo.

- Aun así, la cantidad de direcciones IPv6 es tan abrumadora, que generalmente se asignan bloques de direcciones amplios aunque actualmente no se necesiten.

Multicast: En IPv6 el tráfico "multicast" opera de la misma forma que en IPv4. Dispositivos IPv6 ubicados en distintos lugares pueden recibir tráfico dirigido a una única dirección "multicast". Las direcciones IPv6 "multicast" tienen la estructura presentada en la figura 2.13:

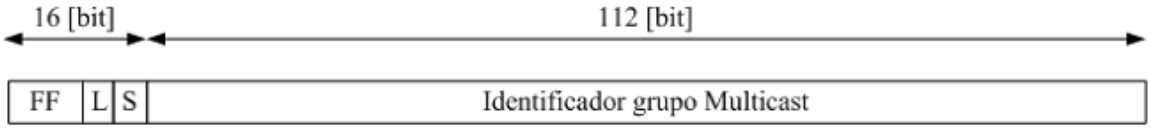


Figura 2.13 - Estructura Direcciones "Multicast"

El campo L indica el tiempo de vida de un grupo "multicast", tomando el valor de 0 cuando es un grupo permanente y 1 cuando es un grupo "multicast" temporal. El campo S (scope) indica el contexto o alcance del grupo, de acuerdo a los valores presentados en la tabla 2.6.

Valor de S (hexadecimal de 4 [bit])	Contexto del grupo
1	Interfaz
2	Enlace
5	Sitio
8	Organización
E	Global
Otros valores	Sin asignar o reservado

Tabla 2.6 - Códigos de Contexto Dirección "Multicast" (UTFSM (FELIPE ERNESTO JARA SABA), 2009)

IPv6 elimina el uso de las direcciones "broadcast", sustituyéndolas por direcciones "multicast". Esto permite hacer una selección más precisa de los destinatarios de una solicitud, evitando sobrecarga de mensajes en redes de muchos nodos. En la tabla 2.7 se muestran algunos de los grupos multicast fijos existentes.

Dirección Multicast	Descripción
FF01::1	Todos los nodos en la interfaz
FF02::1	Todos los nodos en el enlace
FF01::2	Todos los routers en la interfaz
FF02::2	Todos los routers en el enlace
FF05::2	Todos los routers en el sitio

Tabla 2.7 - Direcciones de Grupos "Multicast" Fijos (UTFSM (FELIPE ERNESTO JARA SABA), 2009)

Dirección Multicast de Nodo Solicitado: Para realizar la asociación entre direcciones capa 2 (MAC) y direcciones IPv6, se utiliza la dirección "multicast" de nodo solicitado. Esta dirección contiene parte de la dirección IPv6 que se desea consultar y posee la estructura descrita en la figura 2.14.

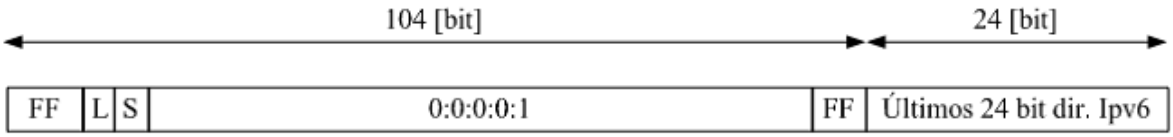


Figura 2.14 – Estructura Dirección "Multicast" de Nodo Solicitado (UTFSM (FELIPE ERNESTO JARA SABA), 2009)

Cada vez que un nodo se configura con una dirección IPv6, se une automáticamente al grupo multicast indicado por su dirección de nodo solicitado. Dado que dicha dirección toma solo los últimos 24 bit de la dirección IPv6, en un mismo grupo multicast pueden existir varios nodos con distintas direcciones IP. En la tabla 2.8 se pueden observar algunas direcciones IPv6 y sus correspondientes direcciones multicast de nodo solicitado.

Dirección IPv6	Dirección multicast de nodo solicitado
2800:270:bcd0:3::1	ff02::1:ff00:1
2800:270::1230:1000:a34:9e9a	ff02::1:ff34:9e9a
2800:270::34de:2000:a34:9e9a	ff02::1:ff34:9e9a
fc00:0:0:1::aaaa:a1	ff02::1::ffaa:a1

Tabla 2.8 - Ejemplos de Direcciones "Multicast" de Nodo Solicitado. (UTFSM (FELIPE ERNESTO JARA SABA), 2009)

Cuando un nodo desea enviar un paquete a un vecino presente en el mismo enlace y no tiene su dirección física, envía un mensaje que contiene la dirección IPv6 a consultar al grupo "multicast" de nodo solicitado correspondiente dicha dirección. Todos los nodos que estén en dicho grupo multicast reciben el mensaje, pero solo responde el nodo configurado con la dirección IPv6 solicitada.

Anycast: Una dirección "anycast" es aquella que identifica a un grupo de interfaces. Los paquetes enviados a una dirección anycast son reenviados por la infraestructura de enrutamiento hacia la interfaz más cercana al origen del paquete. Con el fin de facilitar la entrega, la infraestructura de enrutamiento debe conocer las interfaces que están asociadas a una dirección anycast y su distancia en métricas de enrutamiento.

Para configurar una dirección "anycast", basta con configurar una misma dirección Unicast en distintos dispositivos, junto con configurar en cada "router" una ruta directa hacia dicha dirección (/128). La idea es que cada "router" posea en su tabla de enrutamiento varias entradas hacia la misma dirección, con sus métricas asociadas. Al fallar la ruta más cercana, se selecciona automáticamente la siguiente.

El uso de "anycast" permite entre otras cosas implementar balanceo de carga y tolerancia a fallas. Por lo general, su uso se suele restringir al contexto de un sitio o red local. Las direcciones "anycast", al igual que las "multicast" solo son válidas como direcciones de destino en los paquetes IPv6.

Direcciones 6to4: Según el RFC3056, son direcciones que facilitan la conexión de dominios IPv6 a través de nubes IPv4. Posee un prefijo asignado 2002::/16. Para que se asigne a los sitios, se usa el formato 2002:IPv4::/48

001 0x0002	IPv4	SLA	Interface ID
Prefijo 6to4 (16 bits)	Dirección IPv4 pública del sitio (32 bits)	Topología del sitio (16 bits)	Identificador de interfaz (64 bits)

Tabla 2.9 - Direcciones 6to4

Prefijos de los Tipos de Direcciones: El prefijo es la parte de la dirección que indica las partes que tienen valores fijos o los bits del identificador de red.

Tipo de Dirección	Notación IPv6
Unspecified	::/128
Loopback	::1/128
Multicast	FF00::/8
Link-Local Unicast	FE80::/10
Unique Local Address (ULA)	FC00::/7
Global Unicast	
IPv4-mapped	::FFFF:IPv4/128

Tabla 2.10 - Prefijos de Direcciones IPv6 (UTFSM (FELIPE ERNESTO JARA SABA), 2009)

Algoritmos de Enrutamiento

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

2.11 se presentan las nuevas versiones desarrolladas para IPv6.

Protocolo enrutamiento	Versión IPv6
RIP	RIPng
EIGRP	EIGRP para IPv6
OSPF	OSPFv3
IS-IS	Integrated IS-IS
BGP	BGP-MP
EIGRP	EIGRP for IPv6

Tabla 2.11 Protocolos de Enrutamiento en IPv6 (UTFSM (FELIPE ERNESTO JARA SABA), 2009)

Protocolos Complementarios para IPv6

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

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

Cabecera ICMPv6:

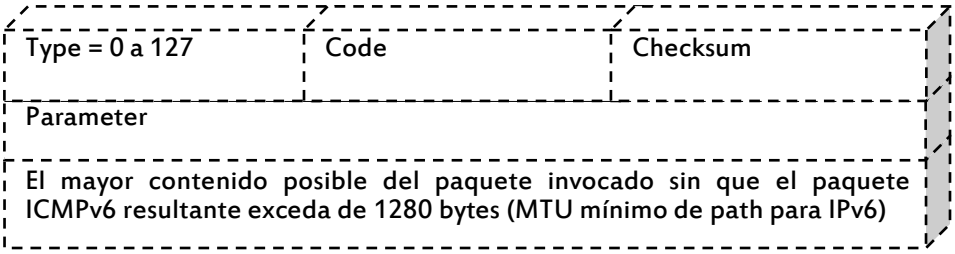


Figura 2.15 - Cabecera ICMPv6

- Type: Indica el tipo de mensaje. Este valor determina el formato de la información a recibir.

- Code: Depende del tipo de mensaje. Es usado para crear un nuevo subnivel de clasificación de los mensajes.

- Checksum: Es usado para detectar la corrupción de los datos en los mensajes ICMPv6 y en parte de las cabeceras IPv6.

- Parameter: Contiene el cuerpo del mensaje.

Tipos de Mensajes de Error Icmpv6:

- Destino inalcanzable (tipo=1, parámetro = 0).
- No hay ruta al destino (código=0).
- Comunicación con el destino prohibida administrativamente (código=1).
- Más allá del ámbito de la dirección origen (código=2).
- Dirección inalcanzable (código=3).
- Puerto inalcanzable (código=4).
- Dirección origen falló política de ingreso/egreso (código=5).
- Ruta a destino rechazada (código=6).
- Paquete demasiado grande (tipo=2, código=0, parámetro=next hop MTU).

- Tiempo excedido (tipo=3, parámetro=0).

- Límite de saltos excedidos en tránsito (código=0).

- Tiempo de reensamblado de fragmentos excedido (código=1).

- Problemas de parámetros (tipo=4, parámetro = offset to error).

- Campo de cabecera erróneo (código=0).

- Tipo no reconocido de "next header" (código=1).

- Opción IPv6 no reconocida (código=2).

Mensajes ICMP de Error: Los mensajes de error tienen un cero en el bit de mayor orden en el campo Type, por lo tanto el valor del campo Type es de 0 a 127. Los mensajes informativos a su vez, poseen valores para el campo Type de 128 a 255.

Mensajes ICMP Informativos:

- Echo Request (tipo=128, código=0).

- Echo Reply (tipo=129, código=0)

- Mensajes MLD (Multicast Listener Discovery).

- Query, report, done (funciona similar a IGMP para IPv4).

Protocolo de Descubrimiento de Vecinos: El protocolo de descubrimiento de vecinos (NDP por sus siglas en inglés) es un protocolo necesario para el correcto funcionamiento de las redes IPv6. Es el encargado de descubrir otros nodos en el enlace, realizar la resolución de direcciones IPv6 y direcciones MAC, encontrar los "routers" disponibles y mantener información actualizada sobre el estado de los caminos hacia otros nodos.

Este protocolo realiza funciones para IPv6 similares a las realizadas por ARP en IPV4. Para el intercambio de información, utiliza mensajes ICMPv6. En la tabla 2.12 se

presentan las funciones que realiza, junto al equivalente en IPv4.

Característica de NDP	Descripción	Equivalente IPv4
Descubrimiento de "routers"	Permite a los dispositivos detectar a los "routers" presentes en el enlace.	ICMP Router Discovery
Descubrimiento de prefijo	Permite a los nodos conocer el prefijo utilizado en el enlace.	No disponible
Descubrimiento de parámetros	Permite a los nodos auto configurar parámetros como MTU o número máximo de saltos.	PMTU Discovery
Autoconfiguración de direcciones	Permite a los dispositivos auto configurar su propia dirección.	No disponible
Resolución de direcciones	Permite a los nodos determinar las direcciones capa 2 de los dispositivos presentes en el enlace.	ARP
Determinación próximo salto	Permite a los nodos determinar el próximo salto para un destino dado.	Tabla ARP y/o tabla de enrutamiento en los dispositivos.
Detección de vecinos inalcanzables(NUD)	Detecta si se puede alcanzar un determinado nodo.	"Dead Gateway Detection"
Detección de direcciones duplicadas (DAD)	Permite a los nodos determinar si una dirección está en uso.	ARP con origen=0
Redirección	Permite a los "routers" informar a los nodos de un mejor próximo salto para una dirección en particular.	ICMPv4 Redirect

Tabla 2.12 - Características Protocolo de Descubrimiento de Vecinos (UTFSM (FELIPE ERNESTO JARA SABA), 2009)

Neighbor Discovery Protocol (NDP) define 5 tipos de paquetes: Router Solicitation (RS), Router Advertisement (RA), Neighbor Solicitation (NS), Neighbor Advertisement (NA) y Redirect.

Paquete Router Advertisement (RA): En una red (link) con capacidad de broadcast, cada router envía periódicamente paquetes multicast RA. Un host recibe los RAs de todos los routers, construyendo una lista de routers por defecto. El algoritmo de Neighbor Unreachability Detection (NUD) detecta si existen problemas para alcanzar a los routers que se han almacenado en la lista de routers por defecto.

Los RAs contienen una lista de prefijos usados por los hosts para determinar si una dirección destino de un paquete pertenece a dicho enlace y para la autoconfiguración de direcciones. Los RAs y los Flags asociados a cada prefijo permiten a los routers indicar a los hosts como realizar la autoconfiguración (ya sea stateless o DHCPv6).

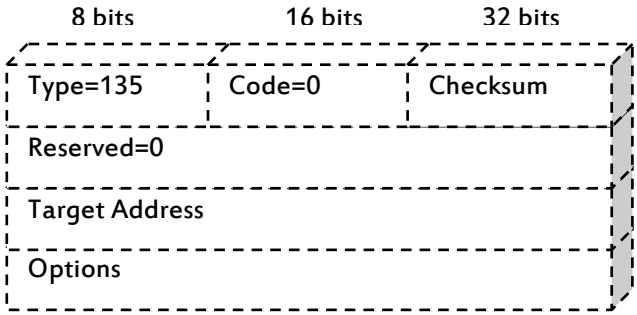


Figura 2.16 - Paquete Router Advertising

El campo Target Address contiene la dirección IPv6 objetivo de la solicitud, la cual no debe ser una dirección multicast. Igual que en RS, la única opción soportada actualmente es Source LinkLayer Address.

Paquete Neighbor Advertisement (NA): Un nodo envía NAs como respuesta a un NS y envía NAs no solicitados para propagar nueva información rápidamente.

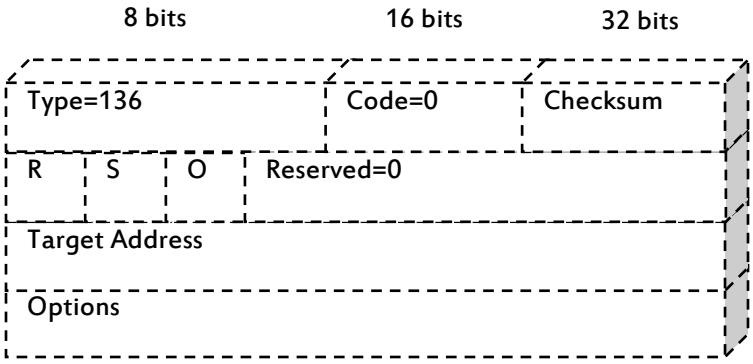


Figura 2.17 - Paquete Neighbor Advertising

- Flags:
    - R: Router Flag = 1 indica que el emisor es un router.
    - S: Solicited Flag=1 indica que se envía como respuesta a un NS.
    - O: Override Flag=1 indica que deben actualizarse las caches.

- El campo Target Address es igual al de los NS en caso de ser un NA solicitado. Si es un NA no solicitado, contiene la dirección MAC que ha cambiado. No puede ser una dirección multicast. La única opción disponible es el Target Link-Layer Address.

Paquete Redirect: Los routers envían paquetes Redirect para informar a un host que existe otro router mejor en el camino hacia el destino final. Los hosts pueden ser redireccionados a otro router considerado como mejor desde el punto de vista de los protocolos de enrutamiento, pero también pueden ser informados que el destino es un vecino mediante un paquete Redirect.

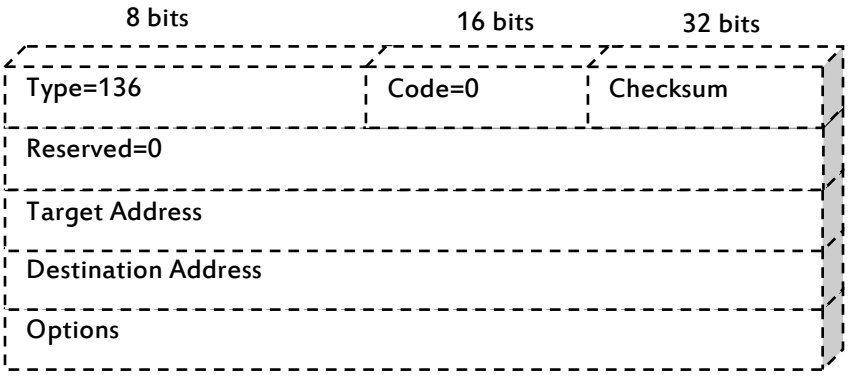


Figura 2.18 - Paquete Redirect

- Target Address contiene la dirección IPv6 del "first hop" que es mejor usar para llegar al "Destination Address" del paquete ICMPv6. A su vez, la Destination Address es la dirección IPv6 de destino que es redireccionada al "target address" del paquete ICMPv6.

Mecanismos de Configuración de Direcciones: En IPv6 existen tres distintas formas en las que un nodo puede obtener una dirección IPv6: de forma estática, autoconfiguración sin estados y mediante DHCPv6 (con estado).

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

Autoconfiguración Sin Estados ("Stateless"): El procedimiento de autoconfiguración sin estados utiliza el protocolo de descubrimiento de vecinos NDP para reconocer a los "routers" presentes en el enlace y generar una dirección IPv6 a partir

del prefijo que estos anuncian. Los pasos que realiza un nodo para obtener una dirección son los siguientes:

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

- Generar un identificador de interfaz: Para generar el resto de la dirección IPv6, el nodo genera un identificador de interfaz. Puede generarla a partir de su dirección MAC (como en las direcciones locales al enlace) o de forma aleatoria.

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

Algunas ventajas o beneficios de la autoconfiguración stateless son:

- No se necesita configuración manual de cada máquina antes de conectarla a la red.

- Los sitios pequeños compuestos de pocas máquinas conectadas al mismo segmento no necesitarían de un servidor DHCPv6 ni de un router para comunicarse, podrían usar direcciones link-local.

- Un sitio grande con varias subredes tampoco necesitaría un servidor DHCPv6 para la configuración de direcciones.

- Facilita el cambio de prefijo de un sitio completo, mediante el uso de varias direcciones por interfaz y cambios en los tiempos de vida.

Configuración Stateful: Dinamic Host Configuration Protocol para IPv6 o DHCPV6 (RFC 3315) establece una contraparte a la Autoconfiguración Stateless de direcciones IPv6. De acuerdo al RFC, DHCPv6 se usa cuando no se encuentra un router, o si

el mensaje RA habilita el uso de DHCPv6 de manera explícita. También existe un DHCPv6 stateless (RFC3736) pero solo es usado de forma experimental por el momento, o en los ISP para asignar prefijos de forma temporal y automática a routers de clientes.

DHCPv6 funciona de acuerdo al modelo cliente/servidor. Desde la perspectiva del servidor, este responde a las peticiones de los clientes, de manera opcional, provee a los clientes de una dirección IPv6 y de otros parámetros de configuración (como servidores DNS, pero no puede asignarse un Default Gateway). Los servidores DHCPv6 escuchan en direcciones multicast específicas: FF02::1:2 (Todos los servidores DHCP y los Relay Agents) y FF05::1:3 (Todos los servidores DHCP). Además memorizan el estado de los clientes y son capaces de proveer métodos para asegurar el control de acceso a los recursos de la red.

Soporte IPv6 en Sistemas Operativos, Aplicaciones y Servicios

Soporte IPv6 en Sistemas Operativos: Prácticamente todos los sistemas operativos desarrollados actualmente cuentan con soporte IPv6. Para las organizaciones y empresas, dicha característica es vista como una garantía de que dichos productos funcionaran adecuadamente en los próximos años. Sin embargo, los ciclos de adopción de los sistemas operativos son extensos, lo que hace necesario revisar el soporte IPv6 en versiones anteriores de dichos sistemas. En la tabla 2.14 se presenta un resumen con el soporte IPv6 de los sistemas operativos más utilizados por usuarios y servidores.

Sistema Operativo	Soporte IPv6	Observaciones
Windows 7	Sí	
Windows Vista	Sí	
Windows XP	Sí	
Windows 2003	Sí	
Windows 2000	No	Soporte parcial a través de software adicional
Windows 95/98/NT	No	Soporte parcial a través de software adicional
Linux	Sí	Desde kernel 2.2
FreeBSD	Sí	Desde versión 4
Solaris	Sí	Desde versión 8
Mac OSX	Sí	Desde versión 10.2
Iphone (Mac OSX)	No	
Windows Mobile	Sí	Desde versión 2003

Tabla 2.13 - Soporte de sistemas operativos para IPv6 (UTFSM (FELIPE ERNESTO JARA SABA), 2009).

Sistemas Operativos Windows: Microsoft se encuentra trabajando activamente en el desarrollo de integración de IPv6 en sus productos desde la primera publicación oficial del protocolo. Actualmente cuenta con soporte IPv6 en los sistemas operativos Windows XP, Vista, 7, Server 2003 y Server 2008. Versiones anteriores no cuenta con soporte oficial de Microsoft, sin embargo existen ciertos parches y actualizaciones creadas por terceros que permiten a dichos sistemas contar con un limitado soporte a IPv6.

Windows XP y Windows Server 2003:

- El soporte IPv6 en dichos sistemas debe ser instalado manualmente.

- La dirección del servidor DNS a utilizar debe ser una dirección IPv4. No soportan realizar consultas DNS a través de IPv6.

- No cuentan con una interfaz gráfica para modificar la información IPv6 de una interfaz, se debe utilizar la línea de comandos.

- No soportan el compartir impresoras ni archivos a través de IPv6.

- El firewall incorporado en Windows XP soporta IPv6, pero no se pueden crear reglas específicas para dicho protocolo.

- No soportan IPv6 móvil.

Windows Vista, Windows 7 y Windows Server 2008:

- Estos sistemas operativos cuentan con la última implementación IPv6 desarrollada por Microsoft, la cual incorpora todas las características definidas del protocolo.

- IPv6 es el protocolo capa 3 utilizado por omisión en Windows Vista y Windows 7. Cuando IPv4 e IPv6 se encuentran activados, estos sistemas operativos intentaran conectarse a la dirección IPv6 de un dispositivo remoto.

- Incorporan una interfaz gráfica para la configuración del protocolo.

- Windows 7 incorpora una función denominada Direct Access que proporciona acceso a los recursos de una red a usuarios remotos (similar a una VPN). Es una de las primeras aplicaciones desarrolladas que sólo funciona en IPv6.

Sistemas Operativos BSD: Los sistemas operativos basados en BSD fueron los primeros en incluir soporte IPv6, dado los trabajos realizados en el proyecto KAME. El proyecto KAME fue un esfuerzo conjunto de 6 grandes organizaciones en Japón cuyo objetivo fue proporcionar una implementación gratuita de IPv6 e IPSec a los sistemas operativos basados en BSD. Este proyecto fue uno de los más importantes en el desarrollo inicial de IPv6, siendo la base y referente de implementaciones realizadas en otros sistemas operativos. Los desarrollos realizados por el proyecto KAME están presentes en los sistemas operativos BSD a partir de FreeBSD 4.0, NetBSD 1.5 y OpenBSD 2.7. En la actualidad, el proyecto KAME ha finalizado, sin embargo todo el código creado forma parte de las actuales versiones de los sistemas operativos mencionados.

Sistemas Operativos Linux: Las primeras implementaciones de IPv6 en Linux fueron publicadas el año 1996 y estaban basadas en el proyecto KAME de los sistemas operativos BSD. Uno de los mayores contribuidores al desarrollo IPv6 en Linux es el proyecto USAGI (UniverSAl playGround for Ipv6) manejado por un grupo de voluntarios que buscan implementar todas las

funciones de IPv6 en el núcleo de Linux. Linux cuenta con soporte IPv6 oficialmente desde la versión 2.2. Sin embargo no se recomienda su uso para IPv6, ya que todos los avances y mejoras respecto al protocolo se están realizando en las versiones 2.4.x y 2.6.x.

Soporte IPv6 en Aplicaciones:

Soporte IPv6 en Aplicaciones de Uso Común: Existen en la actualidad innumerables aplicaciones que incluyen algún tipo de soporte para IPv6. En la tabla 2.15 se presenta un resumen del soporte que proveen algunas de las aplicaciones de mayor uso en ambientes hogareños y/o de oficina.

Aplicación	¿Soporte de Ipv6?	1er versión con soporte Ipv6	Notas
Windows Explorer	Si	4.01	En versiones anteriores a la 7.0 no se puede especificar directamente una dirección IPv6, es necesario el apoyo de un servidor DNS.
Firefox	Sí	1.5	
Windows Mail	Sí		Soporta uso directo de direcciones IPv6 para configurar cuentas de correo
Outlook	Sí	2003	Soporta uso directo de direcciones IPv6 para configurar cuentas de correo.
Outlook Express	No		Usar Windows Mail.

Thunderbird	Sí		No se puede especificar directamente una dirección IPv6, es necesario el apoyo de un servidor DNS.
Winamp	Sí	5.34	
VLC	Sí		
Windows Media Player	Sí	9.0	

Tabla 2.14 – Soporte IPv6 de Aplicaciones de Uso Común (UTFSM (FELIPE ERNESTO JARA SABA), 2009).

Soporte IPv6 de aplicaciones hechas a la medida: Las aplicaciones hechas a la medida son aquellas diseñadas específicamente para la empresa bajo sus criterios y necesidades, por ejemplo Sistemas Contables, Sistemas de Información Gerencial y similares, etc. En dado caso estos no sean independientes de la versión del Protocolo de Internet, será necesario contactar a los programadores de dichas aplicaciones para que modifiquen el código de las mismas y así, cuenten con soporte del protocolo IPv6.

Soporte IPv6 en Servicios Asociados:

Servidor DNS (BIND): BIND permite el uso indistinto de IPv4 o IPv6 como protocolo de comunicación (capa 3) para realizar consultas al servidor DNS. El protocolo utilizado es

independiente del tipo de consulta realizada: se pueden consultar por direcciones IPv4 utilizando IPv6 y viceversa.

Respecto a la resolución de nombres a direcciones IPv6, existe el registro "AAAA" que es el equivalente directo al registro "A" utilizado en IPv4. Un nombre de host puede estar asociado a una dirección IPv4 y/o a varias direcciones IPv6, basta con agregar los correspondientes registros en el archivo de zona. En la tabla 2.16 se muestra un ejemplo de ello.

Nombre	Tipo de Registro	Valor
prueba.sv	A	190.87.183.29
prueba.sv	AAAA	2800:270:a3c4::2
prueba.sv	AAAA	3ffe:b00:0:1::1

Tabla 2.15 - Ejemplo de un Sitio Asociado a Direcciones IPv4 e IPv6 en un DNS

Para la resolución inversa de direcciones IPv6, se utiliza el mismo registro PTR utilizado en IPv4. Para construir la parte izquierda del registro, se ingresa cada digito hexadecimal de la dirección IPv6, separándolos por un punto. A esta dirección se agrega el nombre de dominio superior "ip6.arpa".

En la tabla 2.17 se ve un ejemplo para la dirección 3ffe:b00:0:1::1.

Nombre	Tipo de Registro	Valor
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.0.0.0.0.0.0.e.f.f.3.ip6.arpa	PTR	prueba.sv

Tabla 2.16 – Ejemplo de Registro PTR para una dirección IPv6

Servidor Web (Apache): Apache cuenta con soporte IPv6 desde la versión 2.0. Sin embargo, y dada la popularidad de la versión 1.3, se han desarrollados parches que permiten que dicha función funcione con IPv6.

Servicios de Monitoreo y Administración de Redes: La gran mayoría de los "software" de monitoreo y administración de redes se basan en el uso del protocolo SNMP, el cual mediante el uso de estaciones de administración, monitorea y maneja dispositivos que contienen un agente SNMP y se encuentran conectados a una red IP.

Al igual que en el caso de DNS, el protocolo capa 3 utilizado para el transporte de información entre las estaciones de administración y los dispositivos monitoreados, es independiente de la información transmitida. En el caso de

Cisco, el uso de SNMP sobre IPv6 está disponible desde IOS 12.0.

La información que un agente proporciona a una estación de monitoreo, está determinada por la(s) MIB (Management Information Base) que implementa. En un principio, la IETF definió MIBs diferentes para información respecto a IPv4 e IPv6. Sin embargo, en 1996 se definieron las denominadas MIBs unificadas (RFC 2011 y RFC 2096), que reúnen la información de ambos protocolos.

Una de las mayores críticas a este nuevo modelo, es que no permitía especificar contadores de tráfico separados por cada protocolo. Esto implicaba que no era posible obtener estadísticas diferenciadas sobre el número de paquetes transmitidos, erróneos y descartados en una interfaz por cada protocolo IP. A raíz de esto y motivado por diversas necesidades de los usuarios, en el año 2006 se publicaron los documentos RFC 4293 y 4293 que especifican contadores independientes para IPv4 e IPv6.

Comparativa entre los Protocolos IPv4 e IPv6

A continuación se presenta la tabla 2.13, la cual contiene un resumen de las características de los protocolos IPv4 e IPv6, mostrando las diferencias más notorias entre los mismos a modo de comparativa, con el fin de identificar las mejoras y diferencias implementadas por la nueva versión del protocolo IP:

	IPv4	IPv6
Direcciones	Las direcciones de origen y destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de origen y destino tienen una longitud de 128 bits (16 bytes).
IPSec	La compatibilidad es opcional.	La compatibilidad es obligatoria.
Identificación del número de paquetes	No existe ninguna identificación de flujo de paquetes para que los routers controlen la QoS en el encabezado IPv4.	Se incluye la identificación del flujo de paquetes para que los routers controlen la QoS en el encabezado IPv6, utilizando el campo Flow Label (etiqueta de flujo).
Fragmentación	La llevan a cabo los routers y el host que realiza el envío.	No la llevan a cabo los routers, sino únicamente el host que realiza el envío.
Encabezado	Incluye una suma de comprobación.	No incluye una suma de comprobación.
Opciones	El encabezado lo incluye.	Todos se trasladan a los encabezados de extensión IPv6.
Marcos de solicitud ARP	El Protocolo de resolución de direcciones (ARP) utiliza los marcos de solicitud ARP de difusión para resolver una dirección IPv4 como una dirección de capa de vínculo.	Los marcos de solicitud ARP se sustituyen por mensajes de solicitud de vecinos de multidifusión.

Administrar la pertenencia a grupos locales de subred	Se utiliza el Protocolo de administración de grupos de Internet (IGMP).	IGMP se sustituye con los mensajes de Descubrimiento de escucha de multidifusión (MLD).
Determinar la dirección IPv4 de la mejor puerta de enlace predeterminada	Se utiliza el Descubrimiento de routers ICMP, y es opcional.	El Descubrimiento de routers ICMP queda sustituido por la Solicitud de routers ICMPv6 y los mensajes de anuncio de router, y es obligatorio.
Direcciones de multidifusión	Se utilizan para enviar tráfico a todos los nodos de una subred.	No hay direcciones de multidifusión IPv6. De forma alternativa, se utiliza una dirección de multidifusión para todos los nodos de ámbito local del vínculo.
Configuración manual	Debe configurarse manualmente o a través de DHCP.	No requiere configuración manual o a través de DHCP.
DNS	Utiliza registros de recurso (A) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv4.	Utiliza registros de recurso (AAA) de dirección de host en el Sistema de nombres de dominio (DNS) para correlacionar nombres de host con direcciones IPv6.
Direcciones IP relacionados con host	Utiliza registros de recurso (A) de puntero en el dominio DNS IN-ADDR.ARPA para correlacionar direcciones IPv4 con nombres de host.	Utiliza registros de recurso (PTR) de puntero en el dominio DNS IP6.INT para correlacionar direcciones IPv6 con nombres de host.
Tamaño de paquete	Debe admitir un tamaño de 576 bytes (posiblemente fragmentado).	Debe admitir un tamaño de 1280 bytes (sin fragmentación).

Tabla 2.17 - Comparativa entre las Características de los Protocolos IPv4 e IPv6 (Maxitrucos.com & Rodriguez, 2003)

Técnicas de Transición

En la actualidad, existen diversas técnicas o herramientas de transición que permiten migrarse total o parcialmente del protocolo IPv4 a IPv6. Entre las técnicas más utilizadas están los túneles IPv4 a través de IPv6, la pila dual que es una implementación total de ambos protocolos (IPv4 e IPv6), existe también los traductores que convierten paquetes IPv6 a IPv4 y viceversa. Obtenido el 26 de mayo de 2011, de (Internet Society, 2002).

Esto no significa que en futuras ocasiones no vayan a aparecer nuevas técnicas de transición, las cuales deberán ser analizadas en su momento para poder evaluar si son una mejor opción para lograr el objetivo, migrarse al nuevo protocolo IPv6.

Pila Dual (Dual-Stack)

El camino más lógico y evidente de transición es el uso simultáneo de ambos protocolos, en pilas separadas. La forma más directa para los nodos IPv6 de ser compatibles con nodos

IPv4 es proveyendo una implementación completa de IPv4. Los nodos IPv6 que proveen una implementación completa de IPv4 (además de su implementación de IPv6) son llamados nodos "IPv6/IPv4" o nodos de pila dual. Estos nodos tienen la habilidad de enviar y recibir paquetes IPv6 e IPv4, pudiendo así interoperar directamente con nodos IPv4 usando paquetes IPv4, y también operar con nodos IPv6 usando paquetes IPv6.

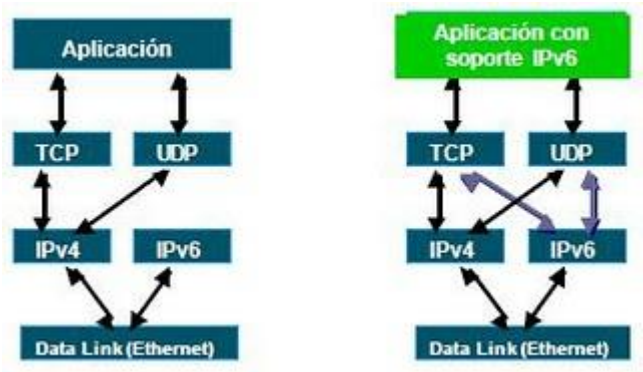


Figura 2.19 - Funcionamiento Pila Dual

La pila dual es una implementación que incluye las pilas de los dos protocolos IPV4 e IPV6, en cada nodo de la red, pudiendo así interoperar entre sí.

De esta forma, un dispositivo con ambas pilas pueden recibir y enviar tráfico a nodos que sólo soportan uno de los dos protocolos (nodos sólo IPv4 o sólo IPv6).

El dispositivo tendrá una dirección en cada pila. Se pueden utilizar direcciones IPv4 e IPv6 relacionadas o no, y se pueden utilizar mecanismos manuales o automáticos para la asignación de las direcciones (cada una correspondiente al protocolo en cuestión). El cambio básicamente se da en la capa de Internet del modelo TCP/IP.

En este caso cada nodo de pila dual en la red tendrá dos direcciones de red, una IPV4 y otra IPv6. Este mecanismo es usado para la comunicación entre nodos IPV6 e IPV4. Para esto se cuenta con nodos IPv6/IPv4.

Capa Dual IP: La capa dual contiene una implementación para capas de protocolos de host a host, para TCP y UDP, todos los protocolos de capas superiores en la capa dual IP pueden comunicar sobre IPV4, IPV6 o túneles IPV6 sobre IPV4 (figura 2.20).

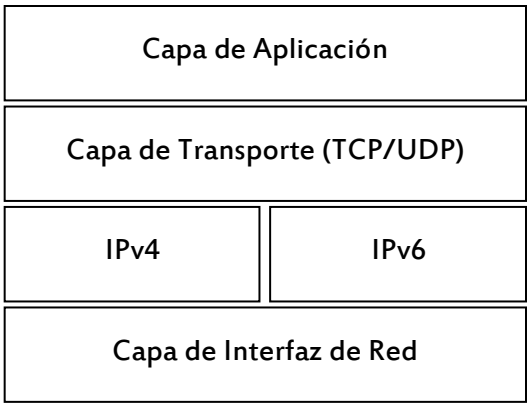


Figura 2.20 - Arquitectura de la capa dual IP (Universidad Politecnica Salesian)

Configuración de Direcciones: Los nodos que tienen que soportar ambos protocolos, ósea los nodos IPV4/IPV6, pueden ser configurados con direcciones IPV4 e IPV6.

Los nodos IPv6/IPv4 usan mecanismos DHCP para adquirir las direcciones IPV4, y mecanismos de autoconfiguración de direcciones sin estado para adquirir las direcciones IPV6.

DNS: El sistema de denominación de dominio (DNS o Domain Naming System) es usado en ambos protocolos, IPV4 e IPV6.

Es un sistema utilizado en Internet para convertir los nombres de los dominios y de sus nodos de red publicados abiertamente en direcciones IP.

Cada unidad de información del DNS se llama Registro de Recurso (RR). Cada registro tiene un tipo asociado que describe el dato que contiene, y una clase que especifica el tipo de red al que se aplica. Esto último se adapta a diferentes esquemas de dirección, como direcciones IP. El RR típico es el registro A, que asocia un nombre completamente cualificado con una dirección IPv4.

El tipo de registro de recurso AAAA es un nuevo registro específico a la clase Internet que almacena una sola dirección IPv6. El DNS de la capa dual soporta las dos versiones de protocolo, soportando tanto registro tipo A de IPv4 o Tipo AAAA de IPv6.

El funcionamiento básico de la pila dual de protocolos junto con su DNS es como se observa en la figura 2.21:

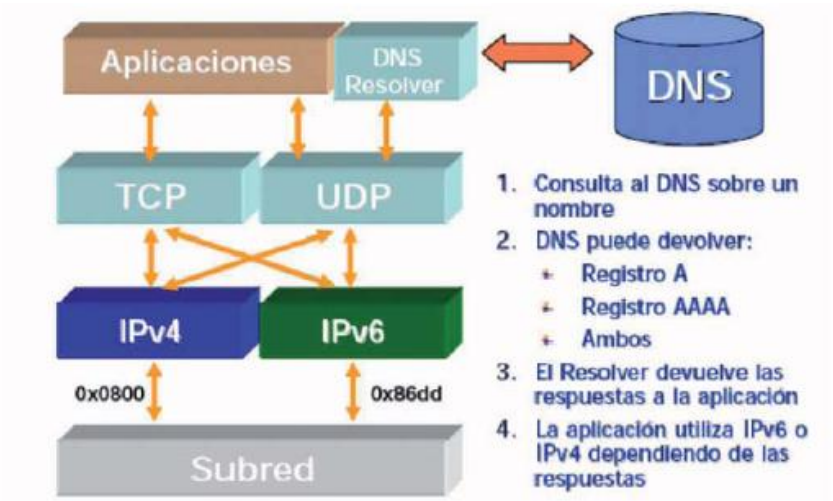


Figura 2.21 - Funcionamiento Pila Dual y DNS (Universidad Politecnica Salesian)

Ventajas y desventajas del uso de la Pila Dual:

Ventajas:

- Pueden coexistir en una misma organización.
- Evita problemas con los mecanismos de traducción.

Desventajas:

- Es necesaria la gestión de dos redes paralelas.
- Incrementa la dificultad en el desarrollo de las aplicaciones.

Túneles

El mecanismo de túneles también es llamado encapsulamiento. Con el encapsulamiento, a un protocolo se le agrega la cabecera de otro protocolo y se establece o trabaja encima de la infraestructura del segundo protocolo.

Túneles IPv4 a través de IPv6 (4en6): Se refiere a túneles de IPv4 en IPv6. El más común es el túnel 4in6. Es un mecanismo que permite la interoperabilidad del Protocolo de Internet versión 4 (IPv4) para ser utilizado en una red IPv6 nativa. 4in6 utiliza un túnel para encapsular el tráfico IPv4 sobre túneles IPv6 configurados tal como se define en el RFC 2473. Los túneles 4in6 suelen ser configurados manualmente pero se puede automatizar a través de protocolos como el TSP (Tunnel Setup Protocol) para permitir una fácil conexión a un Tunnel Broker (provee conectividad mediante encapsulación sobre una infraestructura existente hacia una nueva).

Túneles IPv6 a través de IPv4 (6en4): Estos mecanismos se usan para desplegar una red IPv6 que aún no cuenta con infraestructura propia, mientras que la infraestructura IPv4

global todavía es la base y no puede modificarse o actualizarse en un corto plazo.

La RFC 2893 define la utilización básica de túneles como mecanismo para transportar paquetes IPv6 sobre redes IPv4.

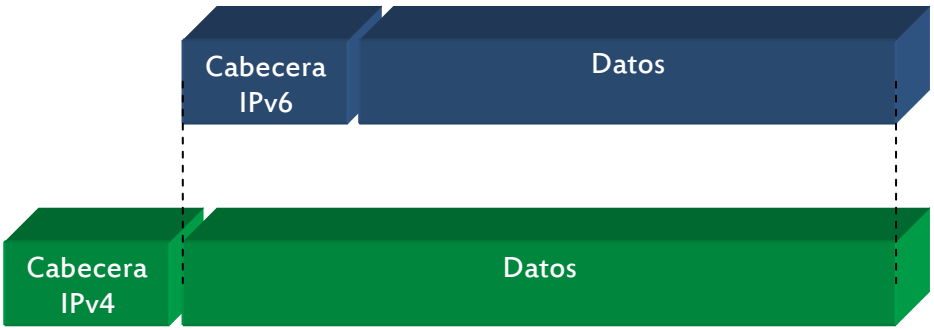


Figura 2.22 – Encapsulamiento IPv6 en IPv4 (Universidad Politecnica Salesian)

El objetivo principal de los túneles es que la infraestructura de enrutamiento existente que es IPV4 puede seguir funcionando y ser utilizada para transportar tráfico IPV6, mientras se da la transición.

En un túnel, el nodo de entrada (nodo de encapsulamiento) crea un paquete IPv4 en el que encapsula el paquete IPv6, y lo transmite encapsulado. La cabecera IPv4 contiene las direcciones fuente y destino y el cuerpo del paquete contiene

la cabecera IPv6 seguido inmediatamente por los datos. El nodo de salida del túnel (nodo de desencapsulamiento) recibe el paquete encapsulado, elimina la cabecera IPv4, actualiza la cabecera IPv6 y procesa el paquete IPv6 recibido.

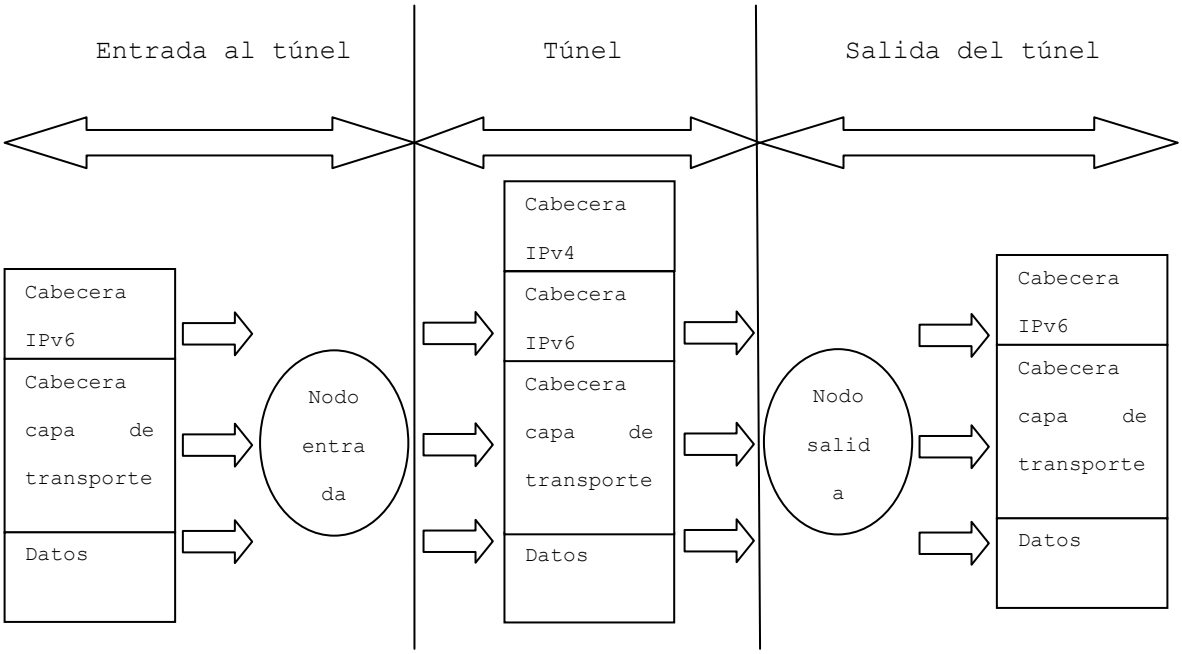


Figura 2.23 – Funcionamiento General Encapsulamiento

Existen diferentes tipos de túneles, cada uno con características diferentes que agregan o limitan su funcionalidad y aplicabilidad. Además, conforme el pasar del tiempo, nuevas técnicas de tunelización irán apareciendo y puede que dejen obsoletas a las técnicas diseñadas previamente. Existen empresas o asociaciones como SixXS que

se mantienen a la vanguardia de las nuevas técnicas y sus características, lo que facilita su análisis y comparación para fines de implementación. Obtenido el 27 de mayo de 2011, de (sixxs.net).

A continuación se detallan las técnicas de tunelización mayormente utilizados:

Túnel 6in4: es un mecanismo de transición para la migración de IPv4 a IPv6. 6in4 utiliza un túnel para encapsular tráfico IPv6 sobre enlaces IPv4 explícitamente configurados tal como se define en el RFC 4213 (que dejó obsoleto el RFC 2893 y RFC 1933). El tráfico 6in4 se envía a través de Internet dentro de paquetes IPv4 cuyos encabezados IP tienen el número de protocolo IP establecido en 41. Este número de protocolo está específicamente designado para la encapsulación de IPv6. En 6in4, la cabecera del paquete IPv4 es inmediatamente seguido por el paquete IPv6. Esto significa que la encapsulación de arriba es simplemente el tamaño de la cabecera IPv4 de 20 bytes. Una red Ethernet con unidad de transmisión máxima (MTU) de 1500 bytes, puede enviar los paquetes IPv6 de 1480 bytes sin fragmentación. Los túneles 6in4 son generalmente

configurados manualmente, pero por ejemplo, la Utilidad para la Conectividad Automática de Clientes IPv6 (AICCU por sus siglas en inglés) puede configurar los parámetros del túnel de forma automática después de recuperar su información desde el servidor de Información y Control Protocolo (TIC).

Cuando un extremo de un túnel 6in4 está detrás de un NAT, en algunos casos se puede hacer uso de la función DMZ de un router NAT. El router NAT envía todos los paquetes entrantes proto-41 al host configurado.

El protocolo 6in4 no tiene características de seguridad, por lo que fácilmente se puede inyectar paquetes IPv6 por suplantación de la dirección IPv4 de origen de un extremo del túnel y enviarlo al otro extremo. Este problema se puede resolver en parte mediante la aplicación de filtrado en la red o con IPSec. Otra solución es usar un protocolo seguro como AYIYA u otros métodos de hacer un túnel que calculan las firmas digitales para cada paquete, lo que facilita la verificación de la autenticidad del paquete.

Túnel 6over4: es un mecanismo de transición de IPv6 para transmitir paquetes IPv6 entre nodos con doble pila sobre una red IPv4 con multicast habilitado. IPv4 se utiliza como un nivel de enlace virtual (*Ethernet virtual*) sobre el que ejecutar IPv6 y posee soporte para autenticación.

6over4 define un método para generar una dirección IPv6 local a partir de una dirección IPv4, y un mecanismo para realizar un descubrimiento de vecinos (Neighbor Discovery) sobre IPv4.

Como limitante, 6over4 confía en la disponibilidad de multicast de IPv4, que no suele ser implementado en la infraestructura IPv4 (multicast es casi tan reciente como IPv6). 6over4 tiene poco uso práctico y no está soportado por los sistemas operativos más comunes.

Obtenido el 30 de mayo de 2011, de (ietf, 1998).

IPv6 de despliegue rápido (6rd): 6rd es un mecanismo para facilitar el despliegue de IPv6 en las infraestructuras IPv4 de los proveedores de servicios Internet (ISP). Es un mecanismo automático de túnel recientemente estandarizado por

la IETF que permite a los ISP implementar fácilmente IPv6 sobre una red IPv4 existente. Usando la dirección IPv4 y un conjunto estático de parámetros de configuración recibidos en el DHCPv4 opción 6rd, routers domésticos pueden asignar prefijos IPv6 de subredes en la LAN y configurar una ruta por defecto a través de un túnel IPv6 en IPv4 al router frontera 6rd del ISP.

Este mecanismo es fácilmente escalable a un gran número de clientes, ya que ni los routers de frontera 6rd de los ISP ni los servidores DHCPv4 requieren de ninguna configuración por parte de los clientes para el uso de 6rd.

Túnel 6to4: es un mecanismo de transición de Internet para la migración de IPv4 a IPv6, que permite que los paquetes IPv6 se transmitan a través de una red sin la necesidad de configurar túneles explícitos. Existen servidores relay especiales que permitirán a las redes 6to4 comunicarse con redes IPv6 nativas.

6to4 es especialmente relevante durante las fases iniciales de implementación para la conectividad total con IPv6 nativo,

ya que IPv6 no es necesario en los nodos entre el host y el destino. Sin embargo, se piensa sólo como mecanismo de transición y no está destinada a ser utilizada de forma permanente.

6to4 puede ser utilizado por un host individual, o por una red local IPv6. Cuando es utilizado por un host, debe tener una dirección IPv4 conectado, y el host es responsable de la encapsulación de los paquetes IPv6 de salida y desencapsulación de los paquetes 6to4 entrantes. Si el equipo está configurado para enviar paquetes a otros clientes, a menudo de una red local, entonces es un router.

La mayoría de las redes IPv6 utilizan la configuración automática, que requiere los últimos 64 bits para el host. Los primeros 64 bits son el prefijo IPv6. Los primeros 16 bits del prefijo siempre son de 2002: los próximos 32 bits son la dirección IPv4, y los últimos 16 bits del prefijo se eligen arbitrariamente por el router. Dado que el host IPv6 utiliza la configuración automática ya se ha determinado la porción de host único de 64 bits de su dirección, simplemente

hay que esperar por un Router Advertisement que indica los primeros 64 bits de prefijo para tener una direcciones IPv6.

Un router 6to4 sabrá que tiene que enviar un paquete encapsulado directamente sobre IPv4 si los primeros 16 bits son 2002.

6to4 no facilita la interoperabilidad entre nodos IPv4 y nodos IPv6. 6to4 es simplemente un mecanismo transparente utilizado como capa de transporte entre los nodos IPv6.

AYIYA (Anything in Anything): es un protocolo de tunelización utilizado para conectar islas IPv6 entre sí a través de una red IPv4 intermedia. Su nombre viene de la facultad que posee de encapsular los paquetes IPv6 usando diferentes protocolos a nivel de transporte como son TCP, UDP o SCTP. Además, posee la capacidad de atravesar NAT (NAT Traversal) sin que los paquetes o la información que contengan se vean afectados. Otra de las capacidades de AYIYA es su soporte para autenticación de los paquetes. Obtenido el 28 de Agosto de 2011, de (sixxs.net).

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol): es un mecanismo de transición IPv6, definido en el RFC 5214, que pretende transmitir paquetes IPv6 entre nodos de doble pila sobre una red IPv4.

A diferencia de 6over4, ISATAP utiliza IPv4 como un nivel de enlace de una red de acceso múltiple sin broadcast, por lo que no requiere que la red IPv4 subyacente soporte multicast.

ISATAP define un método para generar una dirección IPv6 local a partir de una dirección IPv4, y un mecanismo para realizar el protocolo de descubrimiento de vecinos (Neighbor Discovery Protocol) sobre IPv4.

Generación De La Dirección Local ("Link-Local"): Cualquier máquina que desee participar en ISATAP sobre una red IPv4 puede establecer una interfaz de red IPv6 virtual. La dirección local se determina mediante la concatenación de fe80:0000:0000:0000:0000:5efe: con los 32 bits de la dirección IPv4 (expresado en notación hexadecimal). Por ejemplo, el host 192.0.2.143 utilizaría fe80:0000:0000:0000:0000:5efe:c000:028f como su dirección

IPv6 local (192.0.2.143 es c000028f en la notación hexadecimal). La notación simplificada sería fe80::5efe:c000:28f.

Descubrimiento de vecinos: Como ISATAP utiliza IPv4 como un nivel de enlace sin capacidad de multicast/broadcast-capable (al contrario que Ethernet), el ICMPv6 Neighbor Discovery no se puede implementar de la forma habitual. Este es el motivo por el que ISATAP es un poco más complejo que 6over4.

El nivel de enlace asociado con una dirección IPv6 dada está incluido en los 32 bits más bajos de la dirección IPv6, por lo que el descubrimiento de vecinos no se necesita realmente. Sin embargo, la falta de capacidad multicast impide el uso del descubrimiento automático del router (Router Discovery). Por lo tanto, los hosts con ISATAP tienen que configurar una lista de routers posibles (Potential Routers List o PRL). Cada uno de estos routers es sondeado con poca frecuencia por un mensaje ICMPv6 de descubrimiento de router, para determinar cuáles de ellos están funcionando, y para realizar la autoconfiguración de "unicast-only".

Como limitante, ISATAP está implementado en Microsoft Windows Vista, Windows XP, Windows Mobile y en algunas versiones de Cisco IOS. Debido a una demanda de patentes, las primeras implementaciones fueron retiradas tanto de KAME (BSD) como de USAGI (Linux). Sin embargo IETF ha informado que los propietarios de las patentes no necesitan licencia para los implementadores.

ISATAP también conlleva los mismos riesgos de seguridad que 6to4, el enlace virtual IPv4 debe definirse con cuidado en el perímetro de la red, para que los hosts IPv4 externos no intenten ser parte del enlace ISATAP. Normalmente se puede evitar asegurando que el protocolo no pueda atravesar el corta fuegos.

L2TP (Layer 2 Tunneling Protocol): permite crear túneles IPv6 desde atrás de un NAT dinámico, encapsulando la información en paquetes UDP y usando PPP como protocolo de transporte. Obtenido el 17 de Julio de 2011, de (sixxs.net, 2011).

TSP: es un protocolo de red utilizado para negociar parámetros de configuración de túneles IP entre una maquina

cliente del túnel y su servidor Tunnel Broker (el otro extremo del túnel). Éste protocolo está definido en el RFC 5572 y es ampliamente usado como método de transición de IPv6 por su capacidad para negociar parámetros de túneles IPv6 sobre IPv4 e IPv4 sobre IPv6.

Teredo: es un protocolo tunelizado multiplataforma diseñado para garantizar conectividad IPv6 a nodos que están localizados en redes IPv4. Comparado con otros protocolos similares, este protocolo también es capaz de realizar su función en redes con dispositivos NAT.

Teredo define una manera de encapsular paquetes IPv6 en datagramas UDP IPv4 que pueden ser dirigidos a través de dispositivos NAT y en Internet IPv4. Fue desarrollado por Christian Huitema en Microsoft, y estandarizado por IETF como RFC 4380.

Traductores de Protocolos

Los traductores de protocolos se encargan de traducir datagramas IPv6 a IPv4 y viceversa. Permiten la comunicación

entre sistemas que trabajen únicamente con IPv4 y sistemas que operen solo con IPv6. Traducen las cabeceras de los paquetes entre IPv4 e IPv6 (sólo los campos comunes).

Las técnicas de traducción de protocolos se describen en los RFC 2765 y 2766 y ofrecen otros mecanismos de transición además de la pila dual y las técnicas de tunelización. El objetivo de los mismos es proveer rutas transparentes a los nodos en las redes de IPv6 para comunicarlos con los nodos de redes IPv4 y viceversa.

Tipos de Traductores:

SIIT Stateless IP/ICMP Translation: El SIIT es un algoritmo que traduce entre encabezados de paquetes IPv4 e IPv6 (incluyendo los encabezados ICMP). Este nuevo algoritmo puede usarse como la parte de una solución que permite a hosts IPv6 qué no tiene una dirección IPv4 permanentemente asignada, se comuniquen con hosts que trabajen solo con IPv4.

Con la aplicación de un traductor de protocolo, es posible adaptar la nueva red IPv6 internamente y tener clientes IPv6

que accedan mediante IPv4 a Internet o a cualquier otro nodo que aun trabaje sobre IPv4.

Para este propósito, un nuevo tipo de dirección se ha introducido: la dirección IPv4-traducible. El formato del prefijo para esta dirección es el 0::ffff:0:0:0/96. El identificador del host es una dirección de IPv4 que tiene que ser tomado de un grupo especial de direcciones y asignar al nodo de IPv6 que quiere comunicarse con los nodos de IPv4.

Cuando el traductor recibe un paquete IPv4 y su destino no se encuentra en la red, traduce el encabezado del paquete IPv4 en un encabezado de IPv6. Este es enviado basado en la dirección de destino de IPv6, el encabezado original es eliminado y reemplazado por el encabezado de IPv6, excepto los paquetes de ICPM, el encabezado de la capa de transporte y una porción de los datos quedan inalterados.

Un traductor IPv4-a-IPv6 recibe un datagrama IPv4. Porque está configurado para conocer el grupo de direcciones de IPv4 que representan los nodos de IPv6 interiores, el traductor sabe que el paquete necesita la traducción, entonces quita la

cabecera IPv4 y lo reemplaza con una cabecera IPv6 traduciendo toda la información del título de IPv4 en el título de IPv6.

Por otro lado, para todos los mensajes de ICMPv4, el traductor tiene que computar un checksum válido porque ésta es requerida para ICMPv6. Además de esto, el tipo de valores tienen que ser traducidos y, para los mensajes del error, la cabecera de IP incluida necesita también ser traducida. Las mismas reglas de traducción aplican a la traducción de mensajes de ICMPv6 a mensajes de ICMPv4, sólo en el orden inverso.

En el caso inverso, que la traducción sea de IPv6 a IPv4 el proceso no es muy diferente de la traducción IPv4 a IPv6. En este caso, el traductor sabe que tiene que traducir de IPv6 a IPv4 basado en la dirección del destino IPv4-mapped. Remueve la cabecera IPv6 y lo reemplaza con la cabecera IPv4.

NAT-PT: es una aplicación de SIIT que permite que haya una ruta transparente entre un grupo de hosts IPv6 que cuentan con direcciones IPv4, de la misma manera que NAT para IPv4

permite a un grupo de hosts IPv4 que usan direcciones privadas, puedan usar un grupo de direcciones públicas.

Este mecanismo usa un rango de direcciones de IPv4 para la asignación a los nodos de IPv6 en una base dinámica. Las direcciones IPv4 se asumen como globales y únicas.

En resumen el NAT-PT se coloca como una puerta de enlace entre dos redes, y este se encarga de traducir todas las direcciones de los paquetes que pasan a través de él.

NAT-PT ofrece una solución directa al problema de la interconectividad mediante el uso de enrutamiento transparente y traducción de direcciones y protocolos. De esta forma, aplicaciones en ambas redes pueden comunicarse sin problema alguno.

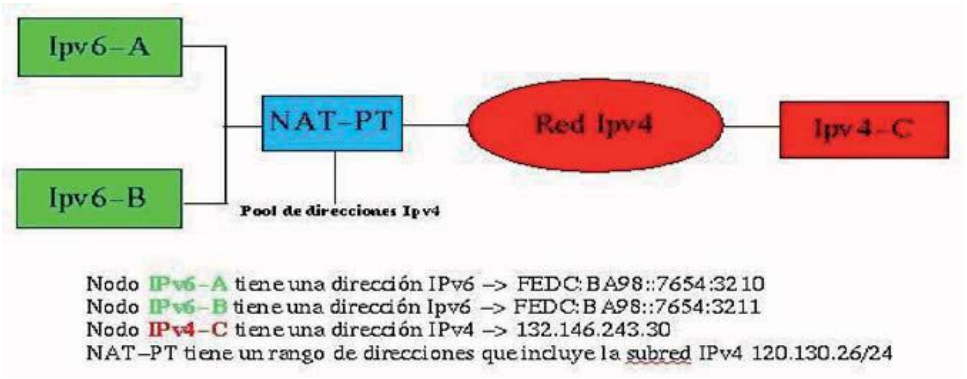


Figura 2.24 - Funcionamiento NAT-PT

Según la figura 2.24, si el nodo A quiere comunicarse con el nodo C, primeramente el nodo A crea un paquete de direcciones de origen y destino con su respectivo prefijo, este prefijo debe ser enrutable dentro la red IPv6, es decir los nodos deben ser configurados para que cualquier paquete que contenga ese prefijo en una dirección de destino sea enrutado al traductor para su traducción.

Cuando se inicia la comunicación por primera vez, el traductor le asigna al nodo A una dirección IPv4 de su rango (pool) de direcciones para que sus paquetes puedan ser enrutados a través de la red IPv4, cuando llega un paquete al traductor, las direcciones de origen y destino son traducidas.

NAT64 (RFC 6052 y RFC 6146): es un mecanismo que permite a hosts IPv6 comunicarse con servidores IPv4. El servidor NAT64 dispone de al menos una dirección IPv4 y un segmento de red IPv6 de 32-bits (por ejemplo 64:ff9b::/96). El cliente IPv6 construye la dirección IPv6 destino utilizando el rango anterior de 96 bits más los 32 bits de la dirección IPv4 con la que desea comunicarse, enviando los paquetes a la dirección resultante. El servidor NAT64 crea entonces un mapeo de NAT entre la dirección IPv6 y la dirección IPv4, permitiendo la comunicación.

Un entorno de NAT64 simplista puede verse como un dispositivo de red (un router, por ejemplo) con al menos dos interfaces. Una de los interfaces está conectada a la red IPv4, y la otra a la red IPv6. La red estará configurada de modo que los paquetes de la red IPv6 para la red IPv4 son encaminados a través de este router. El router realizará todas las traducciones necesarias para transferir paquetes de la red IPv6 a la red IPv4, y viceversa.

Bump in the Stack o BPI (RFC 2767): es un caso particular del NAT-PT con una implementación de pila dual en los hosts.

El mecanismo permite a los hosts comunicarse con otros hosts IPv6 usando las aplicaciones existentes de IPv4. Es decir podemos usar software o aplicaciones IPv4 que de una u otra forma no son compatibles con IPv6, el BPI permite utilizar dichas aplicaciones IPv4 sobre una red IPv6.

La idea es que cuando una máquina IPv4 necesite comunicarse con un nodo IPv6, a su dirección IPv6 se le asigna una dirección Ipv4 de un rango de direcciones que tiene la máquina. La traducción completa del paquete se hace de acuerdo a SIIT.

TRT Transport Relay Translator: Un Transport Relay Translator de IPv6 a IPv4, es un mecanismo que sirve para que hosts que trabajan solamente con IPV6 intercambien tráfico (TCP, UDP) con hosts que usen solamente IPv4. Un sistema de TRT traduce TCP, UDP/IPv6 a TCP, UDP/IPv4, o viceversa. Es decir este mecanismo traduce a nivel de capa de trasporte.

Este mecanismo se encarga de traducir conexiones TCP y paquetes UDP. La comunicación entre los nodos es directa y

transparente. Se coloca también como una puerta de enlace entre las dos redes.

A la máquina de traducción TRT le llegará algún rango de direcciones IPv6 las cuales traducirá a un rango de direcciones IPv4. Cuando una conexión IPv6 de TCP se hace a una de estas direcciones la máquina de traducción TRT hará una conexión de TCP a la dirección IPv4 correspondiente en el mismo puerto, de igual manera para UDP.

TRT se diseña para no requerir ninguna modificación extra en los hosts de inicio IPv6 ni en los hosts destino IPv4. Algunos otros mecanismos de traducción necesitan las modificaciones extras en los hosts de inicio IPv6, limitando su posibilidad de despliegue.

En los traductores de cabecera de IPv6 a IPv4 se debe tener cuidado con el camino MTU y problemas de fragmentación. Sin embargo, TRT es libre de este problema.

Método Analítico

El Método Analítico es aquel método de investigación que consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos para observar las causas, la naturaleza y los efectos. El análisis es la observación y examen de un hecho en particular. Es necesario conocer la naturaleza del fenómeno y objeto que se estudia para comprender su esencia. Este método nos permite conocer más del objeto de estudio, con lo cual se puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías.

Se distinguen los elementos de un fenómeno y se procede a revisar ordenadamente cada uno de ellos por separado. Consiste en la extracción de las partes de un todo, con el objeto de estudiarlas y examinarlas por separado, para ver, por ejemplo las relaciones entre las mismas.

Estas operaciones no existen independientes una de la otra; el análisis de un objeto se realiza a partir de la relación que existe entre los elementos que conforman dicho objeto

como un todo; y a su vez, la síntesis se produce sobre la base de los resultados previos del análisis.

Capítulo III

Situación Actual

La situación actual de la Universidad de El Salvador Facultad Multidisciplinaria de Occidente referente al área de redes y servidores, tanto en recursos humanos como técnicos está definida de la siguiente manera:

Recurso Técnico

Los recursos técnicos (equipo), que posee la institución en su mayoría y los más fundamentales, cuentan con la capacidad para realizar un despliegue del protocolo Ipv6, resultando esto positivo en la evaluación de la institución respecto a la capacidad técnica de implementación.

A continuación se detalla el diagrama de red a nivel cero (figura 3.1) del año 2010 con que cuenta la Universidad de El Salvador Facultad Multidisciplinaria de Occidente, el cual no presenta cambios significativos a la fecha.

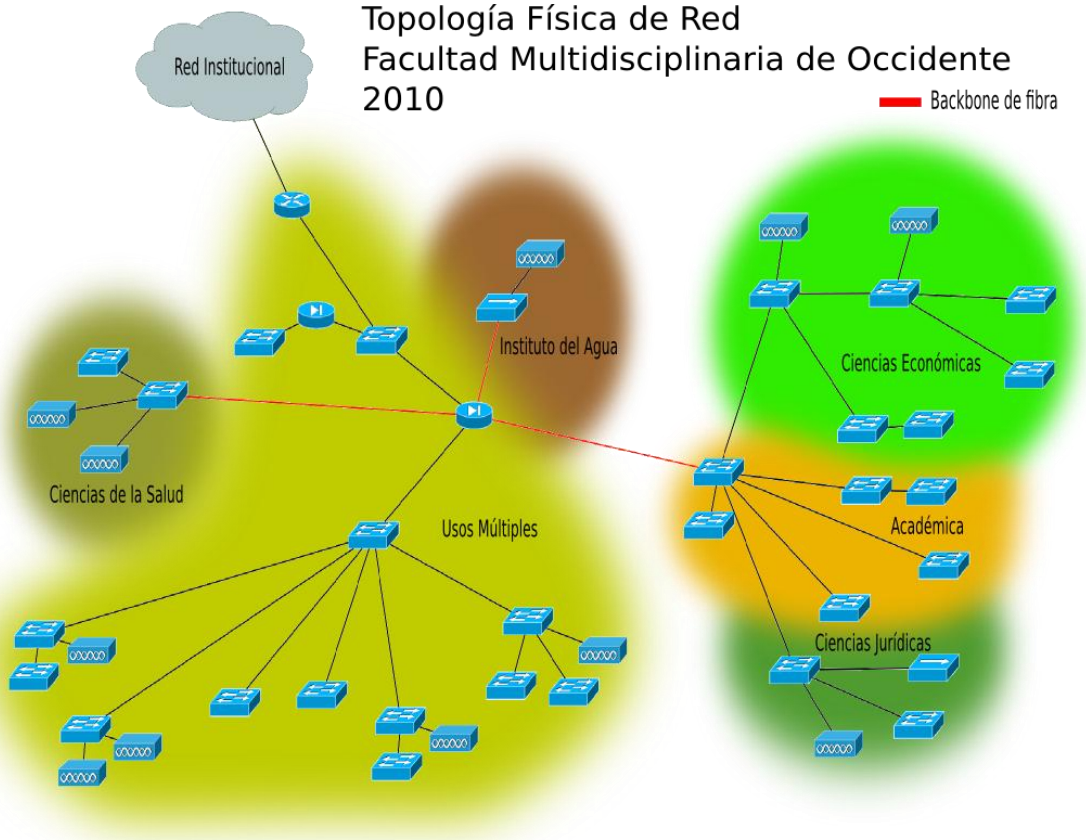


Figura 3.1 – Diagrama de Red UES-FMOcc

Por medidas de seguridad internas de la institución, hay datos técnicos los cuales son restringidos y pueden llegar a dejar algunos vacíos de información sobre la situación actual, pero se aclara que éstos no son indispensables para el desarrollo de este estudio.

Se detalla a continuación el listado de equipo con el cual cuenta la Universidad de El Salvador Facultad Multidisciplinaria de Occidente.

Servidores:

Dell Poweredge 700:

- Procesador Pentium 4 de 2.8 GHz.
- Memoria RAM de 1 GB DDR SDRAM, Máxima memoria soportada 4 GB.
- Disco Duro con capacidad de 160 GB interface Serial ATA.
- Adaptador de red. Data Link Protocol Ethernet, Fast Ethernet y Gigabit Ethernet.

Dell Poweredge 800:

- Procesador Celeron 2.53 GHz
- Tamaño de memoria caché 256.0 KB
- RAM DDR 256.0 MB / 4.0 GB (max)
- Disco Duro de 40.0 GB - Serial ATA
- Adaptador de Red. Data Link Protocol Ethernet, Fast Ethernet y Gigabit Ethernet.

Hp ProLiant DL180 G6 Server:

- Procesador Intel Xeon 5500 y 5600 series.
- Tamaño de memoria caché 12 MB, 8 MB ó 4 MB, Caché nivel 3.
- Memoria RAM 4, 8 ó 16 GB PC3-10600E DDR3 1067 PC3-8500 DDR3 1066.
- Máximo número de discos duros 25.
- Adaptador de red integrado HP NC362i, Puerto Dual integrado, Gigabit Server Adapter.

Hp e40:

- Procesador Pentium Pro 200 MHz.
- Tamaño de memoria caché 256 KB (instalada) / 256 KB (máxima) - L2 Cache.
- RAM 32 MB/ 384 MB (máxima).
- Disco duro de 2.1 GB.
- Adaptador de red PCI - Ethernet, Fast Ethernet.

Proliant ML370:

- Procesador Pentium III 1 Ghz.

- Tamaño de memoria caché 256 KB (instalada) / 256 KB (máxima) - L2 Cache
- Memoria RAM 256 MB.
- Disco duro de 18 GB.
- Adaptador de Red PCI - Ethernet, Fast Ethernet

Dell Poweredge sc1430:

- Procesador Intel Xeon 5000 con 3 GHz (hasta 2).
- Memoria caché 5000 secuencia: Caché de nivel 2 de 2 x 2 MB por procesador; 5100 secuencia: Caché de nivel 2 de 4 MB por procesador; 5300 secuencia: Caché de nivel 2 de 2 x 4 MB por procesador.
- RAM 533 MHz o 667 MHz; 4 DIMM para admitir hasta 8 GB
- Almacenamiento SAS de 3,5” (10.000 rpm): discos duros de 73 GB, 146 GB, 300 GB; SATA de 3,5” (a 7.200 rpm): discos duros de 80 GB, 160 GB, 250 GB, 500 GB.
- Adaptador de Red Broadcom Gigabit integrada.

Proliant ML370:

- Procesador Intel Xeon a 2.8 GHz, 3.0 GHz ó 3.2 GHz (Hasta 2 procesadores).

- Tamaño de memoria caché 1 MB ó 2 MB de caché de segundo nivel (según modelo).
- Memoria RAM 8 GB SDRAM ECC PC2700.
- Almacenamiento 6 discos duros SCSI de 1" (hot-plug o no hot-plug) ó 4 discos duros SATA hot-plug.
- Adaptador de red Broadcom 5721 10/100/1000 PCI-Express.

IBM XSerie 205:

- Procesador Intel Pentium 4 hasta 2.8GHz.
- Tamaño de Memoria Cache 512KB L2.
- RAM 128MB/2GB PC2100
- Disco Duro 360GB IDE, 587.2GB SCSI
- Adaptador Ethernet 10/100/1000

Equipo de red:

DGS-3100-24:

- Switch con 24 puertos GE y 4 puertos SFP.
- Soporte de stack físico vía 2 puertos de stack, 10GE de ancho de banda.
- Soporte 802.1Q VLAN.
- Soporte QoS.

- Características avanzadas de administración.
- Soporta múltiples estándares y protocolos de administración incluidos SNMP, RMON, Telnet, Web-based GUI, SSH/SSL Protocols, y DHCP Relay.

CISCO 2800:

- Dimensión (WxDxH) 43.8 cm x 41.9 cm x 4.5 cm.
- Peso 6.2 kg.
- RAM 128 MB (instalada) / 384 MB (max).
- Memoria Flash 64 MB (instalada) / 128 MB (max).
- Protocolo de enlace de datos Ethernet, Fast Ethernet.

Recurso Humano

Luego de analizar la situación sobre equipos y servicios con los que cuenta la institución abordamos el tema del recurso humano, el cual se convierte en uno de los factores de mayor importancia en una implementación de este tipo.

La institución cuenta únicamente con un empleado en el Área de Redes y Servidores, que cumple con las tareas tanto administrativas como técnicas de la misma, es poco para la

cantidad de trabajo que se debe realizar aun con la red actual.

Una implementación del protocolo IPv6 conlleva más trabajo al personal ya existente, el cual ha asegurado poseer conocimientos sobre implementación y administración de redes que trabajan sobre el protocolo IPv6, en las tres técnicas de transición mayormente utilizadas (Anexos 2 y 3).

Situación Actual del Medio

A la fecha los proveedores de servicios (ISP) en el país no han experimentado la demanda por parte de sus clientes exigiendo la disponibilidad de conexión al protocolo IPv6, esto afecta en gran medida una implementación del protocolo, pues se debe de buscar soluciones a la falta de conexión nativa al mismo, lo cual genera un incremento de los costos de implementación.

Diferentes representantes de algunas instituciones en el país fueron contactados por correo electrónico (Anexo 4) en sus

respuestas se refleja que a nivel nacional, no existen un interés por comenzar a experimentar con el nuevo protocolo.

Capítulo IV

Metodología para la Selección de la Técnica de Transición

La metodología diseñada tiene sus bases en el método analítico. Inicia con la identificación de los factores o variables necesarios para la implementación de las diferentes técnicas de transición entre los protocolos IPv4 e IPv6, para luego analizar su efecto y poder evaluarlas en la empresa o institución donde se realiza el estudio, enfocándose en el objetivo de sugerir la técnica de transición óptima para la misma y obteniendo todo lo necesario para lograr la aplicación de dicha técnica.

A continuación se detallan las variables o factores identificados y la definición de la metodología que sirve como guía para poder evaluar dichas variables y determinar la/s técnicas que puedan ser implementadas en la institución objeto de estudio.

Variables para la Evaluación de Técnicas de Transición

Las variables para identificar la técnica de transición que mejor se apegue a las condiciones y necesidades de una institución o empresa, se obtuvieron mediante el desmembramiento de los requerimientos que cada una de las técnicas necesitan para poder implementarse, agrupando dichas variables conforme a las relaciones existentes entre ellas. De acuerdo a esto han sido definidas principalmente en dos términos: técnicos y económicos.

Variables Técnicas: estas variables vienen dadas por la definición, requerimientos y limitantes de las técnicas de transición citadas en el Capítulo II. Estas variables son las que permiten determinar en primera instancia las técnicas de transición que son factibles de implementar en la institución dependiendo de las condiciones técnicas actuales e intereses de la misma.

Variables Económicas: estas variables aunque tienen una base técnica, son consideradas también económicas por la alta influencia que ejercen en términos monetarios. Dichas

variables ayudarán a la empresa o institución a determinar qué tan factible es implementar una técnica en particular de acuerdo a su condición económica actual y a la vez marcarán la necesidad de realizar una inversión para poder implementarlo. Sirven también como indicadores para la toma de decisión sobre si se realizará dicha inversión y así poder efectuar de nuevo la evaluación técnica y determinar si bajo las nuevas condiciones es factible la implementación la técnica de transición elegida previamente o si es mejor seleccionar otra.

Por otro lado, en caso que la técnica de transición seleccionada sea Túnel, deberán evaluarse otras variables para determinar el tipo de túnel que se deba implementar:

Variables para Túneles: estas variables son referidas a aspectos técnicos específicos de los túneles y los requerimientos necesarios para su implementación.

Definición de Variables

A continuación se detallan los aspectos o condiciones a considerar en cada una de las diferentes variables definidas para la evaluación de las técnicas de transición, las cuales serán de gran importancia para determinar qué técnica es la más adecuada a implementar según las condiciones técnicas y económicas de la empresa, así como también, el tipo de túnel que se deba implementar al resultar seleccionada la técnica de tunelización:

Variables Técnicas:

Acceso a Internet Vía IPv4: se refiere a la necesidad de la institución, tanto de acceder a internet para consumir algún servicio en IPv4, como para proveer acceso a los clientes externos IPv4 a los servicios que la institución presta.

Acceso a Internet Vía IPv6: se refiere a la necesidad de la institución, tanto de acceder a internet para consumir algún servicio en IPv6, como para proveer acceso a los clientes externos IPv6 a los servicios que la institución presta.

Disponibilidad de Servicios IPv4 en el Mercado: se refiere a la capacidad por parte de los ISPs en la región para proveer conectividad nativa del protocolo IPv4. Esta variable se verá afectada en el tiempo conforme el agotamiento de direcciones IPv4 sea más palpable.

Disponibilidad de Servicios IPv6 en el Mercado: se refiere a la capacidad por parte de los ISPs en la región para proveer conectividad nativa del protocolo IPv6.

Soporte IPv6 del Equipo de Red Externo para la Implementación de la Técnica de Transición: se refiere a la capacidad del equipo de red frontera (el que provee la conexión hacia internet o redes externas) para la implementación de las técnicas de transición respecto al soporte del protocolo IPv6.

Soporte IPv6 del Equipo de Red Interno para la Implementación de la Técnica de Transición: se refiere a la capacidad del equipo de red dentro de la institución para la implementación de las técnicas de transición respecto al soporte del protocolo IPv6.

Soporte IPv6 del Sistema Operativo en Hosts: en esta variable se considera el soporte IPv6 del sistema operativo instalado en los hosts de la institución.

Soporte IPv6 de los Programas y Aplicaciones Utilizados en la Institución: en ésta variable se consideran todos los programas que hacen uso de la red para su funcionamiento, tanto los programas desarrollados específicamente para la institución, como los diseñados para uso general.

Variables de Túneles:

NAT Traversal: es un término utilizado en las ramas telecomunicación (redes TCP/IP o conexiones UDP), que se refiere a la capacidad de ciertos protocolos o aplicaciones de atravesar Network Address Translation (NAT) sin que el paquete o información de la misma se vea afectada; donde NAT es un mecanismo utilizado por instituciones para brindar la conectividad a internet a sus hosts privados a través de una o varias direcciones IP públicas.

Autenticación: esta variable considera que la aplicación o método de tunelización tenga la capacidad de confirmar la procedencia de la información verificando la identidad digital del remitente de la comunicación.

Reverse DNS: esta variable se enfoca en la capacidad de los métodos tunelización de comunicar paquetes de resolución inversas de los DNS, la cual tiene una gran importancia en las técnicas de seguridad de la red, si la empresa necesita de esto, puede que inhabilite la capacidad de implementar ciertos métodos de tunelización.

Multicast en IPv4: esta variable hace referencia a las técnicas de tunelización que requieren que frente a ellos se encuentre una red IPv4 con soporte a la característica de IPv4 Multicast para poder llevar a cabo su comunicación, para el caso de redes donde esta característica no se encuentre habilitada no se puede hacer uso de ciertos métodos de transición.

Anycast IPv6: esta variable se refiere a la necesidad de ciertas técnicas de tunelización de hacer uso de la característica Anycast IPv6, para poder llevar a cabo su funcionamiento, para este caso cuando la característica no exista en la red, inhabilita la posibilidad de implementar ciertos métodos.

Variables Económicas:

Disponibilidad de Servicios IPv4 en el Mercado: en el ámbito económico, esta variable considera la posibilidad de la presencia o ausencia de servicios IPv4 en el mercado, ya sea que los ISPs dejen de prestar el servicio para este protocolo, o que no se cuente con una dirección IPv4 pública dadas la condiciones de agotamiento de dichas direcciones.

Disponibilidad de Servicios IPv6 en el Mercado: esta variable considera la capacidad de obtener la conectividad nativa a IPv6, ya sea porque algún ISP de la región provea dicho servicio o que sea necesaria la contratación de algún otro servicio para poder obtener dicha conectividad, por ejemplo con el servicio de Clear Channel.

Soporte IPv6 del Equipo de Red Externo para la Implementación de la Técnica de Transición: Esta variable es considerada de tipo económica dado que, en caso el equipo de red frontera no posea soporte IPv6, deberá adquirirse equipo que lo soporte o actualizarlo siempre que sea necesario para la implementación de una técnica en particular, lo cual implica una inversión para la institución.

Soporte IPv6 del Equipo de Red Interno para la Implementación de la Técnica de Transición: Esta variable es considerada de tipo económica dado que, en caso el equipo de red interno de la institución no posea soporte IPv6, deberá adquirirse equipo que lo soporte o actualizarlo siempre que sea necesario para la implementación de una técnica en particular, lo cual implica una inversión para la institución.

Soporte IPv6 del Sistema Operativo en Hosts: Esta variable es considerada de tipo económica dado que, en caso el sistema operativo en los hosts de la red interna de la institución no posea soporte IPv6, puede que deba adquirirse sistemas operativos (en caso sean propietarios) que lo soporte o

actualizarlo siempre que sea necesario para la implementación de una técnica en particular, lo cual implica una inversión para la institución.

Contratación de Servicios Especializados de Redes para la Implementación de la Técnica de Transición: en caso sea necesaria la contratación de cualquier otro servicio de redes (entendidos entre estos, servicios de desempaquetado para túneles o routers relay, etc.) para la implementación de una técnica en particular, se convertirá en una inversión adicional para la empresa o institución en estudio.

Capacitación del Recurso Humano para la Implementación de la Técnica de Transición y su Administración: esta variable indica si es necesario o no el capacitar al personal del área de redes de la institución tanto en la implementación del técnica de transición, como en la administración del mismo luego de su implementación.

Contratación de Consultoría Externa para la Implementación de la Técnica de Transición: en caso de que el personal del área de redes no cuente con la capacidad necesaria para

implementar la técnica o sea insuficiente en cantidad, será necesaria la contratación de una empresa para que realice la implementación del mismo.

Contratación de Nuevo Personal en el Área de Redes para Apoyo en la Implementación de la Técnica de Transición: si el personal del área de redes de la institución es insuficiente para la implementación de la técnica, será necesaria la contratación temporal de personal que sirva de apoyo mientras se realiza la implementación.

Contratación de Nuevo Personal en el Área de Redes para Apoyo en la Administración de la Técnica de Transición: si el personal del área de redes de la institución es insuficiente para la administración de la red luego de la implementación de la técnica de transición debido a la carga de trabajo que esto genera, será necesaria la contratación permanente de personal nuevo que sirva de apoyo continuo para la administración de la red implementada.

Definición de la Metodología para la Selección de la Técnica de Transición

En base a las variables previamente definidas, se ha diseñado la siguiente metodología que servirá como guía para seleccionar la técnica de transición para la migración del protocolo IPv4 al protocolo IPv6 que mejor se apegue a las necesidades y/o condiciones de la empresa o institución en estudio.

Cabe mencionar, que ésta metodología puede estar sujeta a cambios según nuevas técnicas de transición que vayan surgiendo en el mundo, las cuales por consiguiente, puede que generen nuevos factores o variables que necesiten ser evaluados para la implementación de los mismos.

El siguiente diagrama muestra los pasos a seguir para evaluar la Metodología de Selección de la Técnica de Transición:

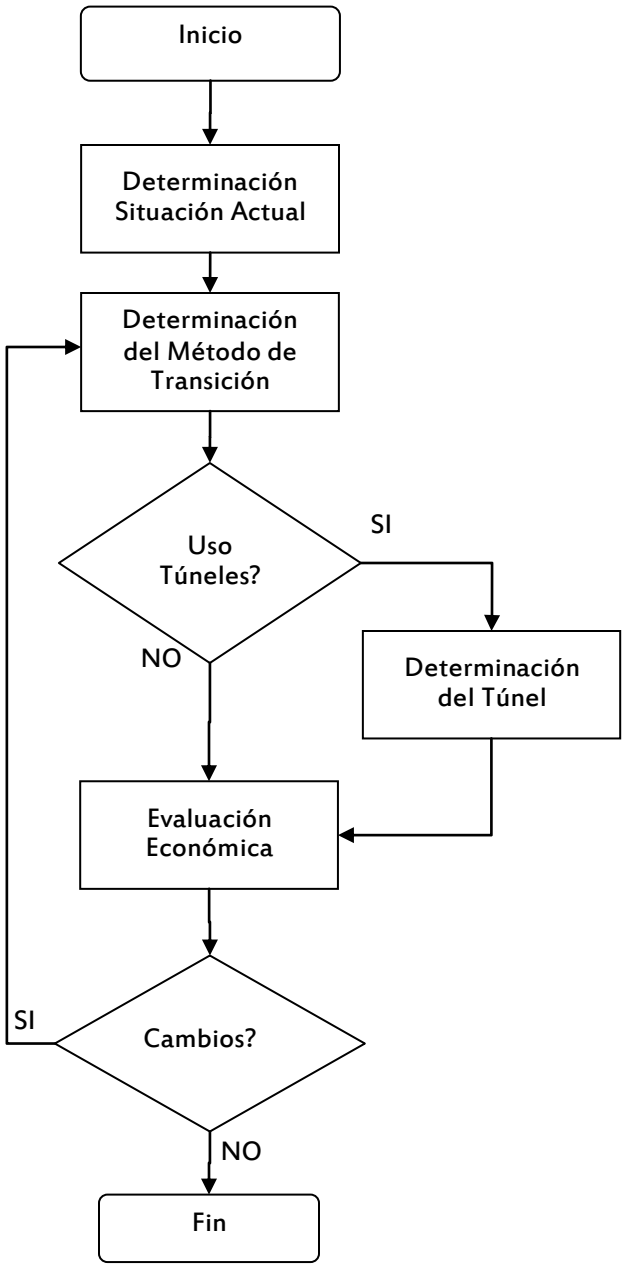


Figura 4.1 - Diagrama de Evaluación de Metodología para la Selección de la Técnica de Transición

A continuación se detallan los pasos a seguir para poder evaluar las técnicas de transición y determinar la factibilidad de su implementación.

Para ver ejemplos sobre la evaluación de la metodología y el llenado de las tablas de la misma, referirse a los anexos 6 y 8.

Determinación de la Situación Actual

En esta fase deberán recopilarse los datos referentes principalmente al área de redes de la empresa o institución objeto de estudio acerca de los siguientes criterios:

- Necesidad por parte de la empresa de consumir servicios de proveedores IPv6 o de proveer servicios a clientes IPv6 en la web.

- Necesidad por parte de la empresa de consumir servicios de proveedores IPv4 o de proveer servicios a clientes IPv4 en la web.

- Servicios de conectividad nativa IPv6 e IPv4 de los ISPs a nivel regional o internacional (dependiendo de la necesidad de conectarse a través del protocolo IPv6 y/o IPv4) y cotización los mismos en caso existan.
- Soporte del equipo de red existente en la institución para el protocolo IPv6 y las diferentes técnicas de transición expuestos anteriormente. En caso de no contar con dicho equipo, realizar la cotización de equipo con soporte para IPv6 para así determinar si es factible la obtención del mismo.

- Soporte IPv6 de los sistemas operativos instalados tanto en los equipos de los servidores de la empresa o institución, como en los hosts de la red interna de la misma.

- Soporte IPv6 de las aplicaciones instaladas en los servidores y hosts de la empresa o institución que necesiten realizar alguna conexión a través de la red. En caso se realice una migración al protocolo IPv6 deberán tomarse en cuenta estos aspectos, ya que tanto el software de aplicación, como las soluciones de

software diseñadas especialmente para la institución o empresa que necesite una conexión a través de la red, deberán contar con soporte para el protocolo IPv6, caso contrario, deberán sustituirse o actualizarse a una versión que ya cuente con dicho soporte.

Determinación de las Técnicas de Transición

Esta fase consiste en la evaluación de la información recopilada en la fase anterior, sometiendo estos a determinadas tablas que proporciona la metodología, con el fin de facilitar la selección de la técnica adecuada para la institución o empresa en base a su situación actual.

Para comenzar la evaluación se debe completar la tabla de variables técnicas, para ello se utiliza la información recopilada en la fase anterior de la metodología:

Código	Variables	Existe
1	Necesidades de acceso a Internet IPv6	
2	Necesidades de acceso a Internet IPv4	
3	Disponibilidad de servicios Ipv6	
4	Disponibilidad de servicios IPv4	
5	Soporte Ipv6 en equipo de Red externa	
6	Soporte IPv6 en equipo de Red Interna	

7	Soporte Ipv6 en Host
8	Soporte IPv6 en Sistemas Operativos de Host
9	Soporte IPv6 de Aplicaciones

Tabla 4.1 - Variables Técnicas

Es importante resaltar que los códigos que aparecen en la primera columna de la tabla son utilizados para reconocer las variables en las otras tablas que proporciona la metodología de selección.

El segundo paso es completar las tablas de evaluación para red interna y red externa (tablas 4.3 y 4.4) para determinar qué tipo de metodología se tendría que utilizar en cada una de las mismas, para ello se ha diseñado una tabla con los resultados de evaluar las variables contra las técnicas actuales de transición, la cual servirá como guía de cuales técnicas son viables implementar y cuáles no, según cada una de las variables expuestas existan o no en la empresa o institución, o en su medio. Dicha tabla se detalla a continuación:

	Técnicas / Variables	Existe					No Existe				
		NAT/ IPv6	**Pila Dual**	**Túnel 6en4**	**Túnel 4en6**	**IPv6**	**NAT/ IPv6**	**Pila Dual**	**Túnel 6en4**	**Túnel 4en6**	**IPv6**
1	Necesidades Acceso IPv6.	No	Si	Si	No	Si	Si	Si	Si	Si	Si
2	Necesidades Acceso IPv4.	Si	Si	Si	Si	No	No	Si	Si	No	Si
3	Disponibilidad Servicio IPv6	No	Si	No	Si	Si	Si	No	Si	No	No
4	Disponibilidad Servicio IPv4	Si	Si	Si	No	No	No	No	No	Si	Si
5	Soporte IPv6 en Equipo de Red Externo	Si	Si	Si	Si	Si	No	No	Si	Si	No
6	Soporte IPv6 en Equipo de Red Interno	Si	Si	Si	Si	Si	No	No	Si	Si	No
7	Soporte IPv6 Host	Si	Si	Si	Si	Si	No	No	No	No	No
8	Soporte IPv6 SO	Si	Si	Si	Si	Si	No	No	No	No	No
9	Soporte IPv6 App	Si	Si	Si	Si	Si	No	Si	Si	Si	No

Tabla 4.2 - Técnicas de Transición por Variable

La siguiente tabla es necesaria para la selección de la técnica a utilizar en la red interna de la empresa o institución. Para llevar a cabo esta evaluación se requiere rellenar con una marca (✓) la casilla correspondiente a cada variable, si es que la técnica evaluada puede ser implementada en la existencia o ausencia de dicha variable (según resultados de la tabla 4.2), caso contrario, si la técnica no puede ser implementado se le asignara una equis (x). La técnica evaluada como mejor es la que al finalizar la evaluación sume el mayor número de marcas en la matriz.

	1	2	6	7	8	9	Total
NAT/IPv6							
Pila Dual							
Túnel 6 en 4							
Túnel 4 en 6							
IPv6							

Tabla 4.3 - Evaluación Red Interna

Luego de rellenar esta tabla habrá que examinar que variables obtuvieron resultados negativos en cada técnica y evaluar si se cuenta con la posibilidad de modificar dicho estado de la variable para mejorar su calificación.

Después de la obtención de la técnica a utilizar en la red interna de la empresa o institución, se procede a la selección de la técnica de transición a utilizar en la red externa, la cual servirá para que pueda contar con una conexión a internet a través del protocolo IPv6 o IPv4, según sea requerido.

Para la selección de la técnica de transición para la red externa, se debe hacer uso de la tabla 4.2 con los resultados de las variables de red externa, como apoyo para rellenar la tabla 4.4, y en la columna total se reflejará el número de marcas que cada técnica de transición obtuvo en la evaluación, tomando como óptima la técnica con mayor número de marcas según la situación actual de la empresa.

	1	2	3	4	5	Total
NAT/IPv6						
Pila Dual						
Túnel 6 en 4						
Túnel 4 en 6						
IPv6						

Tabla 4.4 - Evaluación Red Externa

Luego de la determinación de la técnica de transición de la red externa e interna, si el resultado es un Túnel IPv6 sobre

IPv4, deberá realizarse otra evaluación para determinar el tipo de túnel que se deba implementar.

Determinación del Tipo Túnel

Para la determinación de los túneles tiene que llenarse la tabla 4.5, la cual cuenta con una serie de características que podrían manejar los diferentes túneles existentes en la actualidad y que pueden ser necesarios o requeridos por la institución en estudio.

Código	Variables	Se necesita
A	NAT Traversal	
B	Autenticación	
C	DNS Reverse	
Código	**Variables**	**Existe**
D	Multicast IPv4	
E	Anycast IPv6	

Tabla 4.5 - Requerimientos Túneles

Al igual que las tablas anteriores esta contiene una serie de características donde el usuario de la metodología confirmará la existencia o necesidad de las mismas para su red.

Para la selección de la técnica de tunelización óptima, la empresa o institución se tendrá que auxiliar de la tabla 4.6, la cual contiene los resultados de las variables en caso sean necesarias para la empresa o institución, o requeridas para la implementación del túnel. Las variables que tengan un "Si" por resultado denotarán que la técnica de tunelización posee soporte para dicha variable, por tanto, es factible su implementación, caso contrario, cuando tengan un "No", si es una variable que provee la técnica de tunelización (las marcadas con una "(P)") es porque dicha variable no se puede satisfacer con la técnica de tunelización en cuestión; si tiene un "No" y es una variable de requisito (las marcadas con una "(R)") es porque dicha variable no influye para la selección de esa técnica de tunelización en particular.

		6to4	6in4	6over4	6rd	AYIYA	ISATAP	L2TP	TSP / UDPv6	Teredo
A	**NAT Traversal (P)**	No	Si	No	Si	Si	No	Si	Si	Si
B	**Autenticación (P)**	No	No	No	No	Si	No	Si	Si	No
C	**DNS Reverse (P)**	Si	Si	Si	Si	Si	Si	Si	Si	No
D	**Multicast en IPv4 (R)**	No	No	Si	No	No	No	No	No	No
E	**Anycast en IPv6 (R)**	Si	No	No	No	No	No	No	No	No

Tabla 4.6 - Resultados Evaluación Túneles

Luego, con la ayuda de la tabla 4.6 se puede completar la siguiente matriz (tabla 4.7), dependiendo del tipo de variable que se esté evaluando:

Variables que provee la técnica de tunelización (P): se coloca una marca (✓) en la técnica de tunelización cuando sea requerida (tabla 4.5) y tenga un "Si" en la tabla 4.6, si es un "No" se colocará una (x); en caso no sea requerida (tabla 4.5), se coloca una marca (✓) en toda la columna de la tabla 4.7.

Variables requeridas por la técnica de tunelización (R): se colocará una marca (✓) en caso sea requerido por la técnica y exista dicho aspecto en la red que se esté trabajando, o cuando dicho aspecto no sea requerido (tenga un "No" en la tabla 4.6). Se colocará una (x) en caso dicho aspecto no pueda satisfacerse bajo las condiciones actuales de la red, en éste caso, la técnica de tunelización que no satisfaga el requerimiento es eliminada automáticamente de las técnicas factibles de implementación.

	A	B	C	D	E	Total
6to4						
6in4						
6over4						
6rd						
AYIYA						
ISATAP						
L2TP						
TSP/UDPv6						
Teredo						

Tabla 4.7 – Evaluación Túneles

La técnica de túnel con mayor número de marcas será la más apta para implementar en la institución o empresa, basándose solamente en los aspectos más generales de las técnicas de tunelización. Los literales en la parte superior son los códigos de las características o variables que podemos encontrar en la tabla 4.5 y 4.6.

Evaluación Económica

La Evaluación Económica es una fase opcional en la evaluación de la metodología, pues es decisión de la empresa o institución objeto de estudio el invertir en los factores contemplados en la misma. Esta evaluación servirá para descubrir si es factible la implementación de otras técnicas de transición mediante la inversión en alguno de los aspectos

que anteriormente hayan limitado la selección de una técnica en particular. Además, denotará aspectos cuya inversión sea necesaria para la correcta implementación y puesta en función de la técnica de transición seleccionada.

Para efectuar la evaluación económica se utilizará la siguiente tabla de variables:

Código	Variable	Inversión
1	Disponibilidad de Servicios IPv4 en el Mercado	
2	Disponibilidad de Servicios IPv6 en el Mercado	
3	Soporte IPv6 del equipo de red externo para la implementación de la técnica de transición	
4	Soporte IPv6 del equipo de red interno para la implementación de la técnica de transición	
5	Soporte IPv6 del Sistema Operativo en hosts	
6	Contratación de servicios especializados de redes para la implementación de la técnica de transición	
7	Capacitación del Recurso Humano para la implementación de la técnica de transición y su administración	
8	Contratación de consultoría externa para la implementación de la técnica de transición	
9	Contratación de nuevo personal para el área de redes para apoyo para la implementación de la técnica de transición	
10	Contratación de nuevo personal para el área de redes para apoyo para la administración de la técnica de transición	

Tabla 4.8 - Evaluación de Variables Económicas

Las variables sobre las cuales se pueda o se desee invertir se les colocará una marca (✓), y en las que no se desee invertir se les colocará una equis (x).

En caso sea factible la inversión en una de las variables numeradas entre el 1 y el 5, deberá realizarse de nuevo la evaluación técnica, ya que estas variables corresponden a las variables técnicas del mismo nombre, las cuales, al realizar una inversión y obtener acceso a ellas, afectará de manera directa y positiva a las demás técnica de transición que no hayan sido seleccionadas como óptimas, pues los aspectos contemplados en esas variables permiten o limitan la implementación de algunas de las técnicas.

Por otro lado, las variable del 6 al 10 son principalmente indicadores que muestran la necesidad de invertir sobre ciertos aspectos que sean necesarios para la ejecución de la implementación, pero que no limitan de manera técnica la selección de alguna de las técnicas de transición, por lo tanto, no deberá realizarse de nuevo la evaluación técnica.

Es importante mencionar, que éstas variables permiten tener una perspectiva más amplia sobre las diferentes técnicas que se pueden implementar y sobre los gastos en los que pueda incurrir la empresa o institución objeto de estudio para su

implementación, pero no se basan en las condiciones económicas de la misma.

Conclusiones

Al evaluar las condiciones de la Universidad de El Salvador Facultad Multidisciplinaria de Occidente utilizando la Metodología de Selección de Técnicas de Transición diseñada en éste trabajo de grado, se obtuvo como resultado que las técnicas óptimas para la implementación transitiva del protocolo IPv6 en la institución son la técnica denominada Doble Pila a nivel de la red interna de la misma, con el fin de mantener en funcionamiento tanto el protocolo IPv6 e IPv4 en dicha red; y a nivel de red externa (conexión a internet) la técnica de transición Túnel 6in4 dado que aun no existen implementaciones nativas de IPv6 a nivel de ISPs.

- La Universidad de El Salvador Facultad Multidisciplinaria de Occidente cuenta con equipo de red con soporte para implementación del protocolo IPv6, lo que a la vez provee la posibilidad de realizar pruebas sobre el nuevo protocolo y sus características y funciones, e incluso faculta a la institución para poder realizar implementaciones del mismo en su red.

- Los prototipos son modelos a escala basados en la red de la Universidad de El Salvador Facultad Multidisciplinaria de Occidente que demuestra de una forma minimalista la implementación de las técnicas sugeridas por la Metodología de Selección de Técnicas de Transición.

- La información encontrada en todo el documento es un punto relevante para obtener el conocimiento básico sobre los 2 protocolos tanto IPv4 como IPv6, así también se puede encontrar información de las principales diferencia entre los mismos, software que pueden trabajar sobre ellos; así como también conocimiento general de las técnicas de transición más utilizadas a nivel mundial, e información necesaria para lograr una mejor comprensión de la Metodología para la Selección de Técnica de Transición.

Recomendaciones

- Considerando que el estudio realizado determinó la factibilidad de que la Universidad de El Salvador Facultad Multidisciplinaria de Occidente implemente el protocolo IPv6 en la red, se recomienda primeramente realizar pruebas dentro de un ambiente controlado para observar el comportamiento de los equipos y servicios trabajando con dicho protocolo.

- A corto o mediano plazo, mantener la comunicación a través del protocolo IPv4, mientras se da el proceso migratorio hacia el protocolo IPv6.

- La metodología se puede ver afectada con la aparición de nuevas técnicas de transición, para lo cual se debe de realizar un análisis de las nuevas variables que puedan afectar a la metodología y así poder considerar dentro de ésta las nuevas técnicas.

- El equipo de red con el que cuenta la Universidad de El Salvador Facultad Multidisciplinaria de Occidente en su mayoría brinda el soporte para realizar una

implementación del protocolo IPv6 a nivel de conectividad a lo cual fue orientado el proyecto, dicho esto se recomienda la investigación futura de medidas de seguridad para una implementación de este tipo, de la mano a una evaluación del equipo y software de la institución en cuanto al soporte para dichas medidas.

- Los prototipos creados fueron realizados en base al esquema de red proporcionado por la institución, en el cual fueron omitidos ciertos equipos así como software por motivos de seguridad, los cuales en caso de realizar una implementación aun en un ambiente de prueba se recomienda considerarlos.

Glosario

6over4: Una tecnología IPv6 diseñada para favorecer la coexistencia con IPv4, que proporciona conectividad unicast y multicast a través de una infraestructura IPv4 con soporte para multicast, empleando la red IPv4 como un enlace lógico multicast.

6to4: Una tecnología IPv6 diseñada para favorecer la coexistencia con IPv4, que proporciona conectividad unicast entre redes y máquinas IPv6 a través de una infraestructura IPv4. 6to4 utiliza una dirección pública IPv4 para construir un prefijo global IPv6.

Anycast (dirección): Es una dirección del rango reservado para las direcciones unicast que identifica múltiples interfaces y es empleada para la entrega de uno a uno-entre-varios. Con un ruteo apropiado, los datagramas dirigidos a una dirección de tipo anycast serán entregados en una única interfaz, la más cercana.

Cabecera de fragmentación: Una cabecera de extensión IPv6 que contiene información para reensamblado para ser utilizada en el nodo receptor.

Cabecera de opción hop-by-hop: Una cabecera de extensión de IPv6 que contiene opciones que deben ser procesadas por todos los routers intermedios y el final.

Cabeceras de extensión: Cabeceras que se sitúan entre la cabecera IPv6 y las cabeceras de los protocolos de nivel superior que son empleadas para dotar de funcionalidades adicionales a IPv6.

Descubrimiento del Path MTU: Consiste en el empleo del mensaje Too Big mediante ICMPv6 para descubrir el valor máximo de MTU IPv6 en todos los enlaces entre dos equipos.

DHCP (Dynamic Host Configuration Protocol): Un protocolo de configuración con estado ("stateful") que proporciona direcciones IP y otros parámetros de configuración para conexión a una red IP.

Dirección IP: Identificador asignado a nivel de la capa de red a un interfaz o conjunto de interfaces que puede ser empleado como campo de origen o destino en datagramas IPv6.

DNS (Domain Name System): Un sistema jerárquico de almacenamiento y su protocolo asociado para almacenar y recuperar información sobre nombres y direcciones IP.

ESP (Encapsulating Security Payload): Una cabecera y cola de extensión IPv6 que proporciona autenticación del origen de datos, integridad y confidencialidad de datos y servicio anti-repetición para la carga del datagrama encapsulado por la cabecera y cola.

EUI (Extended Unique Identifier): Dirección del nivel de enlace definida por el IEEE (Institute of Electrical and Electronic Engineers).

Fragmentación: Proceso por el que se divide la carga de un datagrama IPv6 en fragmentos por la máquina emisora de modo que todos los fragmentos tienen una MTU apropiada al camino a seguir hasta el destino.

Fragmento: Una porción de una carga enviada en un datagrama IPv6 enviada por un host. Los fragmentos contienen una cabecera de fragmentación.

Gateway: es un dispositivo, que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

Host o nodo: Una máquina que es típicamente el origen y destino del tráfico IP y va a descartar discretamente tráfico que no esté dirigido específicamente a él mismo.

IANA: es la Agencia de Asignación de Números de Internet. Era el antiguo registro central de los protocolos Internet, como puertos, números de protocolo y empresa, opciones y códigos. Fue sustituido en 1998 por ICANN.

ICANN: Es una corporación sin fines de lucro de beneficio público con participantes de todo el mundo dedicados a

mantener la seguridad, estabilidad y la interoperabilidad de Internet. Promueve la competencia y desarrolla políticas sobre los identificadores únicos de Internet.

IETF: Internet Engineering Task Force. Es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad. Fue creada en EE.UU. en 1986. La IETF es mundialmente conocida por ser la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC.

Interfaz: Una representación de un nexo físico o lógico de un nodo a un enlace. Un ejemplo de un interfaz físico es un interfaz de red. Un ejemplo de un interfaz lógico es un interfaz de túnel.

Internet 2: es un consorcio de redes avanzadas dirigido por la comunidad de investigación y educación de los EE.UU. Tecnologías avanzadas que permiten servicios y logros más allá del alcance de las instituciones individuales.

IPSec (Internet Protocol Security): Seguridad del protocolo de Internet. Un marco de estándares abiertos que proporciona comunicaciones privadas y autenticadas a nivel de red, por medio de servicios criptográficos. IPSEC soporta autenticación a nivel de entidades de red, autenticación del origen de datos, integridad y cifrado de datos y protección ante repeticiones.

ISATAP (Intra-Site Automatic Tunneling Addressing Protocol): Una tecnología de coexistencia que proporciona conectividad IPv6 unicast entre máquinas IPv6 situadas en una intranet IPv4. ISATAP, obtiene un identificador de interfaz a partir de la dirección IPv4 (pública o privada) asignada a la máquina. Este identificador se utiliza para el establecimiento de túneles automáticos a través de la infraestructura IPv4.

ISP: es una empresa que brinda conexión a Internet a sus clientes.

Link-Local (dirección): Es la dirección IPv6 ::1, que se asigna a la interfaz local.

MAC (dirección): Dirección de nivel de enlace de tecnologías típicas de redes locales como Ethernet, Token Ring y FDDI. También se la conoce como dirección física, dirección del hardware o dirección del adaptador de red.

MTU (Unidad Máxima de Transmisión): Es la unidad de datos del protocolo más grande que se puede enviar. Las unidades máximas de transmisión se definen a nivel de enlace (tamaño máximo de trama) y a nivel de red o de Internet (tamaño máximo de los paquetes IPv6).

Multicast (dirección): Es una dirección que identifica múltiples interfaces y que se emplea en entregas de datos uno-a-muchos. Mediante la topología de ruteo multicast apropiada, los paquetes dirigidos a una dirección multicast se entregarán a todas las interfaces identificadas por ella.

NAT (Network Address Translator): Es un router IP que traduce direcciones y puertos al reenviar paquetes entre una red con direcciones privadas e Internet.

Neighbor Discovery: Es un conjunto de mensajes y procesos ICMPv6 que determinan las relaciones entre nodos vecinos. El descubrimiento de vecinos reemplaza a ARP, el descubrimiento de rutas ICMP y el mensaje de redirección ICMP empleados en IPv4. También proporciona detección de vecino inaccesible.

Nodo IPv4: Un nodo que implementa IPv4; puede enviar y recibir paquetes IPv4. Puede ser un nodo con soporte sólo IPv4 o un nodo dual IPv4/IPv6.

Nodo IPv6: Nodo que implementa IPv6; puede enviar y recibir paquetes IPv6. Un nodo IPv6 puede ser bien un nodo con soporte IPv6 o un nodo dual IPv6/IPv4.

Paquete: La unidad de datos del protocolo (PDU) existente a nivel Internet. En el caso de IPv6, un paquete consta de una cabecera y la carga útil IPv6.

Path MTU (MTU de ruta): Tamaño máximo de un paquete IPv6 que puede enviarse sin emplear fragmentación entre una fuente y un destino sobre una ruta en una red IPv6. La path MTU ruta

coincide con la menor MTU de enlace para todos los enlaces de dicha ruta.

PDU: Conjunto de datos correspondiente a una capa concreta en una arquitectura de red en capas. La unidad de datos de la unidad n se convierte en la carga útil de la capa n-1 (la capa inferior).

Pila Dual: Una arquitectura para nodos IPv6/IPv4 en la que existen dos implementaciones completas de la pila de protocolos, una para IPv4 y otra para IPv6, cada una de ellas con su propia implementación de la capa de transporte (TCP y UDP).

PPP: también llamado protocolo punto a punto, es un protocolo de nivel de enlace estandarizado en el documento RFC 1661 asociado a la pila TCP/IP de uso en Internet.

Prefijo de red: Es la parte fija de la dirección que se utiliza para determinar el identificador de la subred, la ruta o el rango de direcciones.

RAICES: es la Red Nacional de Investigación y Educación de El Salvador (NREN) y es miembro fundador de CLARA (Cooperación Latino Americana de Redes Avanzadas). Es socio local de DANTE (Delivering Advanced Network To Europe) y de CLARA para el Proyecto ALICE (América Latina Interconecta con Europa) y su continuación, ALICE2.

Red: Dos o más subredes conectadas por routers.

RFC: o Request For Comments por sus siglas en inglés, son una serie de notas sobre internet que comenzaron a publicarse en 1969. Cada una de ellas individualmente es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de Internet, que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades. Pueden encontrarse en http://tools.ietf.org/html/.

RIR: Registro Regional de Internet por sus siglas en inglés. Es una organización que supervisa la asignación y el registro de recursos de números de Internet dentro de una región particular del mundo. Los recursos incluyen direcciones IP

(tanto IPv4 como IPv6) y números de sistemas autónomos (para su uso en encaminamiento BGP).

Router Advertisement: Mensaje de descubrimiento de vecinos enviado por un router bien de forma pseudo-periódica o como respuesta a un mensaje de solicitud de router. El anuncio incluye al menos información acerca de un prefijo que será el que luego utilice el host para calcular su dirección IPv6 unicast según el mecanismo "stateless".

Router Discovery: Procedimiento de descubrimiento de vecinos que permite descubrir los routers conectados en un determinado enlace.

Router Relay: Un router IPv6/IPv4 que redirige tráfico dirigido a direcciones 6to4 entre routers 6to4 en Internet y máquinas de la Internet IPv6.

Router: Nodo que puede retransmitir datagramas que no van específicamente destinados a él. En una red IPv6 un router suele enviar además anuncios relativos a su presencia y su información de configuración.

Transición: Hablando de IPv6, consiste en la conversión de nodos sólo IPv4 a nodos con doble pila, o sólo IPv6.

Túnel: Un túnel IPv6 sobre IPv4, en los que los puntos finales son determinados por configuración manual.
Túneles IPv6 sobre IPv4: Consiste en enviar paquetes IPv6 con una cabecera IPv4, de forma que el tráfico IPv6 pueda enviarse sobre una infraestructura IPv4. En la cabecera IPv4, el campo de Protocolo toma el valor 41.

Tunnel Broker: es un servicio que provee un túnel en la red (Internet). Estos túneles proveen conectividad encapsulando los paquetes de nuevas infraestructuras de red para que puedan viajar a través de infraestructuras ya existentes.

Unicast (dirección): Dirección que identifica a una única interfaz y que permite comunicaciones punto a punto a nivel de red. El alcance o ámbito de utilización de esa dirección es precisamente aquél en el que esa dirección es única.

Bibliografía

¿CÓMO SE ELABORA UN CUESTIONARIO? (s.f.). Recuperado el 16 de mayo de 2011, de ¿CÓMO SE ELABORA UN CUESTIONARIO?: http://www.scribd.com/doc/238904/COMO-SE-ELABORA-UN-CUESTIONARIO

Barrios Dueñas, J. (2009). *Introduccion a IP version 4*. Recuperado el 4 de mayo de 2011, de http://www.alcancelibre.org/staticpages/index.php/introduccion-ipv4

Consuintel. (s.f.). *Consuintel.com.* Recuperado el 30 de Mayo de 2011, de Tutorial de IPv6: http://www.consulintel.com/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf

Consuintel. (s.f.). *ipv6 cuba.* Recuperado el 30 de Mayo de 2011, de IPv6 la siguiente generacion: http://www.cu.ipv6tf.org/pdf/IPv6%20-%20La%20Nueva%20Generacion.pdf

Contato-i. (s.f.). *contacto-i.* Recuperado el 27 de Julio de 2011, de http://www.contacto-i.org/site/index.php?option=com_content&view=article&id=138:seleccion-de-tecnologia&catid=39:guia-practica-para-hacer-seleccion-de-tecnologia&Itemid=55

Curso de protocolos TCP/IP. (9 de octubre de 2001). Recuperado el 4 de mayo de 2011, de Protocolo ARP: http://www.saulo.net/pub/tcpip/a.htm

Finlayson, M. M. (Junio de 1984). *Request for Comments: 903* . Recuperado el 4 de mayo de 2011, de RARP: http://www.ietf.org/rfc/rfc0903.txt

IANA. (22 de 4 de 2010). *Internet Control Message Protocol (ICMP) Parameters.* Recuperado el 4 de mayo de 2011, de Internet Control Message Protocol (ICMP) Parameters: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml

ietf. (agosto de 1998). *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*. Recuperado el 30 de mayo de

2011, de Transmission of IPv6 over IPv4 Domains without Explicit Tunnels: http://tools.ietf.org/html/draft-carpenter-ipng-6over4-04

Internet Society. (enero de 2002). *isoc member briefi ng #6.* Recuperado el 26 de mayo de 2001, de The Transition to IPv6: http://www.isoc.org/briefings/006/isocbriefing06.pdf

IPv6 chile. (s.f.). *Mecanismos de Transición IPv4/IPv6.* Recuperado el 12 de Junio de 2011, de Mecanismos de Transición IPv4/IPv6: http://www.ipv6.cl/noticia/mecanismos-de-transicion-ipv4ipv6

López Ruiz, M., Schmelkes, C., & Crespo, J. C. (julio de 2002). *Monografias.com.* Obtenido de Diseño de cuestionarios: http://www.monografias.com/trabajos15/disenio-cuestionarios/disenio-cuestionarios.shtml

Maxitrucos.com, & Rodriguez, M. C. (2 de Septiembre de 2003). *IPv6 El cercano gran desconocido.* Recuperado el 4 de Mayo de 2011, de IPv6 El cercano gran desconocido: http://www.evidalia.es/trucos/index_v2-261-11.html

network world & Eric Carmès. (1 de marzo de 2002). *De IPv4 a IPv6: asegurando la coexistencia.* Recuperado el 25 de mayo de 2011, de De IPv4 a IPv6: asegurando la coexistencia: http://www.networkworld.es/De-IPv4-a-IPv6:-asegurando-la-coexistencia/seccion-Telecomunicaciones/articulo-131858

Plummer, D. C. (noviembre de 1982). *Request For Comments: 826.* Recuperado el 4 de mayo de 2011, de ARP: http://www.rfc-es.org/rfc/rfc0826-es.txt

RAICES. (Diciembre de 2005). *Red Avanzada de Investigación, Ciencia y Educación Salvadoreña (RAICES)*. Recuperado el 4 de Mayo de 2011, de Red Avanzada de Investigación, Ciencia y Educación Salvadoreña (RAICES): http://www.raices.org.sv/

Ralli Ucendo, C. (s.f.). *Mecanismos de Transicion IPv4 – IPv6.* Recuperado el 11 de Julio de 2011, de http://www.cu.ipv6tf.org/pdf/carlos_ralli_transitiontutorial.pdf

sixxs.net. (s.f.). *AYIYA*. Recuperado el 28 de agosto de 2011, de AYIYA: http://www.sixxs.net/tools/ayiya/

sixxs.net. (s.f.). *Frequently Asked Questions (FAQ)*. Recuperado el 27 de mayo de 2011, de IPv6 Transition Mechanism / Tunneling Comparison: http://www.sixxs.net/faq/connectivity/?faq=comparison

sixxs.net. (4 de Julio de 2011). *Tuneles*. Recuperado el 17 de Julio de 2011, de L2TP: http://www.sixxs.net/wiki/L2tp

Universidad de Malaga. (2002). *Herramientas web para la enseñanzas de protocolos de comunicacion*. Recuperado el 4 de mayo de 2011, de El protocolo ICMP: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/icmp.html

Universidad Nacional de La Matanza (Marcelo Claudio Périssé). (27 de Junio de 2008). *www.cyta.com.ar.* Recuperado el 27 de Junio de 2011, de Internet2 e IPV6: http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/ipv6/ipv6.htm

Universidad Politécnica de Madrid. (11 de enero de 2010). *Protocolo IPsec.* Recuperado el 4 de mayo de 2011, de IPsec:

http://laurel.datsi.fi.upm.es/proyectos/teldatsi/teldatsi/protocolos_de_comunicaciones/protocolo_ipsec

Universidad Politecnica Salesian. (s.f.). *Herramientas de transicion a IPv6.* Recuperado el 2 de 6 de 2011, de Herramientas de transicion a IPv6: http://dspace.ups.edu.ec/bitstream/123456789/205/3/Capitulo%202.pdf

Urueña León, E. E. (2005). *Direccionamiento IPv4.* Recuperado el 4 de mayo de 2011, de http://www.monografias.com/trabajos30/direccionamiento-ip/direccionamiento-ip.shtml

UTFSM (FELIPE ERNESTO JARA SABA). (abril de 2009). *Estudio e Implementacion de una Red IPv6 en la UTFSM.* Recuperado el 1 de mayo de 2011, de Estudio e Implementacion de una Red IPv6 en la UTFSM: http://portalipv6.lacnic.net/files/documentos/ImplementacionIpv6_UTFSM_proyecto.pdf

Anexos

Anexo 1

Presupuesto servicios de Conectividad de Redes

Ciudad Universitaria, 6 de Octubre de 2009

Lic. Noe Navarrete
Vicerrector Administrativo

Presente

Universidad de El Salvador
AMERICA CENTRAL

Estimado Lic. Navarrete,

Por este medio le saludo, deseándole éxitos en su gestión.

Por este medio entrego a usted el requerimiento técnico de servicios de Conectividad de Redes y a la vez solicito su amable gestión para facilitar la contratación de estos servicios durante el periodo del 1 de Enero de 2010 al Diciembre 31 de 2010.

Es.	Ca	Articulo	Descripción	Precio	M.	Total
54203	1	Línea Dedicada	[illegible]	[illegible]	[illegible]	[illegible]
54203	1	Línea Dedicada	[illegible]	[illegible]	[illegible]	[illegible]
54203	1	Línea Dedicada	Enlace Campus Central – Santa Ana	$700.00	10Mb	$700.00
54203	1	Línea Dedicada	[illegible]	[illegible]	[illegible]	[illegible]
54203	1	Línea Dedicada	Enlace Campus Central – Redes Avanza-das	$700.00	10Mb	$700.00
54203	20	Acceso a Internet	[illegible]	[illegible]	[illegible]	[illegible]
54203	1	Acceso a Internet	[illegible]	[illegible]	[illegible]	[illegible]
54203	1	Acceso a Internet	[illegible]	[illegible]	[illegible]	[illegible]
54203	1	Acceso a Internet	[illegible]	[illegible]	[illegible]	[illegible]
54203	1	Acceso a Internet	[illegible]	[illegible]	[illegible]	[illegible]
54203	1	Acceso a Internet	[illegible]	[illegible]	[illegible]	[illegible]
54203	1	Acceso a Internet	[illegible]	[illegible]	[illegible]	[illegible]
54203	4	E1 DID	[illegible]	[illegible]	[illegible]	[illegible]
					Total	[illegible]

Sírvase comunicarse con migo con cualquier consulta. Me despido de usted agradeciendo de antemano su atención a esta nota.

Eric Lopez
Gestión de Sistemas de Información y Telecomunicaciones

Anexo 2

Cuestionario 1 – Situación Actual Universidad de El Salvador

Facultad Multidisciplinaria de Occidente.

Universidad de El Salvador

Facultad Multidisciplinaria de Occidente

Área de Redes y Servidores

Cuestionario 1

Proyecto: Diseño de un prototipo de implementación del protocolo IPv6 en la red de la Universidad de El Salvador Facultad Multidisciplinaria de Occidente.

Objetivo: Recolectar información sobre la situación actual de la infraestructura de red de la Universidad de El Salvador Facultad Multidisciplinaria de Occidente la cual será utilizada como fuente de información para el proyecto antes citado.

Instrucciones: A continuación se presenta varias preguntas relativas a la situación actual de la infraestructura de red de la institución, incluido en esto topologías, equipo, software, entre otras. Conteste escribiendo en los aspectos correspondientes sus respuestas.

1. ¿Cuenta con un esquema de red detallado de la UES-FMOcc? Si _X_ No _____ . Si su respuesta es sí, ¿Podría proporcionarlo al grupo de estudio? Si _X_ No ____ .

2. ¿Cuenta con un esquema de red que contenga los equipos con soporte a IPv6 e IPv4? Si _____ No _X_ . Si su respuesta es sí, ¿Podría proporcionarlo al grupo de estudio? Si _____ No _X_ .

3. ¿Cuenta con un listado de modelos de equipo utilizados en el DMZ Si _X_ No ____ . Si su respuesta es sí, ¿Podría proporcionarlo al grupo de estudio? Si _X_ No ____ .

4. ¿Cuenta con un listado de aplicaciones y sus versiones que están siendo utilizados en los equipos del DMZ? Si ____ No _X_ . Si su respuesta es sí, ¿Podría proporcionarlo al grupo de estudio? Si ____ No ____ .

5. ¿Cuenta con conexiones a través de IPv6 entre su equipo de Red en el DMZ? Si _X_ No ___.

6. Si cuenta con conexión con IPv6 en su DMZ, ¿Cuenta con un esquema de red de dichas conexiones? Si _____ No __X__ . Si su respuesta es sí, ¿Podría proporcionarlo al grupo de estudio? Si ____ No ____ .

7. ¿Se encuentran en uso dichas conexiones? Si _____ No __X__ . Si su respuesta es sí, ¿Cuál es el uso que se le da? Si ____ No ____ .

8. Del equipo con que cuenta en la infraestructura de red que tiene soporte IPv6 ¿Existe alguno que sea emulado? Si ____ No __X__ .

9. ¿Cuenta con más equipo con soporte IPv6 en la red de la institución que se encuentre fuera del DMZ? Si __X__ No ____ .

10. ¿Cuenta con un listado de este equipo? Si _____ No __X__ . Si su respuesta es sí, ¿Podría proporcionarlo al grupo de estudio? Si ____ No ____ .

11. ¿Cuenta con un listado de los servicios de red desplegados? Si __X__ No _____ . Si su respuesta es sí, ¿Podría proporcionarlo al grupo de estudio? Si ____ No __X__ .

12. ¿Cuenta con un listado de servicios desplegados únicamente en IPv6? Si ____ No __X__ . Si su respuesta es sí, ¿Podría proporcionarlo al grupo de estudio? Si ____ No ____ .

F. _____

Juan Carlos Peña

Administrador Área de Redes y Servidores

Santa Ana, 19 de Mayo de 2011

Anexo 3

Cuestionario 2 – Situación Actual Universidad de El Salvador

Facultad Multidisciplinaria de Occidente.

Universidad de El Salvador

Facultad Multidisciplinaria de Occidente

Área de Redes y Servidores

Cuestionario 2

Proyecto: Diseño de un prototipo de implementación del protocolo IPv6 en la red de la Universidad de El Salvador Facultad Multidisciplinaria de Occidente.

Objetivo: Recolectar información sobre la situación actual del recurso humano con el que cuenta la Universidad de El Salvador Facultad Multidisciplinaria de Occidente la cual será utilizada como fuente de información para el proyecto antes citado.

Instrucciones: A continuación se presenta varias preguntas relativas a la situación actual del recurso humano con el que cuenta la Universidad de El Salvador Facultad Multidisciplinaria de Occidente. Conteste escribiendo en los aspectos correspondientes sus respuestas.

1. ¿Posee los conocimientos necesarios para desarrollar una implementación de una red IPv6? Si X No ____ .
2. ¿Considera necesario la contratación de más personal para la implementación del protocolo IPv6? Si X No ____ .
3. ¿Considera necesaria la realización de una capacitación del personal del Área de Redes y Servidores para implementar IPv6? Si X No ____ .
4. ¿Considera necesaria la realización de una capacitación de los usuarios de la red de la institución para implementar IPv6? Si X No ____ .
5. ¿Podría ejecutar la implementación de IPv6 nativo? Si X No ___.
6. ¿Podría ejecutar la implementación de ipv6 mediante la técnica dual-stack? Si X No ____ .

Santa Ana, 10 de Junio de 2011

7. ¿Podría ejecutar la implementación de IPv6 mediante la técnica de túneles?
   Si X No ____ .

F. _____

Juan Carlos Peña

Administrador Área de Redes y Servidores

Santa Ana, 10 de Junio de 2011

Anexo 4

Contacto por Correo Electrónico con Rafael Ibarra,

Profesional de la organización RAICES. Situación Actual del

Mercado Nacional y Aspectos Generales sobre IPv6.

From: ribarra@di.uca.edu.sv
To: carlosfigueroacl@hotmail.com
Date: Tue, 5 Jul 2011 08:44:21 -0600
Subject: Re: informacion ipv6

Hola:

Ver respuestas abajo:
El 27 Jun 2011 a las 20:47, KiQ FiguEroa escribio:

Buen Día.

Mi nombre es Carlos Figueroa actualmente estoy trabajando en un estudio sobre los métodos de transición de Ipv4 a Ipv6 como parte de mi trabajo de graduación de la Universidad.

He revisado la documentación del sitio web http://www.raices.org.sv y me ha parecido de mucha importancia así como brindado mucha ayuda, sin embargo acudo a Uds. pues tengo un par de vacíos de información.

Por lo expuesto en su sitio web y otros sitios en los cuales hace referencia Uds, veo son la organización con mayor movimiento hacia ipv6 en El Salvador, por esto acudo a su ayuda inicialmente en los siguientes puntos:

-¿Los ISPs en El Salvador están brindando servicios ipv6 nativos?

Aun no. Que sepamos, no hay demasiada preocupación por este tema en los ISP. Tampoco es que sea urgente, por otro lado, pero se deben iniciar las planificaciones, pruebas y acciones en el tema.

-¿De brindar dichos servicios, Tienen alguna información de cuál es el rango de precios en los q oscila contratar dichos servicios?

No.

-¿Qué método o métodos son los más empleados como medio de transición en el país o Centro América?

Los más recomendados son 6to4 y Teredo. No sabemos cuáles se están usando.

-¿El costo de implementación de los métodos tanto de contratación de servicios como de soporte administrativos?

No está precisado aun.

-¿Qué aspectos pueden ser importantes para considerar por las instituciones y empresas para migrarse y usar un método en particular? por ejemplo (económico, técnico (el equipo, personal y servicios), seguridad).

Hay que considerar la infraestructura que tiene cada empresa, pues los enrutadores deben poder manejar IPv6, y verificar los demás elementos de red.

También se debe proveer capacitación al personal.

Sé que es una información bastante específica y de la cual tal vez no la posean toda. Pero agradeceré profundamente su colaboración con la información que les sea posible facilitarme, de no ser ninguna de esta cualquiera que Ud. consideren de utilidad.

Deseándoles éxitos en sus labores me despido de Ud.

Atte. Carlos Enrique Figueroa J.

Rafael (Lito) Ibarra
El Salvador (SV)
Tel +(503) 2210-6600, ext. 911
Fax +(503) 2210-6936

Anexo 5

Contacto por Correo Electrónico con Eric Báez, IPv6 Chile.

Situación Actual de IPv6 en Chile.

Date: Fri, 24 Jun 2011 14:43:22 -0400
Subject: Re: [Contacto] Información
From: ebaez@niclabs.cl
To: carlosfigueroacl@hotmail.com

Estimado Carlos

Agradecemos tu comunicación y los comentarios sobre el sitio www.ipv6.cl, que es una acción de difusión del proyecto IPv6 para Chile, respondemos sus consultas a continuación:

-¿Los ISPs en Chile están brindando servicios ipv6 nativos?

Actualmente hay un solo ISP que brinda servicios IPv6 nativos, se trata de GTD, empresa pionera en la región en la provisión de servicios IPv6 nativos, desde 2009 (http://www.grupogtd.com/ipv6/) Aparte de esta empresa, (que tiene importante presencia en servicios corporativos, más que residenciales) no existe en Chile otro ISP entregando servicios IPv6 nativos.

Las empresas de telecomunicaciones que participan del proyecto IPv6 para Chile, que en su conjunto representan el 80 por ciento de la conectividad de banda ancha fija y el 100 por ciento de la banda ancha móvil, no están entregando aún servicios con direccionamiento IPv6 a sus clientes, ni tampoco han precisado fechas en las que entregarán dichos servicios.

-¿De brindar dichos servicios, tienen alguna información de cuál es el rango de precios en los q oscila contratar dichos servicios?

Por la información que manejamos GTD no realiza un cobro adicional a sus clientes por direccionamiento IPv6 nativo.

-¿Que método o métodos son los más empleados como medio de transición en Chile?

Todavía no hay ninguno implementado, lo que sí sabemos es que en general las empresas están preparando sus backbone, que son MPLS y se ha utilizado mucho el método 6VPL

-¿El costo de implementación de los métodos tanto de contratación de servicios como de soporte administrativos?

No hay estudios sobre costos para el mercado local en servicios de transición, pero en el TCO (Total Cost Ownership) asociado a despliegues/transiciones a IPv6, buena parte implica la formación y nivelación del recurso humano, técnicos y profesionales de la organización. Malasia calculó que el 70 por ciento de su programa de transición a IPv6 radicaría en formación y entrenamiento (puesto que el hardware ya tiene ciclos de renovación asociados, independientes de una u otra tecnología), (referencias en el informe de octubre de 2010 de Tendencias en IPv6 http://www.ipv6.cl/tendencias/informe-IPv6-octubre-2010) es un tema discutido en listas de las comunidades de administradores y operadores de redes regionales como este ejemplo http://mail.lacnic.net/pipermail/lactf/2008-November/002079.html

saludos cordiales
Eric Báez
NIC Chile Research Labs

Anexo 6

Evaluación de la Metodología para la Selección de Técnica de Transición según la Situación Actual de la Universidad de El Salvador Facultad Multidisciplinaria de Occidente

Variables Técnicas

Código	Variables	Existe
1	Necesidades de acceso a Internet IPv6	✓
2	Necesidades de acceso a Internet IPv4	✓
3	Disponibilidad de servicios Ipv6	X
4	Disponibilidad de servicios IPv4	✓
5	Soporte Ipv6 en equipo de Red externa	✓
6	Soporte IPv6 en equipo de Red Interna	✓
7	Soporte Ipv6 en Host	✓
8	Soporte IPv6 en SO de host	✓
9	Soporte IPv6 de aplicaciones	✓

La evaluacion de la metodología en la table de variables técnicas obtenidas de la situacion actual de la institución y el medio en el que se encuentra, arrojó resultados positivos para 8 de ellas siendo unicamente mal evaluada la Disponibilidad de Servicios IPv6, ya que actualmente no hay algún ISP en la región que provea conexión nativa a través de dicho protocolo.

Evaluación Red interna

	1	2	6	7	8	9	Total
NAT/IPv6	X	✓	✓	✓	✓	✓	5
Pila Dual	✓	✓	✓	✓	✓	✓	6
Túnel 6 en 4	✓	✓	✓	✓	✓	✓	6
Túnel 4 en 6	X	✓	✓	✓	✓	✓	5
IPv6	✓	X	✓	✓	✓	✓	5

La tabla para la selección de técnica de transición para la red interna mostró como resultado dos opciones las cuales fueron Pila Dual y Túnel 6 en 4, escojiendo entre éstas la técnica Pila Dual por ser la de implementacion mas sencilla y la recomendación por los expertos de mantener la conectividad con ambos protocolos durante el período de transición.

Evaluación Red Externa

	1	2	3	4	5	Total
NAT/IPv6	X	✓	✓	✓	✓	4
Pila Dual	✓	✓	X	✓	✓	4
Túnel 6 en 4	✓	✓	✓	✓	✓	5
Túnel 4 en 6	X	✓	X	X	✓	2
IPv6	✓	X	X	X	✓	2

La tabla para la selección de técnia de transición para la red externa mostró como resultado óptimo la técnica Túnel 6 en 4.

Requerimientos Túneles

Código	Variables	Se Necesita
A	NAT Traversal	X
B	Autenticación	X
C	Reverse DNS	✓
Código	**Variable**	**Existe**
D	Multicast IPv4	X
E	Anycast IPv6	X

Dado que en la Evaluación para la Red Externa se seleccionó como óptima una técnica de tunelización, se procedió a evaluar que técnica de tunelización era la más recomendada usando la fase de determinación de técnica de tunelización de la Metodología para Selección de Técnica de Transición. La tabal de variables de túneles fue rellenada en base a la situcion actual del medio y de la institución, evaluando si estas existen o se necesitan.

Evaluación Túneles

	A	B	C	D	E	Total
6to4	✓	✓	✓	✓	X	Eliminado
6in4	✓	✓	✓	✓	✓	5
6over4	✓	✓	✓	X	✓	Eliminado
6rd	✓	✓	✓	✓	✓	5
AYIYA	✓	✓	✓	✓	✓	5
ISATAP	✓	✓	✓	✓	✓	5
L2TP	✓	✓	✓	✓	✓	5
TSP/UDPv6	✓	✓	✓	✓	✓	5
Teredo	✓	✓	X	✓	✓	4

Dentro de las tecnicas de túneles encontramos muchas opciones para poder implementar, siendo seleccionada la tecnica 6in4 por su mayor aplicación en la red, su amplia documentación y su compatibilidad con la mayoría de equipos.

Evaluación Variables Económicas

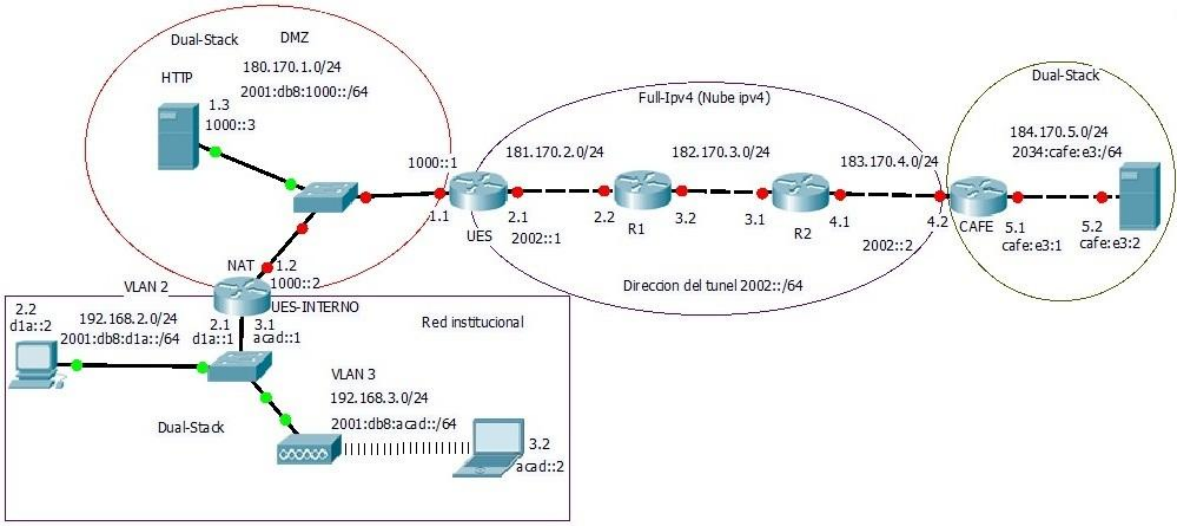
Código	Variable	Inversión
1	Disponibilidad de Servicios IPv4 en el Mercado	X
2	Disponibilidad de Servicios IPv6 en el Mercado	X
3	Soporte IPv6 del equipo de red externo para la implementación de la técnica de transición	X
4	Soporte IPv6 del equipo de red interno para la implementación de la técnica de transición	X
5	Soporte IPv6 del Sistema Operativo en hosts	X
6	Contratación de servicios especializados de redes para la implementación de la técnica de transición	X
7	Capacitación del Recurso Humano para la implementación de la técnica de transición y su administración	X
8	Contratación de consultoría externa para la implementación de la técnica de transición	X
9	Contratación de nuevo personal para el área de redes para apoyo para la implementación de la técnica de transición	X
10	Contratación de nuevo personal para el área de redes para apoyo para la administración de la técnica de transición	X

Dado que no se realizará ninguna inversión, las variables técnicas no sufrirán cambios, por lo cual, las técnicas recomendadas anteriormente serán las utilizadas para el prototipo.

Anexo 7

Diagrama Prototipo Pila Dual y Túnel 6in4

A continuación se presenta el diagrama del prototipo de implementación del protocolo IPv6 en la Universidad de El Salvador Facultad Multidisciplinaria de Occidente, el cual se basa en los resultados obtenidos en el Anexo 6 y consiste en una implementación de la técnica de transición Pila Dual en la red interna de la institución y un túnel 6in4 en la red externa con el fin de lograr alcanzar los servicios IPv6 externos.



Anexo 8

Evaluación de la Metodología para la Selección de Técnica de Transición para una migración total al protocolo IPv6 de la red de la Universidad de El Salvador Facultad Multidisciplinaria de Occidente

Evaluación Variables Económicas

Código	Variable	Inversión
1	Disponibilidad de Servicios IPv4 en el Mercado	X
2	Disponibilidad de Servicios IPv6 en el Mercado	✓
3	Soporte IPv6 del equipo de red externo para la implementación de la técnica de transición	X
4	Soporte IPv6 del equipo de red interno para la implementación de la técnica de transición	X
5	Soporte IPv6 del Sistema Operativo en hosts	X
6	Contratación de servicios especializados de redes para la implementación de la técnica de transición	X
7	Capacitación del Recurso Humano para la implementación de la técnica de transición y su administración	X
8	Contratación de consultoría externa para la implementación de la técnica de transición	X
9	Contratación de nuevo personal para el área de redes para apoyo para la implementación de la técnica de transición	X
10	Contratación de nuevo personal para el área de redes para apoyo para la administración de la técnica de transición	X

La evaluación económica se realizó en base a supuestos, evaluando factores que en un futuro cambiarán, como por ejemplo la ausencia de necesidad y disponibilidad de servicios en IPv4.

Generaría la necesidad de invertir en la contratación de sercicios en IPv6.

Variables Técnicas

Código	Variables	Existe
1	Necesidades de acceso a Internet IPv6	✓
2	Necesidades de acceso a Internet IPv4	X
3	Disponibilidad de servicios Ipv6	✓
4	Disponibilidad de servicios IPv4	X
5	Soporte Ipv6 en equipo de Red externa	✓
6	Soporte IPv6 en equipo de Red Interna	✓
7	Soporte Ipv6 en Host	✓
8	Soporte IPv6 en SO de host	✓
9	Soporte IPv6 de aplicaciones	✓

Al realizar la evaluación de las variables con los cambios antes explicados obtenemos resultados positivos en la mayoria de las variables con excepción en Disponibilidad y Necesidad de Ipv4.

Evaluación Red Interna

	1	2	6	7	8	9	Total
NAT/IPv6	X	X	✓	✓	✓	✓	4
Pila Dual	✓	✓	✓	✓	✓	✓	6
Túnel 6 en 4	✓	✓	✓	✓	✓	✓	6
Túnel 4 en 6	X	X	✓	✓	✓	✓	4
IPv6	✓	✓	✓	✓	✓	✓	6

La tabla para la selección de la técnica para la red interna nos arroja como resultado tres posibles soluciones entre ellas Pila Dual y Túnel 6 en 4, lo cual es factible pues aun cuando ya no son necesarios los servicios en IPv4 y no exista la Disponibilidad de estos, no hay nada que impida la implementación de IPv4 en el esquema de red interno en la institución. Pero se optó por una implementación de IPv6 con el fin de migrarse totalmente al nuevo protocolo.

Evaluación Red Externa

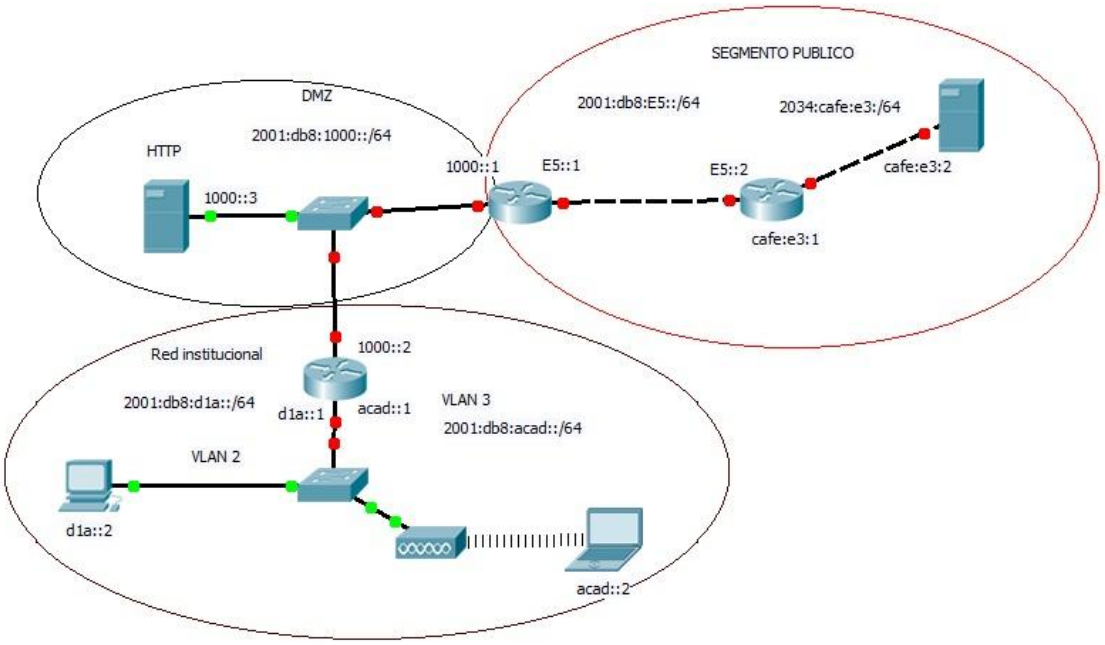
	1	2	3	4	5	Total
NAT/IPv6	X	X	X	X	✓	1
Pila Dual	✓	✓	✓	X	✓	4
Túnel 6 en 4	✓	✓	X	X	✓	3
Túnel 4 en 6	X	X	✓	✓	✓	3
IPv6	✓	✓	✓	✓	✓	5

La tabla para la selección de la técnica de transición en la red externa nos da un resultado único de implementacion el cual es IPv6 en su forma nativa.

Anexo 9

Diagrama Prototipo IPv6 Nativo

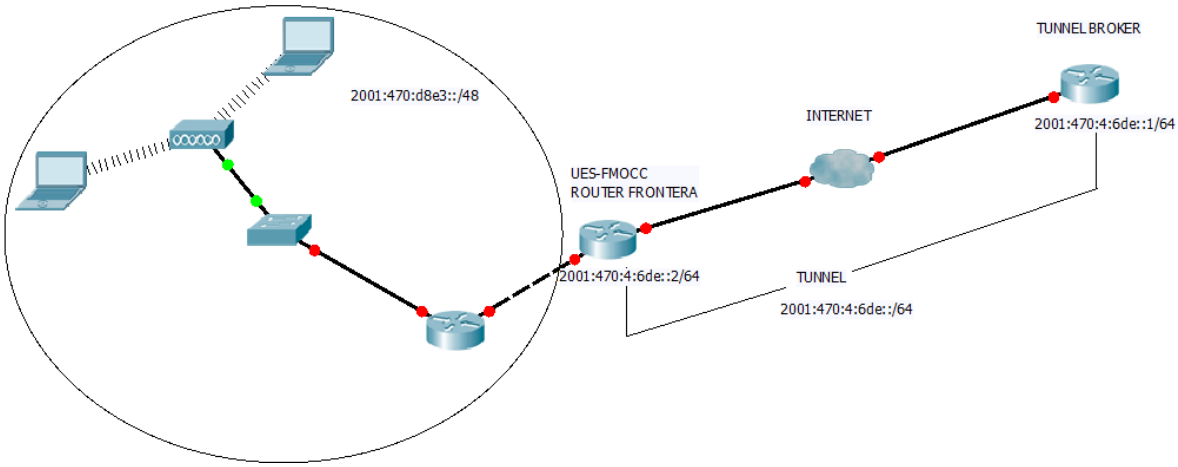
El siguiente diagrama muestra el prototipo diseñado en base al Anexo 8, el cual, determinó una migración completa al protocolo IPv6.



Anexo 9

Diagrama de Túnel 6in4 implementado en la red de la Universidad de El Salvador Facultad Multidisciplinaria de Occidente

A modo de prueba, se implementó en la institución un túnel 6 en 4 con el fin de lograr una conexión a internet a través del nuevo protocolo.



Anexo 10

Configuraciones de Equipo Utilizado en los Prototipos

Configuraciones de routers:

Router UES:

```
version 12.4
!
!
ipv6 unicast-routing
!
!
interface FastEthernet0/0
 ip address 180.170.1.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 ipv6 address 2001:DB8:1000::2/64
 ipv6 enable
 ipv6 ospf 6 area 1
!
interface FastEthernet0/1
 no ip address
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 2
 ip address 192.168.2.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 ipv6 address 2001:DB8:D1A::1/64
 ipv6 ospf 6 area 1
!
interface FastEthernet0/1.2
 encapsulation dot1Q 3
 ip address 192.168.3.1 255.255.255.0
 ip nat inside
```

```
 ip virtual-reassembly
 ipv6 address 2001:DB8:ACAD::1/64
!
router ospf 10
 log-adjacency-changes
 network 180.170.1.0 0.0.0.255 area 1
 network 192.168.2.0 0.0.0.255 area 1
 network 192.168.3.0 0.0.0.255 area 1
!
!
no ip http server
no ip http secure-server
!
ip nat inside source list 1 interface FastEthernet0/0
overload
!
access-list 1 permit 192.168.0.0 0.0.255.255
ipv6 router ospf 6
 router-id 10.0.0.2
 log-adjacency-changes
!
!
end
```

Router UES-INTERNO:

```
version 12.4
!
!
ipv6 unicast-routing
!
!
interface Tunnel0
 no ip address
 ipv6 address 2002::2/64
 tunnel source 183.170.4.2
 tunnel destination 181.170.2.1
 tunnel mode ipv6ip
!
interface FastEthernet1/0
 ip address 184.170.5.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2034:CAFE::1/64
 ipv6 enable
!
interface Ethernet2/0
 ip address 183.170.4.2 255.255.255.0
 duplex half
!
ip route 181.170.2.0 255.255.255.0 Ethernet2/0
ip route 182.170.3.0 255.255.255.0 Ethernet2/0
!
no ip http server
no ip http secure-server
!
!
ipv6 route ::/0 Tunnel0
!
!
end
```

Router CAFE:

```
version 12.4
!
!
ipv6 unicast-routing
!
!
interface Tunnel0
 no ip address
 ipv6 address 2002::2/64
 tunnel source 183.170.4.2
 tunnel destination 181.170.2.1
 tunnel mode ipv6ip
!
interface FastEthernet1/0
 ip address 184.170.5.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address 2034:CAFE::1/64
 ipv6 enable
!
interface Ethernet2/0
 ip address 183.170.4.2 255.255.255.0
 duplex half
!

ip route 181.170.2.0 255.255.255.0 Ethernet2/0
ip route 182.170.3.0 255.255.255.0 Ethernet2/0
!
no ip http server
no ip http secure-server
!
!
ipv6 route ::/0 Tunnel0
!
!
end
```

Router R1:

```
version 12.2
!
interface Ethernet0/0
 ip address 181.170.2.2 255.255.255.0
 half-duplex
!
interface Serial0/0
 ip address 182.170.3.2 255.255.255.0
 no fair-queue
!
ip classless
ip route 180.170.1.0 255.255.255.0 Ethernet0/0
ip route 182.170.3.0 255.255.255.0 Serial0/0
ip route 183.170.4.0 255.255.255.0 Serial0/0
ip route 184.170.5.0 255.255.255.0 Serial0/0
ip http server
ip pim bidir-enable
!
!
end
```

Router R2:

```
version 12.0
!
!
interface Ethernet0/0
 ip address 183.170.4.1 255.255.255.0
 no ip directed-broadcast
!
interface Serial0/1
 ip address 182.170.3.1 255.255.255.0
 no ip directed-broadcast
 clockrate 64000
!
ip classless
ip route 180.170.1.0 255.255.255.0 Serial0/1
ip route 181.170.2.0 255.255.255.0 Serial0/1
ip route 184.170.5.0 255.255.255.0 Ethernet0/0
no ip http server
!
!
end
```

Configuraciones de Switches:

Switch UES:

```
version 12.0
!
!
interface FastEthernet0/1
 switchport access vlan 2
!
.
.
!
interface FastEthernet0/4
 switchport access vlan 2
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/6
!
.
.
!
interface FastEthernet0/10
 switchport access vlan 3
!
interface FastEthernet0/11
!
interface GigabitEthernet0/2
!
interface VLAN1
 no ip directed-broadcast
 no ip route-cache
!
!
!
end
```

Servidor Web

Apache en sitio CAFE:

Archivo: ports.conf

```
#/etc/apache/ports.conf

NameVirtualHost 184.170.5.2:80
NameVirtualHost [2034:cafe:e3::2]:80
Listen *:80
```

Archivo: httpd.conf

```
#/etc/apache/httpd.conf
ServerName *:80
```

Archivo: cafeipv4

```
#/etc/apache/sites-avaliables/cafeipv4
<VirtualHost 184.170.5.2:80>
        ServerAdmin webmaster@cafe.com
        DocumentRoot "/home/os/httpd/IPv4/"
</VirtualHost>
```

Archivo: cafeipv6

```
#/etc/apache/sites-avaliables/cafeipv6
<VirtualHost [2034:cafe:e3::2]:80>
        ServerAdmin webmaster@cafe.com
        DocumentRoot "/home/os/httpd/IPv6/"
</VirtualHost>
```

Apache en sitio UESOCC:

Archivo: ports.conf

```
#/etc/apache/ports.conf

NameVirtualHost 180.170.1.3:80
NameVirtualHost [2001:db8:1000::3]:80
Listen *:80
```

Archivo: httpd.conf

```
#/etc/apache/httpd.conf
ServerName *:80
```

Archivo: uesoccipv4

```
#/etc/apache/sites-avaliables/uesoccipv4
<VirtualHost 180.170.1.3:80>
        ServerAdmin webmaster@uesocc.com
        DocumentRoot "/home/os/httpd/IPv4/"
</VirtualHost>
```

Archivo: cafeipv6

```
#/etc/apache/sites-avaliables/uesoccipv6
<VirtualHost [2001:db8:1000::3]:80>
        ServerAdmin webmaster@cafe.com
        DocumentRoot "/home/os/httpd/IPv6/"
</VirtualHost>
```

Configuraciones de servidores DNS:

Archivos de configuración del Dominio CAFE:

Archivo: 2034_cafe_e3.zone

```
; file: /etc/bind/2034_cafe_e3.zone

$TTL 86400
@ IN SOA ns1.cafe.com. dnsadmin.cafe.com. (
               2010072201 ; serial
               28800 ; refresh
               7200 ; retry
               604800 ; expire
               86400 ; ttk
               )
;
@                              IN   NS   ns1.cafe.com.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0      IN   PTR
     www.cafe.com.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0      IN   PTR
     ipv6.cafe.com.
```

Archivo: cafe.com.zone

```
;Archivo:/etc/bind/cafe.com.zone

$TTL    3600
@         IN      SOA     ns1.cafe.com. dnsadmin.cafe.com. (
                          1191280586; serial
                          3600; refresh
                          600; retry
                          86400; expire
                          3600 ); minimum
@         IN      NS       ns1.cafe.com.

ns1       IN      A        184.170.5.2
          IN      AAAA     2034:cafe:e3::2
```

```
www         IN      A       184.170.5.2
            IN      AAAA    2034:cafe:e3::2

ipv6        IN      AAAA    2034:cafe:e3::2

ipv4        IN      A       184.170.5.2
```

Archivo: db.184

```
;Archivo: /etc/bind/db.184

$TTL 604800
@     IN   SOA  ns1.cafe.com. admin.cafe.cafe. (
                      1         ; Serial
                 604800         ; Refresh
                  86400         ; Retry
                2419200         ; Expire
                 604800 ) ; Negative Cache TTL
;
@           IN   NS   ns1.cafe.com.
2.5.170     IN   PTR  ns1.cafe.com.
```

Archivo: named.conf.local

```
;Archivo: /etc/bind/named.conf.local


zone "cafe.com" {
     type master;
     file "/etc/bind/cafe.com.zone";
     allow-update   { none; };
     allow-transfer { 180.170.1.3/24; 2001:db8:1000::3/64; };
     also-notify    { 180.170.1.3; 2001:db8:1000::3; };
};

zone "184.in-addr.arpa" {
     type master;
     file "/etc/bind/db.184";
```

```
     allow-update   { none; };
     allow-transfer { 180.170.1.3/24; 2001:db8:1000::3/64; };
     also-notify    { 180.170.1.3; 2001:db8:1000::3; };
};

zone "3.e.0.0.e.f.a.c.4.3.0.2.ip6.arpa" {
     type master;
     file "/etc/bind/2034_cafe_e3.zone";
     allow-update   { none; };
     allow-transfer { 180.170.1.3/24; 2001:db8:1000::3/64; };
     also-notify    { 180.170.1.3; 2001:db8:1000::3; };
};


zone "uesocc.edu.sv" {
     type slave;
     file "/etc/bind/uesocc.edu.sv.zone";
     allow-transfer { 180.170.1.3; 2001:db8:1000::3; };
     also-notify    { 180.179.1.3; 2001:db8:1000::3; };
     masters        { 180.170.1.3; 2001:db8:1000::3; };
};

zone "180.170.1.in-addr.arpa" {
     type slave;
     file "/etc/bind/db.180.170.1";
     allow-transfer { 180.170.1.3; 2001:db8:1000::3; };
     also-notify    { 180.179.1.3; 2001:db8:1000::3; };
     masters        { 180.170.1.3; 2001:db8:1000::3; };
};

zone "0.0.0.1.8.b.d.0.1.0.0.2.ip6.arpa" {
     type slave;
     file "/etc/bind/2001_db8_1000.zone";
     allow-transfer { 180.170.1.3; 2001:db8:1000::3; };
     also-notify    { 180.179.1.3; 2001:db8:1000::3; };
     masters        { 180.170.1.3; 2001:db8:1000::3; };
};
```

Archivos de configuración del Dominio UESOCC:

Archivo: /etc/bind/2001_db8_1000.zone

```
$TTL 86400
@ IN SOA ns1.uesocc.edu.sv. dnsadmin.uesocc.edu.sv. (
               2010072201 ; serial
               28800 ; refresh
               7200 ; retry
               604800 ; expire
               86400 ; ttk
               )
;
@                              IN   NS   uesocc.edu.sv.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0      IN   PTR
     www.uesocc.edu.sv.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0      IN   PTR
     ipv6.uesocc.edu.sv.
```

Archivo: /etc/bind/uesocc.edu.sv.zone

```
$TTL 604800
@    IN   SOA  uesocc.edu.sv. root.uesocc.edu.sv. (
                     2         ; Serial
                  604800       ; Refresh
                   86400       ; Retry
                 2419200       ; Expire
                  604800 ) ; Negative Cache TTL
;
@    IN   NS   uesocc.edu.sv.
@    IN   A    180.170.1.3
@    IN   AAAA 2001:db8:1000::3


www  IN   A    180.170.1.3
     IN   AAAA 2001:db8:1000::3

ipv4 IN   A    180.170.1.3

ipv6 IN   AAAA 2001:db8:1000::3
```

Archivo: /etc/bind/db.180.170.1

```
$TTL 604800
@    IN   SOA  uesocc.edu.sv. root.uesocc.edu.sv. (
                     1         ; Serial
                604800         ; Refresh
                 86400         ; Retry
                2419200         ; Expire
                 604800 ) ; Negative Cache TTL
;
@    IN   NS   uesocc.edu.sv.
3    IN   PTR  uesocc.edu.sv.
```

Archivo: /etc/bind/named.conf.local

```
; Archivo: "/etc/bind/named.conf.local";

zone "uesocc.edu.sv" {
     type master;
     file "/etc/bind/uesocc.edu.sv.zone";
     allow-update { none;};
     allow-transfer { 184.170.5.2; 2034:cafe:e3::2; };
     also-notify    { 184.170.5.2; 2034:cafe:e3::2; };
};

zone "180.170.1.in-addr.arpa" {
     type master;
     file "/etc/bind/db.180.170.1";
     allow-update   { none; };
     allow-transfer { 184.170.5.2; 2034:cafe:e3::2; };
     also-notify    { 184.170.5.2; 2034:cafe:e3::2; };
};

zone "0.0.0.1.8.b.d.0.1.0.0.2.ip6.arpa" {
     type master;
     file "/etc/bind/2001_db8_1000.zone";
     allow-update { none; };
     allow-transfer { 184.170.5.2; 2034:cafe:e3::2; };
     also-notify    { 184.170.5.2; 2034:cafe:e3::2; };
};
```

```
zone "cafe.com" {
        type slave;
        file "/etc/bind/cafe.com.zone";
     allow-update   { none; };
     allow-transfer { 180.170.1.3/24; 2034:cafe:e3::2/64; };
     allow-notify   { 180.170.1.3/24; 2034:cafe:e3::2/64; };
     master         { 180.170.1.3/24; 2034:cafe:e3::2/64; };
};

zone "184.in-addr.arpa" {
        type slave;
     file "/etc/bind/db.184";
     allow-transfer { 180.170.1.3/24; 2034:cafe:e3::2/64; };
     allow-notify   { 180.170.1.3/24; 2034:cafe:e3::2/64; };
     master         { 180.170.1.3/24; 2034:cafe:e3::2/64; };
};

zone "3.e.0.0.e.f.a.c.4.3.0.2.ip6.arpa" {
        type slave;
     file "/etc/bind/2034_cafe_e3.zone";
     allow-transfer { 180.170.1.3/24; 2034:cafe:e3::2/64; };
     allow-notify   { 180.170.1.3/24; 2034:cafe:e3::2/64; };
     master         { 180.170.1.3/24; 2034:cafe:e3::2/64; };
};
```

Interfaces:

Archivo de configuración de Interfaces para los servidores sitio cafe:

```
# file: /etc/network/interfaces

# The loopback network interface
auto lo
iface lo inet loopback

#------------------------------------------------------------
auto tap0
iface eth0 inet static
address 184.170.5.2
netmask 255.255.255.0
network 184.170.5.0
broadcast 184.170.5.255
gateway 184.170.5.1

#------------------------------------------------------------
#IPV6 static configuration
iface eth0 inet6 static
address 2034:cafe:00e3:0000:0000:0000:0000:0002
netmask 64
gateway 2034:cafe:00e3:0000:0000:0000:0000:0001
#END IPV6 configuration
```

Configuración para routers Prototipo IPv6 Nativo:

Archivo de configuración router CAFE:

```
version 12.4
!
ipv6 unicast-routing
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface FastEthernet1/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:E5::1/64
 ipv6 enable
!
interface FastEthernet1/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2034:CAFE:E3::1/64
 ipv6 enable
!
router bgp 1
 synchronization
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 neighbor 2001:DB8:E5::2 remote-as 2
 auto-summary
 !
 address-family ipv6
 neighbor 2001:DB8:E5::2 activate
 network 2034:CAFE:E3::/64
 exit-address-family
!
no ip http server
no ip http secure-server
!
end
```

Archivo de configuración router UES:

```
version 12.4
!
ip cef
!
!
ipv6 unicast-routing
ipv6 cef
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:1000::1/64
 ipv6 enable
 ipv6 ospf 6 area 1
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:E5::2/64
 ipv6 enable
!
router bgp 2
 bgp router-id 1.1.1.2
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 2001:DB8:E5::1 remote-as 1
 default-metric 2
 !
 address-family ipv6
 neighbor 2001:DB8:E5::1 activate
 redistribute connected
 redistribute ospf 6
 no synchronization
 exit-address-family
!
!
ipv6 router ospf 6
 router-id 10.10.10.11
 log-adjacency-changes
```

```
 default-information originate
 redistribute connected
 redistribute bgp 2 metric 20 include-connected
!
!
end
```

Archivo de configuración router UES-INTERNO:

```
version 12.4
!
!
ipv6 unicast-routing
!
!
interface FastEthernet0/0
 ip address 180.170.1.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 ipv6 address 2001:DB8:1000::2/64
 ipv6 enable
 ipv6 ospf 6 area 1
!
interface FastEthernet0/1
 no ip address
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1.1
 encapsulation dot1Q 2
 ip address 192.168.2.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 ipv6 address 2001:DB8:D1A::1/64
 ipv6 ospf 6 area 1
!
interface FastEthernet0/1.2
 encapsulation dot1Q 3
```

```
 ip address 192.168.3.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 ipv6 address 2001:DB8:ACAD::1/64
 ipv6 ospf 6 area 1
!
interface FastEthernet1/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet1/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router ospf 10
 log-adjacency-changes
 network 180.170.1.0 0.0.0.255 area 1
 network 192.168.2.0 0.0.0.255 area 1
 network 192.168.3.0 0.0.0.255 area 1
!
!
no ip http server
no ip http secure-server
!
ip nat inside source list 1 interface FastEthernet0/0
overload
!
access-list 1 permit 192.168.0.0 0.0.255.255
ipv6 router ospf 6
 router-id 10.0.0.2
 log-adjacency-changes
!
!
end
```

Anexo 11

Reporte de Valores Invertidos en la Ejecución del Proyecto

A continuación se presenta en detalle el Reporte de Valores Invertidos en la Ejecución del Proyecto, el cual contiene el costo del equipo utilizado, asi como

Costo de Equipo para la Ejecución del Proyecto:

Concepto	Costo	Cantidad	Total
Computadora	$ 600.00	6	$ 3,600.00
Switch Catalyst 3500	$ 800.00	2	$ 1,600.00
Router 2600	$ 900.00	2	$ 1,800.00
AP dlink	$ 50.00	1	$ 50.00
IOS cisco 7200	$ 650	1	$ 650.00
Cableado	$ 2.50	10	$ 25.00
UPS	$ 40.00	1	$ 40.00
TOTAL			**$ 7,765.00**

Detalle Total de Valores:

Concepto		Valor
Papelería y Útiles		$ 200.00
Viáticos		$ 518.00
Gastos para Presentaciones		$ 200.00
Gastos en servicios		$ 160.38
Internet (540h*$0.06nav/h*3conexiones)	$ 97.20	
Electricidad (650w/h*540h*$0.18kw/h)	$ 63.18	
Costo de Equipo		$ 7,765.00
Costo por Representación		$ 9000.00
TOTAL		**$ 17,843.38**