UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

Facultad No.9

TÍTULO: Propuesta de estrategia para la migración de la red de la UCI hacia IPv6.

TRABAJO DE DIPLOMA PARA OPTAR POR

EL TÍTULO DE INGENIERO EN CIENCIAS INFORMÁTICAS

AUTOR: Frank Torres Valdés

TUTORES: Ing. Orestes Rodríguez Morales

Lic. Miriam Valdés Abreu

CONSULTOR: Téc. Félix Alberto Suárez Planché

Ciudad de La Habana, 4 de julio de 2008

"Año 50 de la Revolución"

DEDICATORIA

A mi familia

AGRADECIMIENTOS

A todas las personas que me han ayudado en el desarrollo de esta tesis, en especial a Armando Barrera García, Guillermo William y Hedel Nuñez Oliva por el apoyo incondicional.

RESUMEN

Cuba, al igual que muchos países, prepara condiciones para la inevitable transición hacia redes IPv6. En este sentido se dan los primeros pasos en el ordenamiento de los recursos de Internet y se trabaja en la elaboración de los documentos y políticas de transición hacia el nuevo protocolo, a la par que se continúan las labores de divulgación y aprendizaje de los aspectos relacionados con esta tecnología.

La Universidad de las Ciencias Informáticas (UCI) no está ajena a este proceso y ya realiza acciones encaminadas a introducir progresivamente este protocolo en su intranet, sin afectar los servicios que hoy brinda y garantizando la seguridad en el proceso de la migración. El trabajo que se presenta es parte de este esfuerzo y pretende brindar una guía con los pasos a seguir para efectuar la transición en la intranet de la UCI.

Los resultados de este trabajo podrán servir de referencia a otras universidades e instituciones que se propongan la integración de IPv6 en sus redes, contribuyendo de esta manera a la introducción de esta tecnología en el país.

ABSTRACT

Cuba, like other many countries, is preparing conditions for the inevitable transition towards IPv6 networks. It is designated as the successor of IPv4, the current version of the Internet Protocol, for general use on the Internet.

Nowadays, our country is organizing its Internet resources. The involvement of authorities from different areas such as science, technology, educations, and so on, made it possible to establish strategies, procedures and regulations in order to assure the deployment and later adoption of the new protocol. Meantime, the promotion and training programs continues.

The University of Computer Sciences (UCI) is also involving in the IPv6 transition. The University has taken some steps regarding to the research about this issue.

Nowadays, in the understanding that integrating all efforts will result in the early implementation of the new protocol, is time to begin some actions in order to achieve the migration of its Intranet. However, there are some rigorous requirements regarding to the necessary uninterrupted service of the Intranet and its adequate security.

Information, ideas and data developed in this project are part of the mentioned efforts. The basic proposal of this project is to offer a technical guide, step by step, for the Intranet transition.

At the same time, all the experiences of this project and its implementation in that institution could be expanded to other universities, as modest contribution to the Cuban technological development.

INDICE

TABLAS Y FIGURAS

Pág.

TABLAS

FIGURAS

"El mundo camina hacia la era electrónica... Todo indica que esta ciencia se convertirá en algo así como una medida de desarrollo; quien la domine será un país de vanguardia."

Comandante Ernesto Che Guevara, 1962.

INTRODUCCIÓN

IP son las siglas de Protocolo de Internet (*Internet Protocol, IP*). Fue diseñado en los años 70 con el fin de interconectar redes entre sí.

En aquel momento, los equipos informáticos estaban conectados a alguna de las múltiples redes independientes existentes, las cuales estaban separadas y formaban islas incomunicadas entre sí. La aparición de este protocolo permitió conectar todas estas redes aisladas en una gran red unificada, la que conocemos como Internet.

Hoy se emplea mayoritariamente la versión 4 del Protocolo de Internet (IPv4). Sin embargo, el gran número de usuarios, dispositivos, aplicaciones, servicios, y en general el éxito de Internet en sí misma, está llevando esta versión a sus límites.

Ante tal disyuntiva, en los años 90 comenzó la búsqueda de un sustituto que permitiera la continua evolución de Internet, surgiendo así IPv6[1], la versión 6 del Protocolo de Internet. Este fue diseñado por la Fuerza de Tareas de Ingeniería de Internet (*Internet Engineering Task Force, IETF*) para reemplazar en forma gradual a la versión actual, el IPv4.

El IPv4 dispone de un espacio de direcciones de 32 bits, mientras que el IPv6 ofrece un espacio de 128 bits; lo que significa un aumento sustancial en las cantidades de direcciones.

El reducido espacio de direcciones del IPv4, junto la falta de coordinación que para su asignación existió durante la década de los 80, sin ningún tipo de optimización y que dejó espacios de direcciones discontinuos, 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. Estas inclusiones, no contempladas en el análisis inicial, generan complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de las prestaciones incorporadas. Entre las nuevas funcionalidades, vale la pena señalar aquellas encaminadas a permitir la calidad de servicio, la seguridad y la movilidad.

[1] También conocida como Próxima Generación del Protocolo de Internet, IPng.

Cuba, al igual que muchos países, prepara condiciones para la inevitable transición hacia redes IPv6. En este sentido se dan los primeros pasos en el ordenamiento de los recursos de Internet y se trabaja en la elaboración de los documentos y políticas de transición hacia el nuevo protocolo, a la par que se continúan las labores de divulgación y aprendizaje de los aspectos relacionados con esta tecnología.

La Universidad de Ciencia Informáticas (UCI), en su compromiso de aportar al desarrollo tecnológico del país, no está ajena a este proceso; y ya realiza acciones encaminadas a introducir progresivamente este protocolo en su intranet, con la premisa de no afectar los servicios que hoy brinda y garantizando, a su vez, la seguridad necesaria en el proceso de la migración.

El presente trabajo pretende constituir una modesta contribución a este loable esfuerzo. Los estudios, consultas y análisis compilados aportarán los elementos que permitan el establecimiento de una estrategia para la transición ordenada de la Intranet de la Universidad.

Sin embargo, el camino al IPv6 no es una simple transición o migración, se trata de un proceso de evolución e integración ordenada, que requiere de la preparación y del mejoramiento de la red, lo cual implica la capacitación del personal técnico, la adquisición de equipamiento, la configuración de sistemas operativos y la instalación de las aplicaciones necesarias, entre otros; todo en función de los servicios que se quieran brindar; con la premisa de que cumplan las especificaciones IPv6, pero sin soslayar las de IPv4.

Pudiera pensarse que lo más cómodo para efectuar una migración sería interrumpir, por unos días, todos los servicios que ofrece la red y, en este lapso, realizar los cambios necesarios. Obviamente resultaría más cómodo; pero muy poco práctico en casos como la UCI, donde los niveles de informatización son altos y la vida misma de la Universidad se soporta sobre esta red.

Entonces, el **problema** planteado es, bajo qué condiciones sería viable la implementación de IPv6 en la red de la Universidad, sin afectar su vitalidad.

A partir de lo anterior, se ha identificado como **objeto de estudio** el proceso de migración hacia IPv6 en la UCI y el **campo de acción** está definido por los requisitos necesarios para la implementación de este protocolo en la Universidad.

El **objetivo general** de la investigación es establecer la estrategia para migrar la red del centro hacia IPv6, con la condición de no afectar los servicios que se brindan.

En consecuencia con el problema planteado, el objeto de estudio y el objetivo general de la investigación, se han definido un conjunto de **tareas de investigación**. Estas son:

- Establecer las características y posibilidades del IPv6.
- Analizar el desarrollo actual y experiencias de la implementación del IPv6 en el mundo.
- Analizar las características particulares de la red de la UCI.
- Determinar el mecanismo de transición o combinación de ellos que resulta más adecuado, de acuerdo a las condiciones y requerimientos de la UCI, para este proceso.
- Proponer una estrategia para la transición hacia una red IPv6 en el centro.
- Evaluar los riesgos de seguridad que implica la introducción del nuevo protocolo en la red de la UCI.

Para la ejecución de estas tareas, se emplearán los siguientes **métodos**:

Método Teórico: Histórico-Lógico. Se efectuará una amplia revisión bibliográfica orientada a la búsqueda de información técnica referente al protocolo IPv6, su grado de madurez actual, las diferentes técnicas de migración, experiencias, y en general, referente a todas las tendencias, normas y principios que rigen esta tecnología.

Método Teórico: Inductivo – Deductivo. De importante peso en esta investigación, pues se realizará un análisis acerca la implementación del IPv6, de lo particular a lo general. Desde los servidores hasta las estaciones de trabajo, lo que podría significar la implementación de esta tecnología, en toda la extensión de la red.

Método Empírico: Entrevista. Es importante la consulta a los administradores de red de la Universidad y conocer los pormenores, requerimientos, peculiaridades, así como criterios acerca de la estrategia propuesta. Las entrevistas estarán dirigidas fundamentalmente a los administradores del nodo central de la red de la UCI, con el objetivo de conocer en detalles el equipamiento con que se cuenta la red, su topología, la propuesta de adquisición de equipamiento, entre otros elementos; que todo lo cual permitirá definir una propuesta de implementación del protocolo IPv6 en la Universidad.

El trabajo ha sido estructurado en tres capítulos. En el primero se presentan algunas experiencias nacionales e internacionales acerca de la implementación del IPv6 y la situación con respecto al tema en el país. En el segundo capítulo se detallan las especificaciones técnicas de la versión 6 del

Protocolo de Internet. En el tercero se describe la red de la UCI, se analizan variantes factibles para realizar el proceso de tránsito, y, finalmente, se presenta una propuesta de estrategia para la migración, como resultado del estudio realizado.

CAPÍTULO 1

Introducción.

Internet, tal y como hoy existe, basa su funcionamiento en un protocolo conocido como el Protocolo de Internet (IP), el cual se encarga de transportar los datos, contenidos en paquetes o datagramas, a través de la Red. IPv4 es la versión 4 de IP [1][2], que ha sido capaz de superar todas las pruebas impuestas desde su inicio en 1981, y que se aproxima ahora a su lógico fin. Las causas de lo anterior pueden resumirse en:

- El reciente crecimiento exponencial de Internet y el inminente agotamiento del espacio de direcciones IPv4, provocado por la proliferación de dispositivos conectados.
- La aparición de numerosos dispositivos móviles.
- El crecimiento de la denominada Red de Redes y la incapacidad de los enrutadores troncales de Internet para mantener grandes tablas de enrutamiento.
- La necesidad de una configuración más sencilla que permita generalizar el uso de estas nuevas tecnologías.
- El requisito de seguridad en el nivel de IP.
- La necesidad de facilitar la entrega de datos en tiempo real y la capacidad de garantizar determinados parámetros en los servicios, conocido como Calidad de Servicio (*Quality of Service, QoS*).

Por estas razones, a principios de la década del 90, el EITF comenzó a desarrollar una nueva versión del protocolo, llamada a resolver estas limitaciones del IPv4 e incorporar otras mejoras en cuanto a seguridad y eficiencia.

1.1 Conceptos asociados al dominio del problema.

Para profundizar en las características y posibilidades del IPv6, resulta importante enunciar primeramente qué es un Protocolo de Internet, así como conocer la definición conceptual de la versión 6 de este protocolo.

---

[2] [1] Petición de Comentario (*Request For Comments, RFC*). Son documentos cuyos contenidos constituyen una propuesta oficial para un nuevo protocolo de Internet. Ver referencia bibliográfica.

Protocolo de Internet: (*Internet Protocol, IP*). Protocolo para la comunicación en una red a través de paquetes conmutados; es principalmente usado en Internet. Los datos se envían en bloques conocidos como paquetes (datagramas) de un determinado tamaño máximo para cada red (*Maximum Transfer Unit, MTU*). El envío es no fiable (conocido también como mejor esfuerzo); se llama así porque el protocolo IP no garantiza si un paquete alcanza o no su destino correctamente. Un paquete puede llegar dañado, repetido, en otro orden o no llegar. Para la fiabilidad se utiliza el Protocolo de Control de Transmisión (*Transmission Control Protocol, TCP*) de la capa de transporte. [2]

Los paquetes poseen una cabecera con información sobre el dispositivo de origen y el de destino (sus direcciones IP). Con esta información los enrutadores determinan la vía para enviar la información. Cada paquete de un mismo archivo puede enviarse por diferentes rutas, dependiendo de la congestión del momento.

IPv6: Es la versión 6 del Protocolo de Internet, un estándar en desarrollo, encargado de dirigir y encaminar los paquetes a través de una red. El nuevo estándar mejorará el servicio globalmente, así, por ejemplo, permitirá proporcionar a futuras celdas telefónicas y dispositivos móviles, sus direcciones propias y permanentes. [2]

IPv6 está destinado a sustituir al estándar IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados.

A continuación se detallan las limitaciones del IPv4. [3]

1.2 Limitaciones del IPv4.

El Protocolo de Internet (IP) fue diseñado con el fin de interconectar redes entre sí. Los creadores de Internet no predijeron, en ningún momento, el gran éxito que este protocolo iba a tener en tan poco tiempo, ni su aplicación en tantos campos. No es que estuvieran equivocados, sino que las Tecnologías de la Información y las Comunicaciones (TIC) han evolucionado más rápido de lo previsto. Es por esto que la versión actual de IP (IPv4) está llegando a sus límites, con restricciones que comprometen el futuro crecimiento de la Red, y por tanto, la creación e implementación de nuevas aplicaciones, con más posibilidades que las actuales.

1.2.1 Agotamiento del espacio de direcciones IPv4.

El IPv4 tiene un espacio de 4 bytes para direccionar (32 bits), esto significa que existen 4 294 967 296 direcciones. Este número, que puede parecer muy grande, resulta insuficiente para dar una dirección a cada persona del planeta, y mucho menos a cada teléfono móvil, computadora personal (PC), servidor y demás dispositivos que usan el Protocolo de Internet. Es importante puntualizar, además, que no todas estas direcciones son empleadas en Internet para direccionar el equipamiento empleado como anfitrión (*hosts*), ya que algunas de ellas son reservadas, como el interfaz de red virtual para simular un lazo (*loopback*) y otras reservadas para uso específico, como las direcciones privadas. Un ejemplo de ello es la 10.0.0.0/8.

Todo esto, unido al auge que ha tenido Internet en los últimos años ha llevado a que las direcciones de Internet sin asignar se estén terminando. Algunos estudios estiman que su agotamiento total ocurra antes del año 2015.

1.2.2 Problemas introducidos por el uso del Traductor de Direcciones de Red.

Una de las alternativas, a la falta de direcciones, fue el empleo de la Traducción de Direcciones de Red (*Network Address Translator, NAT*) para asignar múltiples direcciones privadas a una sola dirección IP pública. Esta solución, por su parte, ocasionó otros inconvenientes presentes en la actualidad:

- No admite la seguridad basada en estándares en la capa de red.
- Puede crear problemas cuando se conectan dos organizaciones que utilizan el mismo espacio de direcciones privadas.
- No admite comunicación de extremo a extremo, por lo que va en contra de servicios como la telefonía IP.
- Crea un punto único de fallo en la red.
- Compromete las prestaciones y la robustez de la red.

1.2.3 Grandes tablas de enrutamiento en los enrutadores troncales.

Debido a la forma en que se asignan los identificadores de red IPv4, existen normalmente más de 70 000 rutas en la tabla de enrutamiento de los dispositivos troncales de Internet. La infraestructura actual del enrutamiento de IPv4 en Internet es una combinación de enrutamiento jerárquico y plano. Esto provoca retrasos en el procesamiento y reenvío de los paquetes.

1.2.4 Necesidad de una configuración más sencilla.

La mayor parte de las implementaciones actuales del IPv4 deben configurarse manualmente o mediante un protocolo de configuración de direcciones con estado, como el Protocolo de Configuración Dinámico de Terminales (*Dynamic Host Configuration Protocol, DHCP*). Ante un número mayor de equipos y dispositivos que utilizan IP, existe la necesidad de emplear una configuración de direcciones más sencilla y automática, así como otros parámetros de configuración no basados en la administración de una infraestructura DHCP. Sería casi imposible el despliegue de nuevas tecnologías, como la telefonía IP, si para esto se requiere que cada usuario sea capaz de configurar un servidor.

1.2.5 Requisito de seguridad en el nivel de IP.

La comunicación privada a través de un medio público, como Internet, requiere servicios de cifrado que protejan los datos que se envían, ante posibles observaciones o modificaciones durante el tránsito. Si bien hay un estándar para ofrecer seguridad a los paquetes de IPv4, conocida como Seguridad del Protocolo Internet (*Internet Protocol Security, IPSec*), este es opcional.

1.2.6 Falta de mecanismos de Calidad de Servicio.

Otro de los dilemas que enfrenta el IPv4 es su limitante con los mecanismos de Calidad de Servicio, que no es más que la capacidad que tiene una red para dar respuesta al tipo de servicio que necesita cada aplicación. Esta peculiaridad no estuvo presente en el diseño del protocolo, en tanto en aquel momento el asunto no resultaba prioritario.

Ciertamente existen algunos estándares de Calidad de Servicio para IPv4; pero estos resultan algo limitados.

1.2.7 Falta de mecanismos para lograr movilidad.

Hoy en día la tecnología se desarrolla vertiginosamente. Uno de los aportes de esta revolución tecnológica son los dispositivos móviles, tales como los celulares, los Asistentes Digitales Personales (*Personal Digital Assistant, PDA*), las computadoras portátiles, entre otros. Estos equipos necesitan poder conectarse, desde cualquier lugar, a la red. IPv4 no ofrece una solución viable para esto, si se tiene en cuenta que la seguridad resulta un elemento neurálgico en estos casos.

Hasta aquí se han detallado las principales limitaciones que presenta la versión 4 del Protocolo de Internet, lo que evidencia la necesidad de trazar una estrategia en el país para la transición paulatina hacia el nuevo protocolo.

1.3 IPv6 en el mundo. Situación actual y perspectivas.

En un comunicado de prensa, de junio de 2007, del Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC), su Director Ejecutivo anunciaba el inminente agotamiento de las direcciones IPv4, y estimaba que en 3 años se acabarán las direcciones disponibles para conectarse a Internet bajo el protocolo actual.

Aseguró que: "Es un hecho que las direcciones IP basadas en la actual versión del protocolo (IPv4) se terminarán en corto plazo; se estima que en la actualidad queda disponible menos del 18% de total de las direcciones IP versión cuatro" [4].

El tema constituye en la actualidad una preocupación, pues el futuro desarrollo de Internet podría estar comprometido de no comenzar a utilizarse la versión 6 del Protocolo de Internet.

Muchas instituciones, y en especial las universidades, realizan investigaciones acerca del tema, y otras ya realizan pruebas en este sentido.

Hoy funciona la Red 6Bone, que es una red mundial experimental utilizada para probar los conceptos y la puesta en operación de IPv6, en la cual participan más de 55 países.

1.3.1 Casos de estudio.

Entre los casos de estudio se incluyó la Universidad Nacional Autónoma de México (UNAM), que estableció desde 1998 un amplio programa de pruebas y trabajos con temas de IPv6. Por ejemplo, realizó acciones relacionadas con implementaciones, pilas IPv4/IPv6, túneles, software de conexión, aplicaciones multimedia, servidores para Web y Sistema de Nombres de Dominio (*Domain Name System, DNS*), autoconfiguración, calidad de servicio, conexión con redes internacionales de IPv6, entre otros.

Dentro de las primeras pruebas realizadas, destaca la de conexión a la Red 6Bone.

Actualmente un conjunto de instituciones mexicanas realizan acciones para lograr una conexión IPv6 hacia la UNAM. Adicionalmente, otras universidades de Chile, Argentina, Colombia y Perú se han sumado a este proyecto. [5] – [6]

Otra de las experiencias analizadas fue la Red Universitaria Nacional de Chile (REUNA). A esta red se conectan hoy 14 universidades y 2 centros de investigaciones. A continuación se muestra, en la figura 1.1, un esquema de la REUNA:

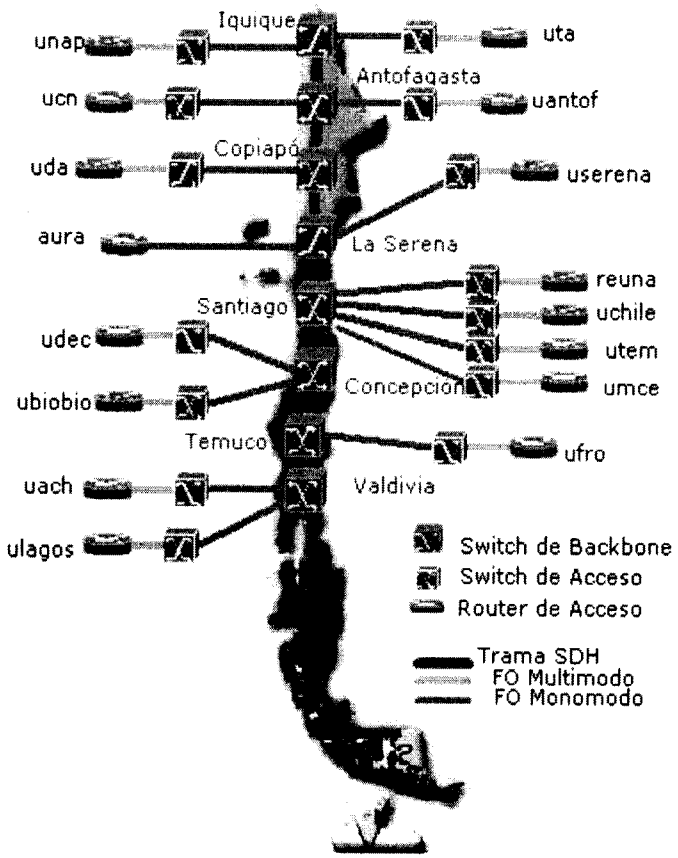

Fig. 1.1. Esquema de la Red Universitaria Nacional de Chile. [7]

Desde hace algo más de 4 años, existe un proyecto para la implementación de IPv6 en la red. En su etapa inicial se realizó la migración a IPv6 a nivel troncal y posteriormente a nivel de redes. La principal limitante que ha tenido la REUNA para avanzar en este proceso ha sido, que el equipamiento que posee, no soporta este protocolo.

1.3.2. Experiencias en la implementación de IPv6 en Cuba.

En el país existe una voluntad política para avanzar y lograr niveles superiores de eficiencia y eficacia, en todas las esferas de la vida económica y social, que redundará en el mejoramiento de la calidad de vida del pueblo cubano. Es indiscutible que el uso de las Tecnologías de la Información y las Comunicaciones juega un papel importante en este empeño. En tal sentido el titular del Ministerio de la Informática y las Comunicaciones (MIC), Comandante de la Revolución Ramiro Valdés, ha hecho énfasis en la necesidad de trabajar con inteligencia y dedicación en un tema tan decisivo como es el futuro tecnológico de la nación. [8]

En este contexto, el IPv6 es un tema importante a considerar. Sin embargo, en Cuba la introducción del IPv6 apenas comienza. A tales fines, labora un Grupo de Trabajo Multidisciplinario encargado de proponer una estrategia nacional que permita, paulatina y ordenadamente, avanzar en esta dirección. Entre sus objetivos están: [9]

- Estudiar las recomendaciones emitidas por IETF y organizaciones de la Región.
- Creación de grupos de trabajo para el estudio de las distintas áreas de implementación.
- Elaborar las recomendaciones para la administración de redes, la comunidad académica, empresas Importadoras de tecnologías, órgano regulador y otras entidades.
- Elaboración de estrategias de divulgación nacional e Internacional del proyecto cubano de IPv6.

Existen algunas experiencias en el país en la implementación de IPv6. Uno de los pioneros en el tema ha sido en Ministerio del Turismo (MINTUR). Esta institución se dio a la tarea de reestructurar su red de datos y, como parte del proceso, incluyó la introducción del nuevo protocolo. [3]

Aunque ciertamente el MINTUR no cuenta aún con una implementación completa, ha logrado un acercamiento, garantizando el primer paso de una evolución definitivamente imprescindible para el futuro de su red.

Se conoce, además, que en el nodo del Ministerio de Educación Superior (MES), también se realizan acciones encaminadas a la implementación de IPv6, aunque no fue posible, por problemas de tiempo, contar con la información relacionada con el trabajo que en este sentido se realiza en dicho Organismo.

CAPÍTULO 2

Introducción

IPv6 fue diseñado teniendo en cuenta las experiencias del trabajo con IPv4. Gracias a esto, se pudieron hacer mejoras y adicionar nuevas funcionalidades, que permiten la potenciación del protocolo y de Internet. Algunas de ellas son:

- Nuevo formato de encabezado.
- Nueva arquitectura de direccionamiento.
- Autoconfiguración.
- Seguridad integrada.
- Mayor soporte para mecanismos de Calidad de Servicio.
- Movilidad.
- Mejoras al Protocolo de Mensajes de Control de Internet (*Internet Control Message Protocol, ICMP*).
- Mejoras en la fragmentación.

En el tópico siguiente se detallan las especificaciones técnicas de este protocolo.

2.1. Estructura del paquete IPv6

Una de las novedades de este protocolo es un nuevo formato del encabezado del paquete, el cual se muestra en la figura 2.1.

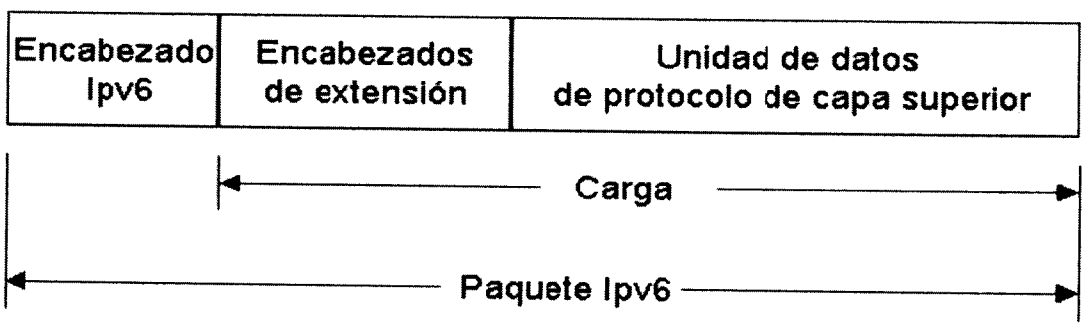

Fig. 2.1. Estructura del paquete IPv6.

A continuación se realiza una descripción detallada del encabezado del paquete IPv6.

2.1.1. Encabezado del paquete IPv6.

El encabezado IPv6 es obligatorio y tiene un tamaño de 40 bytes. Este presenta una nueva estructura para disminuir la carga de trabajo en su procesamiento, la cual se muestra en la Figura 2.2.

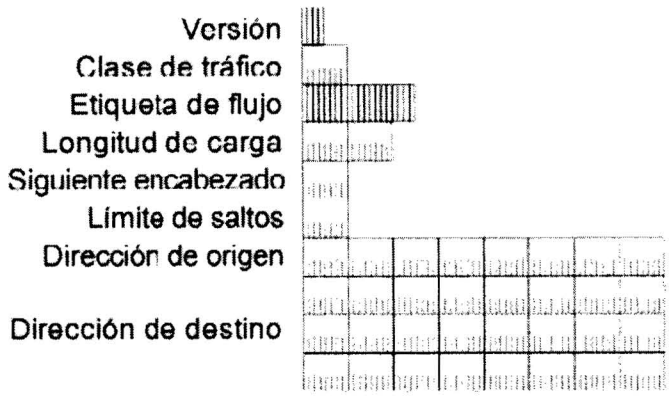

Fig. 2.2. Encabezado del paquete IPv6.

Descripción de los campos del encabezado:

Versión: Tiene 4 bits con el valor 6 (versión del protocolo).

Clase de Tráfico: Tiene 8 bits y es para marcar los paquetes, a fin de que pueda ser usado por el modelo de servicio diferenciado en la implementación de Calidad de Servicio (QoS).

Etiqueta de flujo: Este campo tiene 20 bits. Se usa para marcar paquetes de determinados flujos, a fin de que puedan ser diferenciados en la capa de red. Así, los enrutadores pueden identificar flujos específicos y hacer procesamiento por flujo sin la necesidad de buscar dentro del paquete. Esto hace que el proceso sea más eficiente. Este campo también permite que las aplicaciones puedan identificar el tráfico en los sistemas finales, lo que facilita ofrecer QoS a paquetes que han sido cifrados con IPSec.

Longitud de carga: Este campo tiene 16 bits. Indica la longitud del paquete. Además, incluye los encabezados de extensión y la Unidad de Datos del Protocolo (*Protocol Data Units, PDU*) de nivel superior. Con 16 bits, se puede indicar una carga IPv6 de hasta 65 535 bytes. Para longitudes de

carga superiores a 65 535 bytes, este campo se establece en el valor 0 y se utiliza la opción de carga *Jumbo* en el encabezado de extensión "Opciones de salto a salto".

Encabezado siguiente: Este campo identifica el tipo de información que sigue a continuación del encabezado principal de IPv6. Esta información puede ser un paquete de la capa superior, tal como TCP o Protocolo de Datagrama de Usuario (*User Datagram Protocol, UDP*), o una cabecera de extensión. IPv6 utiliza una manera diferente de manipular los datos opcionales en el encabezado del paquete. En él se define una serie de encabezados de extensión enlazados por el campo "Encabezado Siguiente", encontrado en cada una de los encabezados de extensión. Este mecanismo ofrece mayor eficiencia en el procesamiento de estos, posibilita una mayor velocidad de reenvío, y disminuye la carga de trabajo del enrutador. El diseño de la cabecera de IPv6 permite ampliar fácilmente el protocolo con nuevas características si se agregan encabezados de extensión tras el encabezado del IPv6.

Límite de saltos: Indica el número máximo de enlaces por los que puede viajar el paquete IPv6 antes de que se descarte. El tamaño de este campo es de 8 bits. Cuando el límite de saltos es igual a 0, el paquete se descarta y se envía un mensaje "Fin de tiempo de espera" de ICMP, a la dirección IP de origen.

Dirección de origen: Tiene 128 bits, que son los necesarios para poner la dirección de la terminal de origen.

Dirección de destino: El tamaño es de 128 bits y almacena la dirección del nodo de destino. En la mayoría de los casos, la dirección de destino se establece en la dirección de destino final, pero si hay un encabezado de extensión de "Enrutamiento", la dirección de destino se puede establecer en la interfaz del siguiente enrutador de la lista de rutas de origen. Los encabezados de IPv4 no pueden funcionar conjuntamente con los encabezados de IPv6. Un nodo o un enrutador debe utilizar una implementación de IPv4 e IPv6 para reconocer y procesar ambos formatos de encabezado.

2.1.2. Encabezados de extensión

El encabezado de IPv4 incluye todas las opciones. Por lo tanto, cada enrutador intermedio debe comprobar su existencia y procesarlas cuando están presentes. Esto puede causar un deterioro del rendimiento en el reenvío de paquetes IPv4. Con IPv6, las opciones de entrega y reenvío pasan a los

encabezados de extensión. El único encabezado de extensión que debe procesarse en cada enrutador intermedio es el encabezado de extensión "Opciones de salto a salto". Así aumenta la velocidad de procesamiento del encabezado de IPv6 y mejora el rendimiento del proceso de reenvío. Los encabezados de extensión de IPv6 que deben admitir todos los nodos de IPv6 son:

1. **Encabezado de Opciones salto a salto**: Se utiliza para especificar parámetros de entrega en cada salto de la ruta de acceso al destino. Se identifica por el valor 0 en el campo "Encabezado siguiente".
2. **Encabezado de Opciones de destino**: Se utiliza para especificar parámetros de entrega de paquetes para destinos intermedios o para el destino final. Este encabezado se identifica mediante el valor 60 en el campo "Encabezado siguiente" del encabezado anterior.
3. **Encabezado de Enrutamiento**: De forma similar al enrutamiento de origen que admite IPv4, los nodos de origen de IPv6 pueden utilizar el encabezado de extensión de Enrutamiento para especificar una ruta desde el origen. Esta ruta es una lista de destinos intermedios por donde debe viajar el paquete hasta su destino final. El encabezado de Enrutamiento se identifica mediante el valor 43 en el campo "Encabezado siguiente" del encabezado anterior.
4. **Encabezado de Fragmentación**: Se utiliza para los servicios de fragmentación y ensamblado de IPv6. Este encabezado se identifica por el valor 44 en el campo Encabezado siguiente del encabezado anterior.
5. **Encabezado de Autenticación**: Proporciona autenticación de datos (comprobación del nodo que envió el paquete), integridad de datos (comprobación de que los datos no fueron modificados en el tránsito) y protección contra reproducción (garantía de que los paquetes capturados no se pueden volver a transmitir ni ser aceptados nuevamente como datos válidos) para el paquete IPv6. El encabezado de Autenticación, forma parte de la arquitectura de seguridad para el Protocolo Internet y se identifica por el valor 51 en el campo "Encabezado siguiente" del encabezado anterior.
6. **Encabezado de Carga de seguridad de encapsulación**: Proporciona servicios de confidencialidad, autenticación e integridad de datos para la carga encapsulada. Se diferencia del encabezado de Autenticación en que proporciona servicios de integridad y autenticación de datos para todo el paquete IPv6. Este encabezado se identifica por el valor 50 en el campo "Encabezado siguiente" del encabezado anterior.

En un paquete IPv6 típico, no hay encabezados de extensión. Si se precisa un tratamiento especial por parte de los enrutadores intermedios o de destino, el nodo de envío agrega uno o varios encabezados de extensión. Cada uno de ellos debe adaptarse a los límites de 64 bits (8 bytes). Los encabezados de extensión de tamaño variable contienen un campo "Longitud de extensión de encabezado" y deben utilizar el relleno, cuando sea necesario para asegurarse que el tamaño sea múltiplo de 8.

Los encabezados de extensión se procesan en el orden en que se encuentran. Dado que, el único encabezado de extensión procesado por todos los nodos de la ruta de acceso es el encabezado de Opciones de salto a salto, este debe ser el primero. Hay normas similares para otros encabezados de extensión. Se recomienda que se coloquen en el encabezado de IPv6 en el orden siguiente:

1. Encabezado Opciones de salto a salto.
2. Encabezado Opciones de destino, para destinos intermedios cuando hay encabezado de Enrutamiento.
3. Encabezado Enrutamiento.
4. Encabezado Fragmento.
5. Encabezado Autenticación.
6. Encabezado Carga de seguridad de encapsulación.
7. Encabezado Opciones de destino, para el destino final.

Todos los encabezados pueden aparecer, a lo sumo, una vez en el paquete IPv6, con la excepción del encabezado de Opciones de Destino, el cual puede aparecer dos veces; una antes del encabezado de enrutamiento, y la otra justo antes del encabezado del protocolo del nivel superior.

2.1.3. Unidad de datos del protocolo de nivel superior

La unidad de datos de protocolo (PDU) de nivel superior suele constar de un encabezado de protocolo de nivel superior y su carga (un mensaje ICMP, un mensaje UDP o un segmento TCP). La carga del paquete IPv6 es la combinación de los encabezados de extensión de IPv6 y la PDU de nivel superior.

2.2. Arquitectura de direccionamiento.

Con el surgimiento de IPv6 se elimina una de las principales limitaciones que tiene IPv4 que es el insuficiente número de direcciones que restan por asignar, además de sustituir un tipo de dirección (difusión) por otra, para mejorar la eficiencia de la red.

2.2.1. Espacio de direcciones

La principal causa del surgimiento del IPv6, y una de sus características que más llama la atención, es su amplio espacio de direcciones. Una dirección IPv6 tiene 128 bits, lo que implica 340 282 266 920 938 463 374 607 431 768 211 465 direcciones, muy superior a las casi 4 300 millones de direcciones del IPv4.

2.2.2. Tipos de direcciones IPv6

Se han definido tres (3) tipos de direcciones IPv6:

1. **Unidifusión (*Unicast*)**: Una dirección *unicast* identifica a una sola interfaz en el ámbito del tipo de dirección de *unicast*. Con la topología de enrutamiento de *unicast* apropiada, los paquetes dirigidos a una dirección de *unicast* se entregan a una sola interfaz. Para ajustarse a los sistemas de equilibrio de carga, permite que varias interfaces utilicen la misma dirección, siempre y cuando las distintas interfaces aparezcan como una sola interfaz para la implementación de IPv6 en el nodo [1].
2. **Multidifusión (*Multicast*)**: Una dirección de *multicast* identifica a varias interfaces. Con la topología de enrutamiento de *multicast* apropiada, los paquetes dirigidos a una dirección de *multicast* se entregan a todas las interfaces identificadas por la dirección. Existen varias direcciones de *multicast* reservadas para uso específico [1].
3. ***Anycast***: Una dirección de *anycast* identifica a varias interfaces. Con la topología de enrutamiento apropiada, los paquetes dirigidos a una dirección *anycast* se entregan a una sola interfaz, la más próxima que identifica la dirección. La interfaz "más próxima" se define como la más cercana en términos de distancia de enrutamiento. Una dirección de *multicast* se utiliza para la comunicación "de uno a muchos", con entrega a varias interfaces. Una dirección de *anycast* se utiliza para la comunicación "de uno a uno de muchos", con entrega a una sola interfaz. Estas direcciones no tienen que pertenecer al mismo nodo, por lo que pueden utilizarse para implementar servicios redundantes, como puede ser el servicio de nombres de dominio. [1]

2.2.3 Sintaxis de las direcciones IPv6

La dirección de IPv6 se divide en límites de 16 bits y cada bloque de 16 bits se convierte en un número hexadecimal de 4 dígitos y se separa con signos de dos puntos (:). La siguiente cadena es un ejemplo de una dirección IPv6: 2002:C837:99C1:0000:0000:0000:0000:0001.

Para facilitar su representación, se permiten mecanismos de contracción de la dirección, eliminando los ceros consecutivos. Por consiguiente la dirección anterior puede representarse de la forma: 2002:C837:99C1::1. Es válido decir que la compresión de ceros solo se puede realizar en una de las cadenas consecutivas que existan dentro de la dirección IP. De no efectuarse esto, no habría forma de determinar la cantidad de ceros que corresponderían a cada cadena compactada. Otro detalle importante a señalar es el uso de los prefijos. Por ejemplo, 2002:C837:99C1::1/48 indica que los primeros 48 bits de la dirección corresponden al prefijo de red. La notación de prefijo también se utiliza para expresar los identificadores de red o de subred. [1]

2.2.4 Identificadores de interfaz.

Los identificadores de interfaz en las direcciones *unicast* IPv6 se utilizan para la identificación de interfaces en un determinado enlace. Es necesario que sean únicos en el enlace, aunque no tienen que seguir siendo únicos en un ámbito mayor que este. Por norma general, los identificadores se obtendrán a partir de las direcciones de la capa de enlace y estos pueden ser utilizados en múltiples interfaces del mismo nodo, siempre y cuando no estén conectadas al mismo enlace.

2.2.5 La dirección no especificada.

Así es como se le llama a la dirección 0:0:0:0:0:0:0:0. Esta nunca debe ser asignada a ningún nodo y sólo se permite su uso en casos bien contados, como en el campo de "Dirección origen", cuando una interfaz no tiene asignada ninguna aún. Bajo ningún concepto se debe usar esta dirección como dirección destino de un paquete IPv6 o en la cabecera de Enrutamiento.

2.2.6 La dirección de lazo ("Loopback").

La dirección *unicast* 0:0:0:0:0:0:0:1 recibe el nombre de lazo. Se usa para la comunicación entre servicios de un mismo nodo y nunca se debe mandar un paquete con esta dirección, tanto de origen como destino, sobre un medio físico.

2.2.7 Direcciones IPv6 con direcciones IPv4 embebidas.

Dentro de los mecanismos previstos de transición de IPv4 a IPv6, existe una técnica que permite a las terminales y enrutadores crear túneles dinámicamente, a fin de enviar paquetes IPv6 sobre la infraestructura IPv4 existente. Los nodos que vayan a utilizar esta técnica recibirán una dirección *unicast* IPv6 un tanto especial: los 32 bits más bajos serán la dirección IPv4. A este tipo de direcciones se las llama direcciones IPv6 compatibles con IPv4. También existe otro tipo de dirección IPv6 que contiene a una IPv4 y se utilizará para representar aquellos nodos que sólo disponen de pila IPv4. En este caso los 32 bits más bajos serán iguales que en el caso anterior (la dirección IPv4), pero los 16 bits siguientes por delante serán todos "1". Este tipo de direcciones recibe el nombre de direcciones "*IPv4-mapeado IPv6*".

2.3. Unidad de Transferencia Máxima (MTU) de la ruta.

IPv6 requiere que el nivel de enlace admita un tamaño mínimo de 1 280 bytes para los paquetes IPv6. Los niveles de enlace que no admiten este tamaño deben proporcionar una combinación de fragmentación y reensamblado de nivel de enlace transparente para IPv6. En los niveles de enlace que admiten un tamaño de MTU que se puede configurar, se recomienda que se configuren con un tamaño de MTU de, al menos, 1 500 bytes. [1]

Los nodos de origen de IPv6 pueden fragmentar cargas de protocolos de nivel superior que sean mayores que la unidad MTU de ruta de acceso mediante el proceso y el encabezado de Fragmentación descrito anteriormente. Sin embargo, no se recomienda en absoluto utilizar la fragmentación de IPv6. Un nodo IPv6 debe ser capaz de reensamblar un paquete fragmentado con un tamaño de, al menos, 1 500 bytes.

2.3.1. Descubrimiento de MTU de ruta de acceso.

Al igual que el IPv4, IPv6 proporciona un proceso de descubrimiento de MTU de ruta de acceso mediante el mensaje "Paquete demasiado grande" de ICMP. La unidad MTU de ruta de acceso se descubre mediante el siguiente proceso [1]:

1. El nodo de origen asume que la unidad MTU de la ruta de acceso es la MTU de vínculo de la interfaz en la que se está reenviando el tráfico.
2. El nodo de origen envía datagramas IP con el tamaño de MTU de ruta de acceso.

3. Si un enrutador de la ruta de acceso no puede reenviar el paquete a través de un vínculo con una MTU de vínculo menor que el tamaño del paquete, descarta el paquete IPv6 y devuelve un mensaje "Paquete demasiado grande" al nodo de origen. El mensaje ICMP "Paquete demasiado grande" contiene la unidad MTU del vínculo en el que se produjo el error de reenvío.
4. El nodo de envío configura la unidad MTU de ruta de acceso para los paquetes que se envían al destino, con el valor del campo MTU en el mensaje ICMP "Paquete demasiado grande".

El nodo de envío vuelve a empezar en el paso 2 y repite los pasos 2 a 4, tantas veces como sea necesario, para descubrir la unidad MTU de ruta de acceso. Esta se determina cuando no se reciben mensajes ICMP "Paquete demasiado grande adicionales" o cuando se recibe un mensaje de confirmación del destino. Se recomienda que los nodos IPv6 admitan el descubrimiento de MTU de ruta de acceso. Aquellos que no lo hagan, deben utilizar la unidad MTU de enlace mínima de 1 280 bytes, como MTU de ruta de acceso. [1]

En la figura 2.3 se muestra este proceso, donde el MTU de la ruta del origen al destino resulta ser de 1 300 bytes.

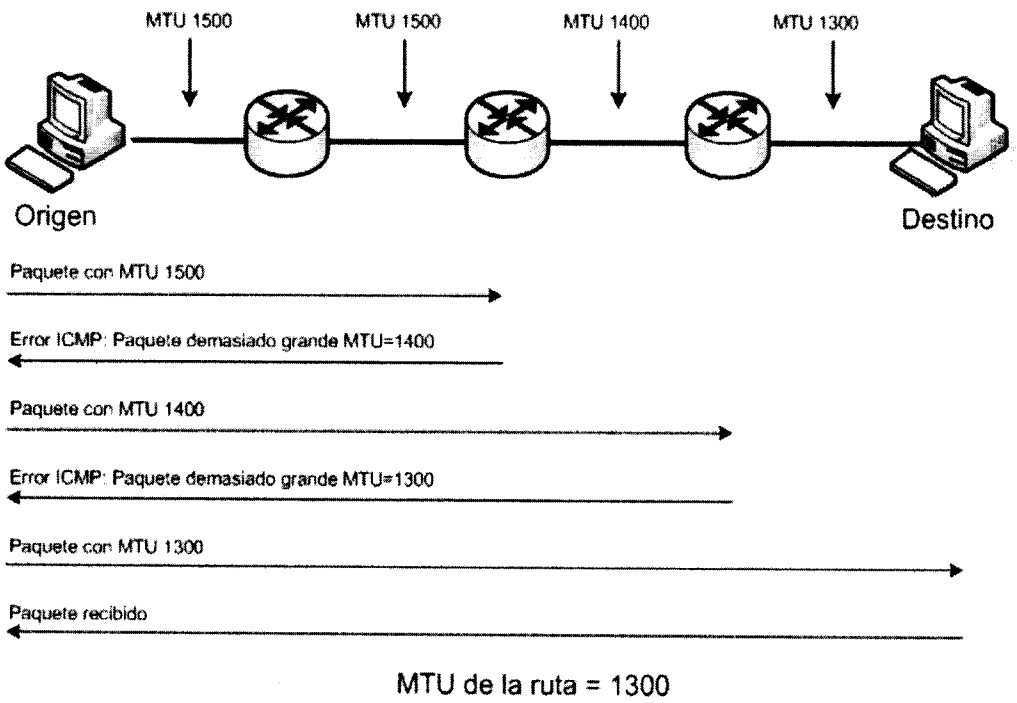

Fig. 2.3 Descubrimiento de MTU de la ruta de acceso

2.3.2. Cambios en MTU de ruta de acceso.

Debido a los cambios de la topología de enrutamiento, la ruta de acceso entre el origen y el destino puede cambiar con el tiempo. Cuando una nueva ruta de acceso necesita una MTU de ruta de acceso menor, el proceso anterior empieza en el paso 3 y repite los pasos 2 a 4, hasta que se descubre la nueva MTU de ruta de acceso. Las disminuciones de MTU de ruta de acceso se descubren inmediatamente a través de la recepción de mensajes ICMP "Paquete demasiado grande". El nodo de envío debe detectar los incrementos en la MTU de ruta de acceso. El nodo de envío puede intentar enviar un paquete IPv6 mayor, después de un mínimo de 5 minutos (se recomienda 10 minutos) al recibir un mensaje ICMP "Paquete demasiado grande'. [1]

2.4. Versión de Protocolo de Mensaje de Control de Internet (ICMPv6)

IPv6 no proporciona servicios para informar acerca de la existencia de errores. En su lugar, IPv6 utiliza una versión actualizada de ICMP, llamada ICMPv6 [1]. ICMPv6 presenta las funciones comunes de ICMP para IPv4, relativas a la elaboración de informes acerca de errores de entrega o reenvío y proporciona un servicio de eco simple para la solución de problemas. El protocolo ICMPv6 también proporciona un marco para lo siguiente:

Descubrimiento de nodos a la escucha de multicast.

MLDv2 (*Multicast Listener Discovery, MLDv2*) [1] es un conjunto de tres mensajes ICMP que reemplazan a la versión 2 del Protocolo de administración de grupos de Internet (*Internet Group Management Protocol version 2, IGMPv2*), para que IPv4 administre la pertenencia a grupos de *multicast*.

Descubrimiento de vecino.

El Protocolo Descubrimiento de Vecino *(Neighbor Discovery, ND*) [1] es un conjunto de cinco mensajes ICMPv6 que administran la comunicación entre nodos en un enlace. ND reemplaza al Protocolo ARP, al proceso de Descubrimiento de enrutadores (*Router Discovery, RD*) y al mensaje de Redirección (*Redirect*) de ICMPv4.

2.4.1. Consideraciones de Seguridad.

ICMPv6 puede ser objeto de varios ataques, sin embargo, el mismo puede viajar en paquetes que utilicen los mecanismos de seguridad que ofrece IPv6, por lo que se disminuyen grandemente los riesgos. Por ejemplo, un administrador puede bloquear todos los mensajes IPv6 cuya fuente no pueda ser autenticada.

2.5. Enrutamiento IPv6.

Las direcciones globales de IPv6 están diseñadas para crear una infraestructura de enrutamiento jerárquica eficiente, que se puede resumir, basada en la aparición de múltiples niveles de proveedores de servicios Internet. En Internet IPv6, los enrutadores troncales tienen tablas de enrutamiento mucho más pequeñas, que corresponden a la infraestructura de enrutamiento de agregadores de nivel superior. IPv6 soporta la mayoría de los protocolos de enrutamiento que existen en la actualidad.

2.5.1. Protocolo de información de enrutamiento.

El Protocolo de Información de enrutamiento de Próxima Generación (RIPng) [1] funciona de igual manera y ofrece los mismos beneficios que el Protocolo de Información de enrutamiento versión 2 (RIPv2) [1]. Las mejoras de RIPng incluyen el soporte de las direcciones IPv6 y sus prefijos. RIPng utiliza la dirección *multicast* FF02::9, para enviar sus mensajes de actualización de rutas.

2.5.2. Protocolo abierto del camino más corto, versión 3.

A pesar de que la mayoría de los algoritmos del Protocolo Abierto del Camino más Corto versión 2 (OSPFv2), son los mismos que los de la versión 3, fueron necesarios algunos cambios, fundamentalmente para soportar las nuevas direcciones IPv6 [1]. Algunos de los cambios más notables incluyen la implementación independiente de la plataforma, procesamiento del protocolo por enlace en vez de por nodo, soporte explícito de múltiples instancias por enlace, y cambios en los mecanismos de autenticación y el formato del paquete.

2.5.3. Protocolo IS-IS.

El protocolo IS-IS es un protocolo de pasarela interior *(Interior Gateway Protocol, IGP)* el cual ha sido modificado para soportar IPv6. Existen propuestas para el intercambio de información de rutas IPv6 usando el protocolo IS-IS y los mecanismos empleados por este para IPv4 [1].

2.5.4. Multiprotocolo de frontera de pasarela.

El Multiprotocolo de frontera de pasarela (*Multiprotocol BGP*) es un protocolo de pasarela exterior (*Exterior Gateway Protocol,* EGP) que funciona de la misma manera que en IPv4, aunque se le han adicionado algunos atributos para el soporte de IPv6 [1].

2.6. Autoconfiguración.

La autoconfiguración es otra de las ventajas que ofrece IPv6 respecto al IPv4. Este proceso resulta transparente para el usuario y consiste en:

- La creación de una dirección de enlace local y comprobar su unicidad en el enlace.
- Determinar qué tipo de información se debe autoconfigurar.
- En el caso de direcciones; determinar qué mecanismo se debe usar para obtenerlas.

La obtención automática de configuración sólo se aplica a terminales y nunca a enrutadores, aunque estos pueden generar su propia dirección de enlace local. IPv6 define tres tipos de mecanismos de autoconfiguración, los cuales se explican a continuación:

2.6.1. Autoconfiguración sin control de estado.

En el caso de autoconfiguración sin control de estado, la configuración necesaria en los terminales es nula y prácticamente nula en los enrutadores. El mecanismo permite al terminal obtener una dirección a partir de información local (el identificador de la interfaz) e información anunciada por los enrutadores (el prefijo de subred). En caso de que no haya enrutadores en el enlace, los terminales pueden generar sus propias direcciones de enlace local utilizando el prefijo reservado para las direcciones locales de enlace (FE80::/64). Estas direcciones le son suficientes para comunicarse entre sí en el enlace [1].

Los objetivos del diseño de este mecanismo son los siguientes:

- No debe ser necesaria la configuración de terminales independientes antes de conectarlos a la red. Para esto, el proceso de autoconfiguración asume que cada interfaz puede suministrar un identificador para formar la dirección IP, junto a un prefijo de red predefinido.
- Las redes pequeñas, que consistan en la interconexión de pocos terminales a un mismo enlace, no deben necesitar la presencia de un enrutador o un servidor que les brinde la configuración necesaria para comunicarse entre sí. Para esto se utilizan las direcciones de *unicast* locales de enlace.
- Las redes un poco más grandes, que consistan en la interconexión de varias subredes a través de enrutadores, no deben necesitar la presencia de servidores que le brinden la comunicación necesaria para comunicarse entre sí. Para esto, los enrutadores se encargan de enviar periódicamente avisos a la red sobre que prefijo utilizar.
- La configuración automática debe servir para facilitar el cambio de numeración de una red de forma transparente para el usuario. Para garantizar este objetivo, se le asignan tiempos de vida a cada dirección asignada a los terminales. En caso de querer cambiar la numeración, se le asignan nuevas direcciones a las interfaces con nuevos tiempos de vida. En el período de transición, ambas direcciones son válidas, hasta que una deja de existir.
- Debe ser posible especificar administrativamente qué mecanismo deben utilizar los terminales para configurarse. De esto también se encargan los enrutadores, los cuales pueden enviar esta información a la red.

2.6.2. Autoconfiguración con control de estado.

En el caso de autoconfiguración con control de estado, los terminales obtienen sus direcciones y otra información de algún servidor. Este servidor puede mantener un control preciso de cuales direcciones han sido asignadas a cada terminal.

A tal efecto, como se explicó anteriormente, se ha desarrollado una versión específica de DHCP para IPv6 llamada DHCPv6 [1] de la cual se resaltan los siguientes aspectos:

- Para la implementación de este mecanismo de autoconfiguración, los terminales se comunican con el servidor mediante el protocolo UDP.
- Los clientes utilizan una dirección local de enlace como origen de sus mensajes.

- Los clientes utilizan el puerto 546 UDP para la comunicación
- Los servidores reciben los mensajes en una dirección *multicast* reservada para ese propósito. Esta dirección es utilizada por el cliente en la mayoría de los mensajes, incluso después de recibir la configuración inicial.
- Los servidores escuchan en el puerto 547 UDP.
- En el caso en que el servidor DHCP no se encuentre en el mismo enlace que el cliente, debe existir un agente DHCP encargado de asignarle la configuración. Esto debe ser transparente para el cliente.
- Tanto los clientes como los servidores, utilizan un identificador único de DHCP. Este no debe cambiar en el tiempo y debe utilizarse el mismo para todas las interfaces, aunque en ocasiones éste se calcula a partir de una de ellas.
- Existe un mecanismo de seguridad en el protocolo DHCPv6, que trata de garantizar la autenticidad de la identidad de los clientes y los servidores, y la integridad del mensaje, no así su privacidad.

La posibilidad de utilizar direcciones multicast y no de difusión (broadcast) en la configuración inicial, es un detalle ventajoso que ofrece IPv6, haciendo más eficiente el trabajo del protocolo.

2.6.3. Autoconfiguración sin control de estado usando DHCPv6.

Existe, además, una extensión al protocolo DHCPv6 que le permite entregar configuración a los terminales sin mantener información de su estado [1]. Este mecanismo es útil para que estos obtengan información adicional a la dirección IP, como puede ser una lista de servidores DNS, sin que se necesite reservar ningún recurso en el servidor. Para que este mecanismo funcione, los terminales deben adquirir una dirección IP por otra vía, típicamente a través del mecanismo de autoconfiguración sin control de estado mencionado anteriormente.

2.6.4. Detección de direcciones.

Para asegurarse de que las direcciones sean únicas, los nodos ejecutan un algoritmo de detección de direcciones duplicadas [1]. Este mecanismo debe ser utilizado en la obtención de una dirección *unicast* por cualquier método (con estado o sin él), con las siguientes excepciones:

- No debe ser utilizado en la verificación de direcciones *anycast*.

- Una implementación puede asumir que; sí se asignan bien los prefijos de red en un enlace, solo es necesario verificar la unicidad de la dirección local de enlace. Esto conlleva a verificar la unicidad del identificador de interfaces en el mismo.

Básicamente el mecanismo de detección de direcciones duplicadas se basa en la emisión de mensajes de solicitud o descubrimiento de vecinos. Si se encuentra alguna dirección duplicada durante el proceso, la misma no podrá ser asignada a la interfaz. Si la dirección fue generada a partir de un identificador de interfaz, debe darse la posibilidad de cambiar este identificador.

2.6.5. Consideraciones de seguridad.

La configuración automática tiene implicaciones de seguridad implícitas, permitiéndole a cualquier terminal obtener información para comunicarse en la red. En el caso de la configuración sin estado, existe además el riesgo de un ataque de negación de servicio, ya que un terminal pudiera comenzar a responder a mensajes de solicitud de vecinos para cualquier dirección. Como resultado de este comportamiento, estas direcciones no podrían ser asignadas. En el caso de la configuración en presencia de un servidor DHCP, aunque existe el mecanismo de autenticación de mensajes, también existen posibles ataques de seguridad. Siempre se asume que el ataque debe originarse dentro de la red de enlace.

2.7. Seguridad integrada.

La compatibilidad con Protocolo de Seguridad de Internet (Internet Protocol Security, IPSec) es un requisito del conjunto de protocolos IPv6 [1]. Este requisito proporciona una solución basada en estándares en respuesta a las necesidades de seguridad de red y aumenta la interoperabilidad entre distintas implementaciones de IPv6.

IPSec fue diseñado originalmente para IPv6, y aunque fue adaptado a IPv4, donde se puede implementar de manera opcional, necesita de mecanismos complicados para evitar los problemas que introduce el uso del Traductor de Direcciones de Red (NAT). En IPv6 todo se vuelve mas transparente, haciendo posible las conexiones seguras extremo a extremo. IPSec no es un solo protocolo, sino un conjunto de protocolos que ofrecen seguridad a las redes IP. Como IPSec trabaja a nivel de la capa IP, es capaz de ofrecer estos mecanismos de seguridad a aplicaciones y protocolos de las capas superiores. Esto último se logra sin necesidad de mecanismos adicionales de seguridad, lo cual

constituye su mayor fortaleza. Algunos de los tipos de servicio de protección que brinda IPSec se resumen en:

- Cifrado de los datos transmitidos para lograr privacidad.
- Chequeo de la integridad de los mensajes, a fin de asegurar que no han sido cambiados en el camino.
- Protección contra algunos tipos de ataque, tales como los de respuesta.
- Posibilidad de que los dispositivos negocien los algoritmos de seguridad y las llaves requeridas.
- Trabajar en dos modos para satisfacer las necesidades de diferentes redes (modo túnel, y modo de transporte).

Las ventajas que tiene IPSec en IPv6, respecto a IPv4, vienen dadas precisamente por la facilidad que brinda IPv6 para establecer comunicaciones extremo a extremo sin el uso de NAT. Además, todas las implementaciones de IPv6 tienen que implementar IPSec.

2.8. Calidad de Servicio.

El término Calidad de Servicio (QoS) en las redes se usa al referirse a la capacidad que tiene la red de proporcionar el tipo de servicio requerido por cada aplicación. Los requerimientos de calidad varían dependiendo de los usuarios y los servicios solicitados. En las redes IP la entrega de los paquetes puede tomar minutos o eventualmente horas, como es el caso de la obtención de un archivo.

Al navegar en Internet o al solicitar acceso a una base de datos remota, la tolerancia podrá ser de segundos, pero no de minutos. En aplicaciones demandantes, tales como sesiones de voz y video en tiempo real, solo se toleran retardos de fracciones de segundos para satisfacer los requerimientos humanos, y algo, también muy importante; es el orden de llegada de los paquetes.

Como se ha señalado, IPv6 se ha diseñado teniendo en cuenta la necesidad de eficiencia en el manejo de paquetes. Además de esto, IPv6 incluye en su encabezamiento dos campos destinados a facilitar los mecanismos de calidad de servicio. Uno de ellos ya existía en IPv4 y se llama "Tipo de Servicio", que en IPv6 se llama "Clase de Servicio", el otro aparece por primera vez en el encabezado IPv6 y se llama "Etiqueta de Flujo" [1].

2.8.1 Etiqueta de flujo.

Los 20 bits del campo "Etiqueta de Flujo" pueden ser usados por la fuente para etiquetar la secuencia de paquetes, para los cuales se requiere un trato especial por los enrutadores IPv6 [1]. Ejemplo de esto puede ser; un servicio de calidad diferente de la normal o algún servicio de tiempo real. La naturaleza de este trato especial debe ser cubierta por los enrutadores, por medio de un protocolo de control, tal como el Protocolo de Reservación de Fuente (*Resource Reservation Protocol, RSVP*) [1], o por la misma información de la etiqueta de los paquetes, por ejemplo, la opción "Salto-a-Salto". Los nodos y los enrutadores que no realizan un etiquetado de flujo, fijan el campo a cero cuando originan un paquete, pasan el campo sin realizar cambios cuando les llega un paquete, e ignoran el campo cuando reciben un paquete. La etiqueta de flujo asignada es elegida de forma seudo aleatoria y uniforme en el rango de 1 a FFFFF hexadecimal. De esta manera se pasa de la forma tradicional de las quíntuplas (dirección fuente, dirección destino, puerto fuente, puerto destino, protocolo de transporte) para identificar un flujo a una tripleta (la dirección fuente, la dirección destino, la etiqueta de flujo) haciendo más eficiente el flujo en IPv6. Como el tráfico se identifica en el encabezado de IPv6, se puede proporcionar compatibilidad con QoS, incluso si la carga de paquetes está cifrada mediante IPSec.

2.9. Movilidad.

La movilidad es otra de las funcionalidades de IPv6 que revolucionará la Internet de hoy. Para que un nodo móvil pueda comunicarse mientras se mueve por diferentes enlaces debe tomar una IP de ese enlace. De esta forma es imposible que los paquetes enviados a la dirección IP principal del nodo lleguen a su destino. El protocolo de Movilidad para IPv6 [1] se encarga de que se pueda alcanzar a un nodo aunque este se esté moviendo por Internet, conectándose a diferentes puntos de acceso. Para lograr este objetivo, el protocolo permite que el nodo mantenga su dirección IP principal y encamina todos los paquetes hacia la nueva dirección IP del enlace en el que se encuentra conectado el nodo. De esta forma se logra que el movimiento del nodo por los diferentes puntos de acceso a la red sea transparente para los protocolos y las aplicaciones de niveles superiores.

2.9.1. Comparación de la Movilidad en IPv4 e IPv6.

El diseño de la Movilidad en IPv6 se beneficia de las experiencias obtenidas en la Movilidad para IPv4 [1] y de las nuevas oportunidades que ofrece IPv6. Es por esto que la movilidad en IPv6 comparte

varias de las características de la movilidad en IPv4, pero ahora se encuentra integrada dentro del protocolo y ofrece muchas más oportunidades. A continuación se mencionan las principales diferencias entre ambas implementaciones:

- No es necesario declarar enrutadores especiales como "Agentes extranjeros", como en IPv4. La movilidad para IPv6 funciona en cualquier lugar, sin necesitar algún tipo de soporte especial por parte del enrutador local.
- El soporte de la optimización de las rutas es algo esencial dentro del protocolo y no un conjunto de extensiones no estándar como sucede en IPv4.
- La optimización de rutas puede funcionar de forma segura, incluso sin asociaciones previas de seguridad.
- Se permite la coexistencia de los mecanismos de optimización de rutas con enrutadores que realizan filtrado en entrada [1].
- Los mecanismos de descubrimiento de vecinos de IPv6 aseguran la comunicación entre el nodo móvil y el enrutador por defecto del enlace actual.
- La mayoría de los paquetes que se envían a un nodo móvil, mientras se encuentra fuera de su enlace principal, se envían utilizando encabezados de enrutamiento y no túneles. Esto reduce la carga que se le adiciona a la red.
- La movilidad IPv6 no es dependiente del protocolo del nivel de enlace, ya que no usa el protocolo de resolución de direcciones (ARP), sino el protocolo de Descubrimiento de Vecino (ND) de IPv6, lo cual además le brinda robustez al protocolo.
- El mecanismo de descubrimiento dinámico de la dirección del agente del enlace principal le devuelve una sola dirección al nodo móvil. En IPv4 se utilizaba un mecanismo de difusión dirigida (*directed broadcast*) que retornaba respuestas independientes desde cada agente del enlace principal.

2.9.2. Funcionamiento básico de la Movilidad en IPv6.

El funcionamiento básico, de forma simplificada, de la Movilidad IP, se resume de la siguiente forma:

- Un nodo móvil siempre debe poder ser alcanzado por su dirección principal, sin importar si este se encuentra conectado a su enlace principal o a cualquier otro enlace.

- La dirección principal de un nodo es una dirección que se le asigna en su enlace principal. Mientras un nodo móvil se encuentra en su enlace principal, los paquetes dirigidos a él se encaminan siguiendo los mecanismos tradicionales de IPv6.
- Cuando un nodo móvil se mueve de su enlace principal y se conecta a otro enlace, adquiere direcciones de ese enlace. Para esto utiliza cualquiera de los mecanismos de configuración automática de IPv6, y comienza a recibir paquetes dirigidos a esas direcciones.
- Cuando un nodo móvil adquiere una dirección de otro enlace, le envía un mensaje al enrutador de su enlace principal con una correspondencia entre su dirección principal y la nueva dirección en la que puede recibir paquetes.
- Los nodos móviles también pueden enviar información sobre su estado actual a los nodos con los que se está comunicando.
- Existen dos modos de comunicación entre el nodo móvil y el nodo remoto. Un modo es a través de túneles en dos sentidos, pasando por el enrutador que se comporta como agente del nodo móvil. El otro es mediante optimización de rutas, el cual es mucho más eficiente pero requiere soporte para movilidad IPv6 en ambos nodos.

Hasta aquí se enuncian las principales especificaciones técnicas relacionadas con el Protocolo de Internet versión 6, lo cual forma parte del marco teórico de esta investigación.

CAPÍTULO 3

Introducción.

En el actual capítulo se presenta una propuesta de estrategia para la implementación del Protocolo IPv6 en la red de la Universidad de Ciencias Informáticas. Para ello se ha tenido en cuenta, además de las posibilidades y ventajas que brinda dicho protocolo, las características físicas de la propia red y los servicios que esta ofrece. Adicionalmente se tuvo presente las propuestas existentes para el cambio de la actual topología de la red y la adquisición de nuevo equipamiento, esto último en fase de ejecución. Todo lo anterior, bajo la premisa de que la introducción de IPv6 debe transcurrir sin afectar la vitalidad de la red.

A continuación se describe la red de la UCI en cuanto a su topología y servicios.

3.1 Descripción de la red de la UCI y servicios que brinda.

En la UCI está la Red de Área Local más grande del país, a la cual se conectan más de 7 500 computadoras, con unos 17 000 usuarios. De estos usuarios; casi 10 000 son estudiantes y el resto son profesores y trabajadores del centro.

La red está formada por el Nodo Central (NC), 3 Nodos Nivel 1 (NN1) y otros 2 Nodos (Rectorado y TV) conectados en forma de estrella.

Las conexiones desde el NC, al Nodo del Rectorado y al Nodo de TV, constituyen enlaces a 1 Gbps Ethernet, en tanto las restantes son a 10 Gbps Ethernet. Está previsto, además, la creación de un futuro NN1 a 10 Gbps Ethernet.

Al NN1 de Docencia (ubicado en el edificio docente 4) se conectan los subnodos de cada uno de los restantes edificios docentes (incluido el subnodo del docente 4), todos mediante un enlace a una velocidad de 1 Gbps Ethernet. Lo mismo ocurre con el NN1 del bloque de Infraestructura Productiva.

El NN1 del bloque Residencia, se interconecta con cada uno de sus tres (3) subnodos mediante 2 enlaces físicos a 1 Gbps Ethernet, es decir; 2 Gbps Ethernet en total.

Todo esto conforma la espina dorsal (*Backbone*) de la red de la UCI. El protocolo que se usa entre equipos de interconexión es el Protocolo de Enrutamiento de Información versión 2 (*Router Information Protocol, RIPv2*).

La distribución actual de la red se muestra en la figura 3.1. [10]

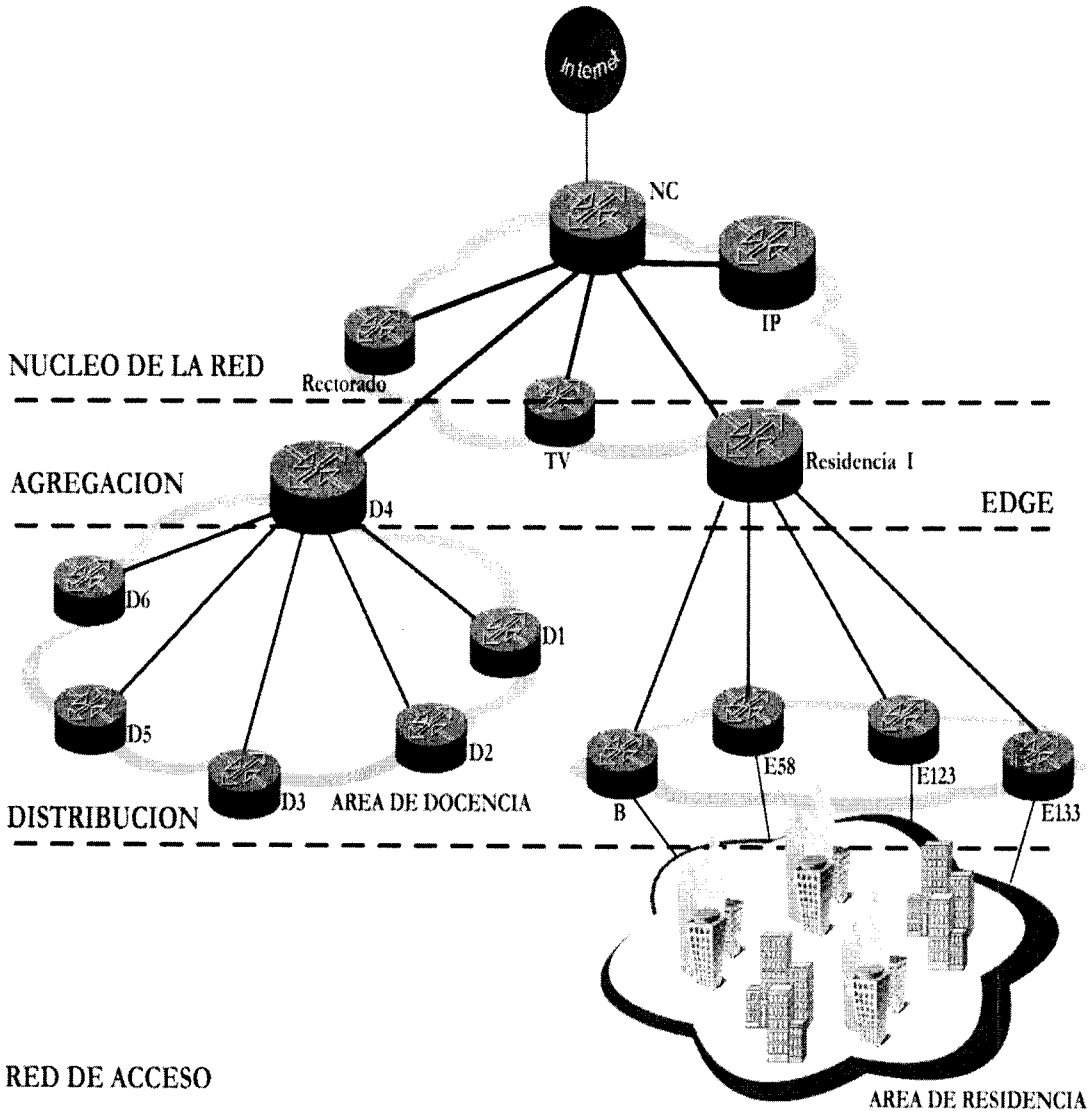

Fig. 3.1. Distribución actual de la red de la UCI.

En los niveles 1 y 2 de la red se encuentran los conmutadores *(switches)* capa 3, los cuales se encargan del enrutamiento de los paquetes. La tabla 3.1 describe el equipamiento que se utiliza.

Fabricante	Modelo	Soporta IPv6
Extreme Network	Black Diamond 6808	No
	Black Diamond 6804	No
	Alpine 3804	No
	Alpine 3802	No
	Alpine 3808	No

Tabla 3.1. Equipamiento que se utiliza en los niveles 1 y 2 de la red.

Adicionalmente, se utiliza un Router Cisco 3845 como enrutador de acceso a Internet; que sí soporta IPv6.

En el resto de la red, la velocidad de transmisión es a 100 Mbps Ethernet, y en los edificios de la Infraestructura Productiva a 1 Gbps Ethernet.

La red de la UCI es una red multiservicios. En su arquitectura se muestran 4 capas, las cuales se explican a continuación.

- Núcleo.- Es la capa donde se encuentran los nodos principales (NC y NN1). Su principal función es el manejo del flujo de datos a gran escala.
- Capa de Agregación.- Se encarga de enlazar nuevos nodos al núcleo de la red, es decir, agrega los nodos nivel 2 (NN2). La Capa de Agregación es una capa intermedia que permite escalar en la cantidad de nodos de acceso que se conectan al borde.
- Capa de Distribución.- Es la capa que contendrá a los nodos que distribuirán la red para brindar servicios al usuario final, o lo que es lo mismo, son aquellos nodos que harán de borde entre el núcleo de la red y la Capa de Acceso.
- Capa de Acceso.- Es donde se encuentran los conmutadores a los cuales se conectan los usuarios finales.

Esta red ofrece un variado grupo de servicios. Estos van, desde los más tradicionales; correo electrónico, mensajería instantánea, acceso a Internet, FTP, entre otros, hasta los más especializados,

como son; la plataforma *Moodle* (para la docencia), el portal de las Comunidades de Desarrollo, Infodrez (portal de ajedrez) e Inter-nos (portal de video bajo demanda).

Uno de los aspectos con más demanda en el centro es la TV. La Universidad dispone de varios canales internos, además de los 4 canales nacionales, Cubavisión Internacional y el canal Habana. Todos se transmiten por cables dedicados, mediante una red independiente a la red de datos.

Actualmente, las señales provenientes de cada uno de los canales antes mencionados se toman del receptor de satélite o del aire (discriminando uno u otro, en dependencia del nivel de señal) y se modulan, mejorando la calidad de la recepción. Para el caso de los canales internos de la Universidad, se dispone de un servidor de video para cada uno de ellos, a partir de los cuales se extrae las señales de audio y video, que luego también son moduladas. Todas estas señales, ya moduladas, son inyectadas a la red de distribución de TV, en tiempo real.

A continuación, en la figura 3.2, se muestra de manera gráfica la actual red de distribución de TV de la UCI. [11].

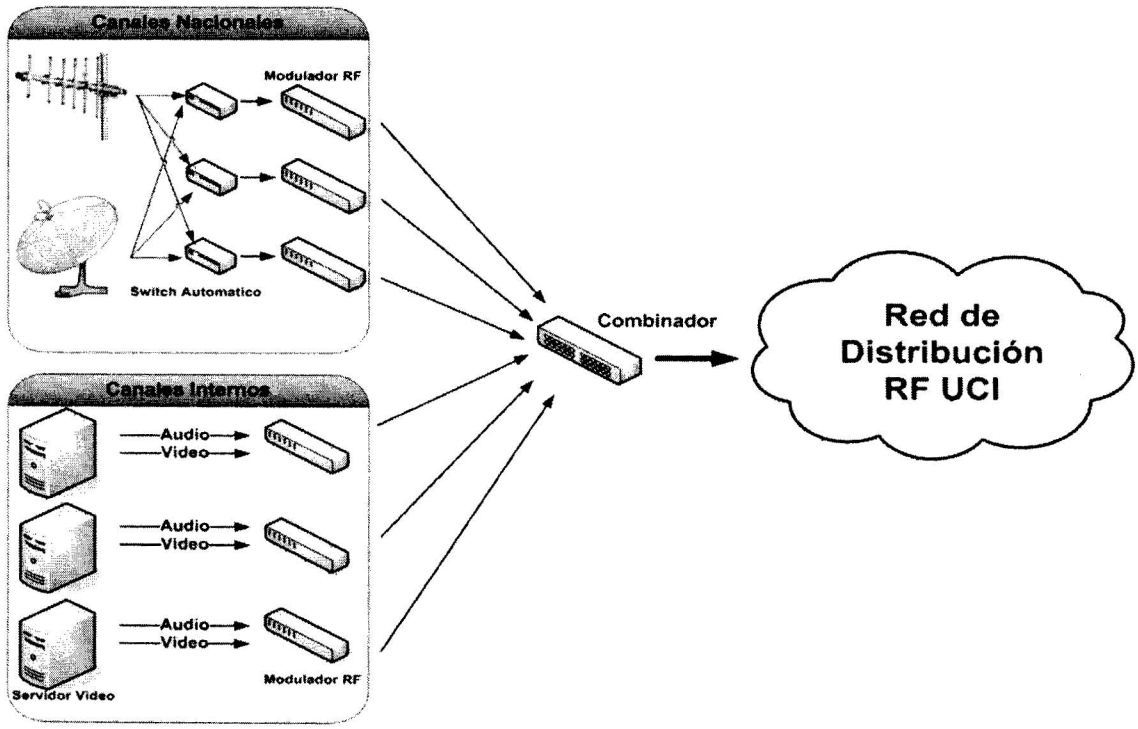

Fig. 3.2. Distribución actual de la red de televisión de la UCI.

3.2 Ventajas de la implementación de IPv6 en la UCI.

Dentro de las ventajas que acarrea la implementación del IPv6, muchas de las cuales se han enunciado en el capitulo anterior, valdría la pena analizar en detalles aquellas que, para el caso particular de la Universidad, resultan neurálgicas. Ellas son:

- Seguridad
- Calidad de servicio

3.2.1 Seguridad.

Con la adopción de medidas de seguridad en la capa IP, se consigue proporcionar, de manera independiente y totalmente transparente al usuario, medidas de seguridad a todas las capas superiores (TCP, UDP,...) sin ningún costo adicional.

Como se explicó en el capítulo anterior, IPv6 incorpora el IPSec, que proporciona autenticidad y confidencialidad a los datagramas IP que circulan por la red. Se utiliza un protocolo de dos fases para el intercambio de claves, que aprovechando la Infraestructura de Intercambio de Mensajes del Protocolo, proporciona un canal auténtico y seguro entre dos usuarios cualesquiera conectados a la red.

La seguridad en IPSec se proporciona mediante dos aspectos de seguridad (*Security Payload*): [1]

1. **Cabecera de autenticación** (*Authentication Header*). Esta cabecera es la encargada de proporcionar autenticidad a los datos (datagramas) que se reciben en dos aspectos:
    - Los datagramas provienen del origen especificado. Se garantiza la autenticidad del origen de los datos (no pueden ser repudiados).
    - Los datagramas (y por tanto los datos que contienen) no han sido modificados.
2. **Cifrado de seguridad** (*Encrypted Security Payload*). De esta forma se garantiza que tan sólo el destinatario legítimo del datagrama (datos) pueda descifrar el contenido del datagrama.

La autenticidad y el cifrado de datos (o datagramas) requieren que tanto el emisor como el receptor compartan una clave, un algoritmo de cifrado/descifrado y una serie de parámetros (como el tiempo de validez de la clave) que diferencian una comunicación segura de otra. Estos parámetros conforman la asociación de seguridad (*Security Association*) que permite unir la autenticidad y la seguridad en IPSec.

En la UCI, donde la mayoría de los servicios, ya sea de uno u otra índole en la Universidad, se soportan sobre la red de datos, los aspectos de seguridad tienen una gran importancia. La implementación de IPv6 permitirá garantizar, de manera transparente para el usuario, que la información que se reciba sea exactamente igual a la que se transmite, sin que pueda ser modificada por el camino.

Téngase presente que por la red circula información relacionada con la gestión docente y administrativa de la Universidad; pero también información y códigos de programas, comprometidos con los proyectos que se desarrollan, tanto para Cuba como para el exterior. Por lo que en este sentido, será de gran beneficio la implementación del protocolo IPV6, por su seguridad nativa.

3.2.2 Calidad de Servicio.

Como se expuso anteriormente, se le llama Calidad de Servicio (QoS) a la capacidad de una red para sostener un comportamiento adecuado del tráfico que transita por ella, garantizando un valor límite (máximo o mínimo) de alguno de los parámetros de QoS. En la tabla 3.2 se muestran algunos parámetros de Calidad de Servicio. [12]

Parámetro	Unidades	Significado
Ancho de Banda *(bandwidth)*	Kbps	Indica el caudal máximo que se puede transmitir.
Retardo *(delay)* o latencia *(latency)*	ms	El tiempo medio que tardan en llegar los paquetes.
Jitter	ms	La fluctuación que se puede producir en el Retardo.
Tasa de pérdidas *(loss rate)*	%	Proporción de paquetes perdidos respecto de los enviados.

Tabla 3.2. Parámetros de Calidad de Servicio.

Según el tipo de aplicaciones, se necesitan determinados requerimientos para cumplir los parámetros de Calidad de Servicio. En la tabla 3.3 se muestran de algunos de ejemplos. [12]

Tipo de aplicación	Ancho de Banda	Retardo	Jitter	Tasa de Pérdidas
Interactivo (telnet, www)	Bajo	Bajo	Medio/alto	Media
Batch (e-mail, ftp)	Alto	Alto	Alto	Alta
Telefonía	Bajo	Bajo	Bajo	Baja
Vídeo interactivo	Alto	Bajo	Bajo	Baja
Vídeo unidireccional (streaming)	Alto	Medio/alto	Bajo	Baja
Frágil (ej.: emulación de circuitos)	Bajo	Bajo	Medio/alto	Nula

Tabla 3.3. Requerimientos de Calidad de Servicio.

Al contar con QoS, es posible asegurar una correcta entrega de la información necesaria o crítica, dando preferencia a aplicaciones de desempeño crítico, donde se comparten simultáneamente los recursos de red con otras aplicaciones no críticas. Esto se logra mediante un uso eficiente de los recursos ante una situación de congestión, seleccionando un tráfico específico de la red, priorizándolo según su importancia relativa, y utilizando métodos de control y evasión de congestión para darles un tratamiento preferencial. Implementando QoS en una red, hace al rendimiento de la red más predecible, y la utilización de ancho de banda más eficiente.

3.2.2.1 Intercambio de Etiquetas Multiprotocolo (Multiprotocol Label Switching, MPLS).

Es un mecanismo de transporte de datos estándar creado por la IETF [1]. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

Permite acelerar el tráfico de información por la red y ayuda al uso de la Calidad de Servicio. MPLS integra sin discontinuidades los niveles de Enlace y Red del modelo de Interconexión de Sistemas

Abiertos (*Open System Interconnection, OSI*); combina lo mejor de cada uno de estos niveles (inteligencia del enrutamiento y rapidez de la conmutación), lo que da nuevas posibilidades, sobretodo en la gestión de la espina dorsal de la Red.

Entre las principales aplicaciones del MPLS está la ingeniería de tráfico, que permite adaptar los flujos de tráfico a los recursos físicos de la red, es decir, equilibrar de forma óptima la utilización de esos recursos.

3.2.2.2 Televisión sobre Protocolo de Internet (IPTV)

Otro de los planes futuros de la UCI es la implementación de la televisión sobre el Protocolo de Internet, que es una variante de televisión digital, basada en el flujo de paquetes multimediales (video streaming). Mediante esta tecnología, la señal de televisión es enviada en paquetes, por la red de datos, utilizando el protocolo IP. Esta tecnología permite la integración con otros servicios, como voz sobre IP (VoIP) y Web, conformando lo que se conoce como *Triple Play*.

Este método permite distribuir contenido de televisión sobre la red IP y brinda al usuario un servicio más personalizado e interactivo. Por ejemplo se puede ver una película en forma simultánea, mientras se intercambia archivos y se tiene una sesión de Chat.

Los servicios interactivos se pueden clasificar por nivel de interacción:

- Interactividad local: servicios interactivos que no necesitan del uso de canal de retorno.
- Interactividad global: servicios interactivos con utilización de canal de retorno (línea telefónica, SMS, ADSL, entre otros).

IPTV usa una señal de transmisión de dos vías, enviada a través de la red y servidores del proveedor; permitiéndole a los usuarios seleccionar contenido por demanda, cambiada en el tiempo, y tomar ventaja de otras opciones interactivas. El usuario deberá tener una conexión de banda ancha y un dispositivo que permita enviar y recibir los requerimientos.

La televisión digital tradicional por cable tiene la capacidad de enviar cientos de canales en forma simultánea a cada suscriptor, lo que crea limitaciones en el número de canales ofrecidos y puede contribuir a escasez del ancho de banda y degradación de la calidad. IPTV por el contrario, envía solo

un programa a la vez, y siempre que se cambia el canal o se selecciona otro programa, un nuevo hilo de contenido se transmite, del proveedor del servicio, directamente a la caja de control del usuario.

Entre las facilidades que brinda la IPTV está poder almacenar los contenidos para verlos las veces que se desee. Además permite realizar pausas, avanzar, retroceder, como si fuera una cinta de video o un DVD.

En la televisión IP se puede diferenciar dos tipos de canales: SDTV (*Standard Definition TV*) y HDTV (*High Definition TV*), definición estándar y alta definición respectivamente. Como es evidente, un canal de HDTV necesita más ancho de banda que uno SDTV (conexión a 8 Mbps por 1.5 Mbps para un canal SDTV). Esto es adicional a lo que se necesite para cualquier otro servicio que se desee brindar en la red. Naturalmente, con ese tráfico se requiere tener implementado QoS para optimizar y acelerar el flujo de los datagramas IP. [12]

Adicionalmente, la implementación de IPTV en la UCI, permitirá unir 2 redes, que en la actualidad son totalmente independientes: la red de datos (con fibra óptica y par trenzado de cobre) y la red de televisión (con cable coaxial).

3.2.2.3 Voz sobre el Protocolo de Internet (VoIP).

Voz sobre IP o Telefonía IP no es más que el enrutamiento de paquetes (de voz) sobre la red basada en el protocolo IP.

Este servicio es prácticamente gratis, puesto que se usa la misma red para llevar datos y voz; además de facilitar varias tareas como es el caso de enrutar automáticamente a un teléfono dentro de la red, sin importar su ubicación, lo que no ocurre así con las redes telefónicas convencionales.

VoIP puede facilitar tareas que serían más difíciles de realizar usando las redes telefónicas tradicionales:

- Las llamadas telefónicas locales pueden ser automáticamente enrutadas a un teléfono VoIP, sin importar desde donde se conecte a la red.
- Algunos paquetes de VoIP incluyen servicios adicionales, como son las conferencias tripartitas, retorno de llamada, remarcación automática, o identificación de llamadas.

El Estándar VoIP, definido en 1996 por la Unión Internacional de Telecomunicaciones (UIT), proporciona a los diversos fabricantes una serie de normas con el fin de que puedan evolucionar en conjunto. Por su estructura el estándar proporciona las siguientes ventajas:

- Permite el control del tráfico de la red, por lo que disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento.
- Es independiente del tipo de red física que lo soporta.
- Permite la integración con las grandes redes de IP actuales.
- Es independiente del hardware utilizado.
- Permite ser implementado tanto en software como en hardware.
- Permite la integración de voz y video.

El propio Estándar define tres elementos fundamentales en su estructura:

- Terminales: Son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware.
- *Gatekeepers*: Son el centro de toda la organización de la VoIP. Normalmente están implementadas en software. En caso de existir, todas las comunicaciones pasarían por él.
- *Gateways*: Se trata del enlace con la red telefónica tradicional, actuando de forma transparente para el usuario.

Con estos tres elementos, la estructura de la red VoIP podría ser la conexión entre los distintos edificios de la Universidad. La ventaja es inmediata pues todas las comunicaciones internas serían completamente gratuitas. [12]

3.3 Migración de la red de la UCI hacia IPv6.

Tal y como se explicó anteriormente, el camino al IPv6 no es una simple transición o migración, se trata de un proceso de evolución e integración ordenada, que requiere de la preparación y del mejoramiento de la red, lo cual implica; la capacitación del personal técnico, la adquisición de equipamiento, y la configuración de sistemas operativos e instalación de las aplicaciones necesarias, entre otros. Todo, en función de los servicios que se quieran brindar; con la premisa de que cumplan las especificaciones IPv6, pero sin soslayar las de IPv4.

En el caso de la UCI, donde los niveles de informatización son altos y la vida misma de la Universidad se soporta sobre esta red, no resulta viable interrumpir, por un período de tiempo dado, todos los servicios que ofrece la misma y, en este lapso, realizar los cambios necesarios.

Precisamente, el problema planteado en esta investigación fue definir bajo qué condiciones sería viable la implementación de IPv6 en la red de la Universidad, sin afectar su vitalidad. Después de realizados los análisis correspondientes, se propone en una primera fase, implementar IPv6 en el núcleo de la red, que incluye las siguientes capas: núcleo, agregación y distribución. Esto implica que en la red de la UCI estarán conviviendo los 2 protocolos, pues en la capa de acceso se continuará utilizando el protocolo IPv4.

Una vez finalizada esta etapa y teniendo en cuenta las experiencias adquiridas, se recomienda proceder a diseñar la implementación de este protocolo en la capa de acceso.

Resulta imprescindible para poder realizar esta migración, la adquisición de equipamiento que soporte IPv6, pues el actual no tiene estas prestaciones. Hoy existe en la Universidad una propuesta para la sustitución del equipamiento de interconexión de la red (*conmutadores* y enrutadores), que prevé la solución de este problema.

Como parte de esta propuesta, se gestiona la compra de equipamiento chino de la firma Huawei. Este equipamiento, de reconocida calidad técnica y de altas prestaciones, soporta IPv6.

A continuación se muestra, en las Figuras 3.3 y 3.4, parte del equipamiento adquirido y sus características técnicas: [13]

a) Conmutador capa 3. (CX300B).

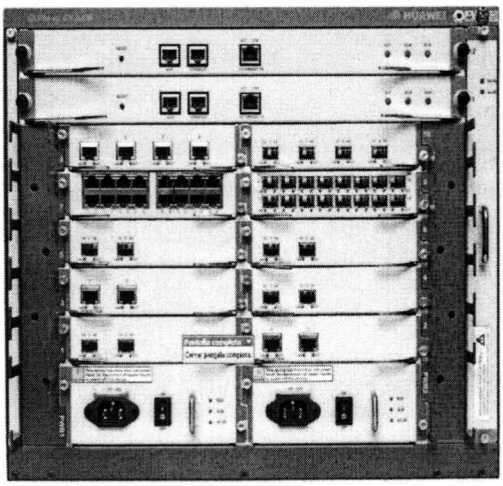

Fig. 3.3. Conmutador capa 3. (CX300B).

Características Técnicas

- Video bajo demanda-
- Televisión por IP.
- Redes de nueva generación.
- Calidad de Servicio.
- Seguridad.

b) Cortafuego o *Firewall* (Eudemon 1000).

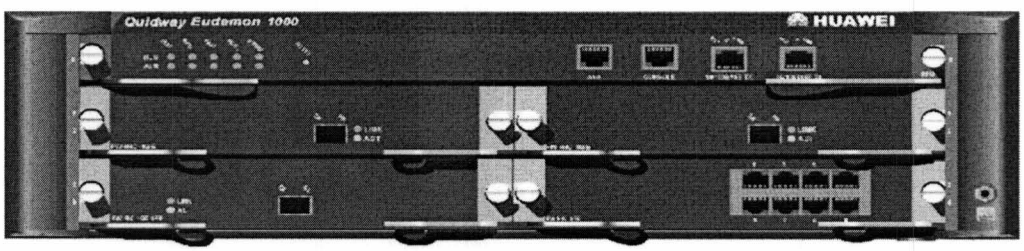

Fig. 3.4. Cortafuego o *Firewall* (Eudemon 1000).

Características Técnicas

- Filtrado de paquetes
- Calidad de Servicio (QoS)
- IPSec
- Defensa contra ataques
- Monitoreo y estadísticas de tráfico

El precio del equipamiento necesario para la implementación de IPv6 en el núcleo de la red se muestra en la tabla 3.4. [13]

No.	Área	Precio Total (USD)
1	NN1 Docente 4	182 339.00
2	NN1 Infraestructura Productiva	182 339.00
3	NN1 Nodo Central	157 915.00
4	NN1 Residencia 1	182 339.00
5	NN1 Residencia 2	157 915.00
6	Sistema de Administración (Software)	115 448.68
	Precio Total	**978 295.68**

Tabla 3.4. Precio total del equipamiento.

Adicionalmente, en la UCI se realizan acciones que permitirán optimizar las prestaciones de la red e implementar otros mecanismos de Calidad de Servicio. Por ejemplo, la actual topología es de estrella, por lo que no resultaría viable realizar ingeniería de tráfico, pues existe un solo camino posible entre los equipos de conectividad de la red y el nodo central.

En la gráfica 3.5 se muestra la futura topología de la red de la UCI. [10]

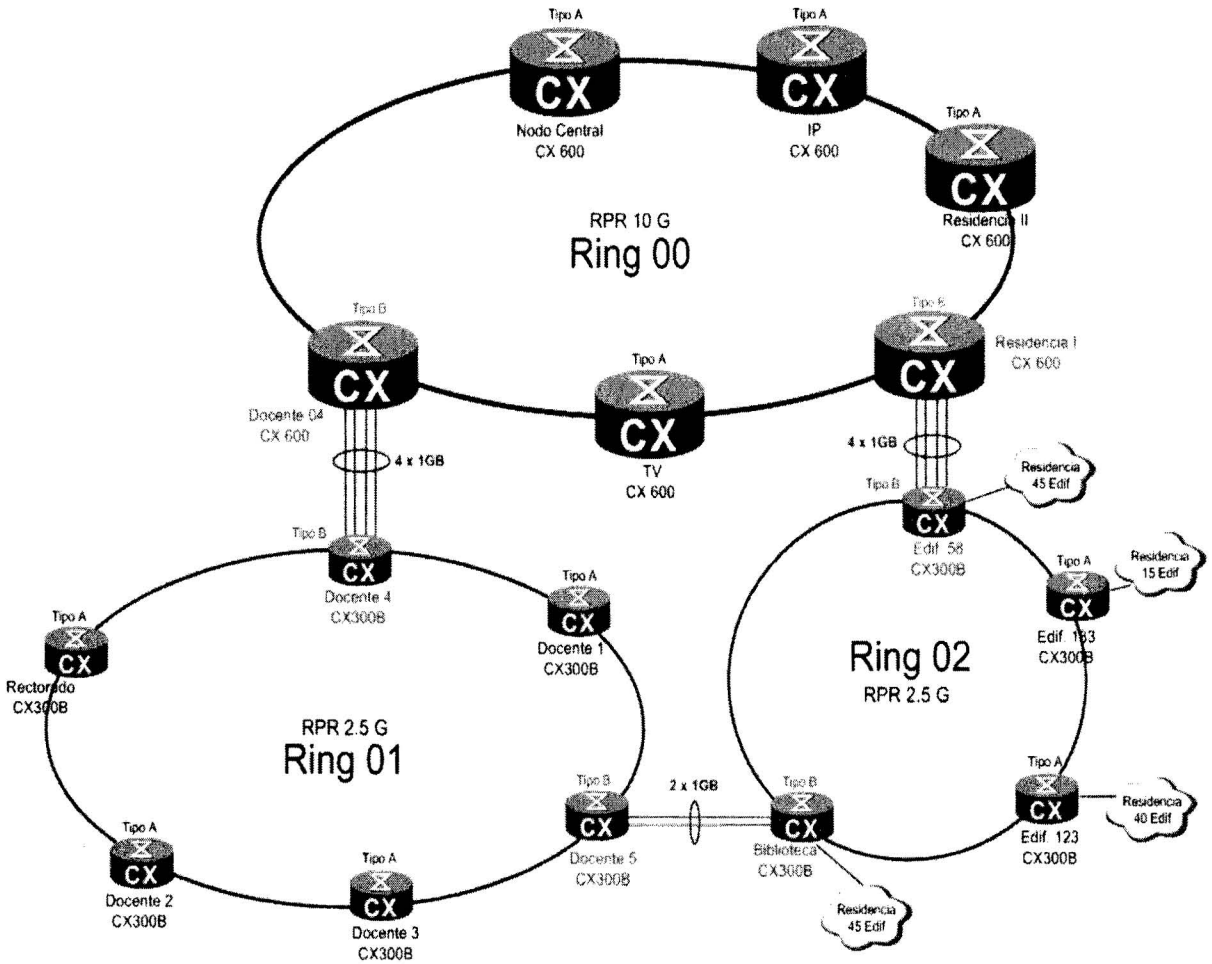

Fig. 3.5. Futura distribución de la red de la UCI.

3.3.1 Mecanismos de Transición. [3]

Existen varios mecanismos para la migración de una red hacia IPv6:

- Mecanismos de doble pila.
- Mecanismos de túneles IPv6 sobre IPv4.
- Redes IPv6 nativas

Mecanismos de doble pila.

Uno de los mecanismos que conceptualmente permite la introducción más sencilla de IPv6 es el uso de doble pila. Con este mecanismo un nodo está equipado con ambas pilas en su Sistema Operativo, y contiene direcciones IPv4 e IPv6. Este nodo es capaz de enviar y recibir paquetes de ambos protocolos para comunicarse con nodos que contengan cualquiera de las dos pilas implementadas. Este es el método más simple para la introducción de IPv6. Constituye el próximo paso en la evolución de Internet, hasta que IPv6 sea el único protocolo utilizado.

Mecanismos de Túneles IPv6 sobre IPv4.

Con estos mecanismos se logra encapsular paquetes IPv6 en paquetes IPv4. Estos paquetes son transmitirlos a través de una infraestructura IPv4 sin cambiar sus protocolos de enrutamiento ni sus enrutadores. Estos mecanismos se usan generalmente cuando un despliegue total de IPv6 no es posible en el momento, y se necesita conectar redes que ya implementan el nuevo protocolo. Los mecanismos de túneles o de encapsular un protocolo en otro, llevan un proceso de tres pasos: encapsular, desencapsular y manipulación de los túneles. Este mecanismo requiere dos puntos extremos, que generalmente son enrutadores de doble pila. Estos enrutadores se encargan de encapsular y desencapsular los paquetes. Todo este proceso lleva asociado una pérdida en el rendimiento de la red.

Redes IPv6 Nativas.

El mayor problema en la implementación de redes IPv6 nativas surge cuando estas redes desean comunicarse con algún nodo que solo implemente IPv4. El único método para hacer esto posible es mediante el uso de mecanismos de traducción. Estos mecanismos pueden ser implementados en la capa de red, la capa de transporte o la capa de aplicación. En la capa de red, las cabeceras de los paquetes son traducidos de una versión a otra, lo cual ocurre en el Sistema Operativo del nodo emisor. Para la implementación de traductores en la capa de transporte, generalmente se introducen terminales doble pila, que se encargan de traducir los paquetes y enviarlos entre ambas redes. En la capa de aplicación lo que se usa es una pasarela de la capa de aplicación

Mientras que las soluciones en la capa de red y transporte son prácticamente transparentes para la capa de aplicación, la solución en esta última necesita de pasarelas para cada aplicación o servicio que se desee implementar.

3.3.2 Mecanismos a utilizar.

Como resultado de la investigación realizada, se propone utilizar el mecanismo de doble pila, que es el más sencillo de implementar y el más utilizado en los procesos de migración.

Estas doble pilas se implementarían en todos los nodos que forman el *Backbone* de la red de la UCI (nodos NN1 y NN2).

La doble pila es una forma de integración y no necesita de mecanismos de migración o herramientas para su implementación. El único paso necesario para hacer que un nodo sea doble pila es activar IPv6 en su Sistema Operativo (SO). Actualmente la tendencia de los fabricantes de SO es activar IPv6 por defecto. Convertir una red o un nodo en doble pila no constituye un riesgo de seguridad en sí. En este caso solo se le está adicionando un protocolo completamente independiente, para el cual habrá que tomar las mismas medidas de seguridad que cuando solo se poseía la pila IPv4.Por ejemplo, si la red o la terminal se protegen con un cortafuego que contiene una serie de reglas para el tráfico IPv4, ahora se deben incluir reglas para IPv6. Si esto no es posible con el mismo cortafuego, se deberá adicionar otro cortafuego que se encargue del asunto.

CONCLUSIONES

Como resultado de esta investigación, se considera que es factible la transición hacia IPv6 en el núcleo de la red de la Universidad de las Ciencias Informáticas sin afectar el funcionamiento de la misma.

El uso de este protocolo permitirá incrementar los niveles de seguridad, implementar nuevos servicios y mejorar la calidad de los que hoy se brindan, todo lo cual redundará en la eficiencia y funcionalidad de la red.

Los resultados de este trabajo podrán servir de referencia a otras Universidades e instituciones que se propongan la integración de IPv6 en sus redes, contribuyendo de esta manera a la introducción de esa tecnología en el país.

RECOMENDACIONES

Se recomienda, para lograr una migración eficiente y exitosa, se consideren las necesidades de capacitación de los administradores y de todas aquellas personas que estén involucradas en el funcionamiento de la red de la UCI.

Además se propone que, una vez finalizada la implementación del protocolo IPv6 en el núcleo de la red de la Universidad, y teniendo en cuenta las experiencias adquiridas, se proceda a diseñar la implementación de este protocolo en la capa de acceso.

REFERENCIAS BIBLIOGRÁFICAS

1. **IETF.** IETF RFC Page. [En línea] [Citado el: 30 de Enero de 2008.] http://www.ietf.org/rfc.html.

2. Wikipedia, la enciclopedia libre. [En línea] [Citado el: 20 de Enero de 2008.] http://es.wikipedia.org.

3. **Alfredo Núñez, Joel.** *Inicio de la transición a IPv6 en la red nacional del Ministerio del Turismo.* Ciudad de La Habana : CUJAE, 2006.

4. **LACNIC.** LACNIC anuncia el inminente agotamiento de las direcciones IPv4. [En línea] 20 de Junio de 2007. [Citado el: 12 de Febrero de 2008.] http://www.lacnic.net/ipv6/sp.

5. **UNAM.** Proyecto IPv6 de la UNAM. [En línea] [Citado el: 20 de Enero de 2008.] http://www.cu.ipv6.unam.mx.

6. **Fernández, Azael y Morales, Olvera.** [En línea] 2001. [Citado el: 27 de Febrero de 2008.] http://www.cu.ipv6tf.org/casos/IPv6_UNAM.pdf.

7. **Jaque, Sandra.** Registro de direcciones de Internet para América Latina y el Caribe. [En línea] Agosto de 2005. [Citado el: 12 de Enero de 2008.] http://www.lacnic.net/ipv6tour/docs/c-lazo-aire6.pdf.

8. **Valdés Menéndez, Ramiro.** *Discurso en la Convención y Feria Internacional Informática 2007.* Ciudad de La Habana : s.n., 2007.

9. Sitio IPv6 Cuba. [En línea] [Citado el: 24 de Enero de 2008.] http://www.cu.ipv6tf.org/.

10. **Rodríguez Morales, Orestes.** *Evolución a IP.* Ciudad de La Habana : Universidad de Ciencias Informáticas, 2008.

11. **Núñez Oliva, Hedel.** *Televisión Digital. IPTV.* Ciudad de La Habana : Universidad de Ciencias Informáticas, 2008.

12. **Irañeta Duménigo, Ianabel y Romero González, Mario.** *Propuesta del Protocolo MPLS para la red de la Universidad de Ciencias Informáticas.* Ciudad de La Habana : s.n., 2007.

13. **Dirección de Gestión Tecnológica.** *Proyección Tecnológica de la infraestructura de la red de datos.* Ciudad de La Habana : Universidad de Ciencias Informáticas, 2008.

BIBLIOGRAFIA

Alfredo Núñez, Joel. *Inicio de la transición a IPv6 en la red nacional del Ministerio del Turismo.* Ciudad de La Habana : CUJAE, 2006.

Alvarez de Zayas, Carlos. *Metodología de la Investigación Científica.* Santiago de Cuba : s.n., 1995.

ARIN. American Registry for Internet Numbers. [En línea] [Citado el: 20 de Enero de 2008.] http://www.arin.net/media/ fact_sheets/Spanish/IPv4_IPv6_spanish.pdf.

Cumbre Mundial sobre la Sociedad de la Información. [En línea] [Citado el: 14 de Abril de 2008.] http://www.itu.int/wsis/index-es.html .

Dirección de Gestión Tecnológica. *Proyección Tecnológica de la infraestructura de la red de datos.* Ciudad de La Habana : Universidad de Ciencias Informáticas, 2008.

Domínguez, José. Sitio IPv6 Cuba. [En línea] 2004. [Citado el: 2 de Abril de 2008.] http://www.cu.ipv6tf.org/casos/deploying-ipv6.pdf .

Fernández, Azael y Morales, Olvera. [En línea] 2001. [Citado el: 27 de Febrero de 2008.] http://www.cu.ipv6tf.org/casos/IPv6_UNAM.pdf.

Fernández Cambronero, David. [En línea] [Citado el: 4 de Mayo de 2008.] http://internetng.dit.upm.es/ponencias-jing/2002/fernandez/Evolucion-IPv4-IPv6-David-Fernandez.PDF.

Fernández, David. Internet de Nueva Generación - Tendencias. [En línea] [Citado el: 4 de Mayo de 2008.] http://internetng.dit.upm.es/ponencias-jing/2002/fernandez/Evolucion-IPv4-IPv6-David-Fernandez.PDF.

Hernández Meléndrez, Edelsys. Infomed, Portal de Salud de Cuba. [En línea] 2006. [Citado el: 11 de Febrero de 2008.] http://www.sld.cu/galerias/pdf/sitios/rehabilitacion-bal/como_escribir_ tesis.pdf.

Hernández Sampier, Roberto. *Metodología de la Investigación I y II.* La Habana : Félix Varela, 2003.

IETF. IETF RFC page. [En línea] [Citado el: 20 de Enero de 2008.] http://www.ietf.org/rfc.html.

IPv6: Servicio de información y soporte. [En línea] [Citado el: 11 de Febrero de 2008.] http://www.6sos.net/documetos/glosario-IPv6-v1-2.pdf.

Irañeta Duménigo, Ianabel y Romero González, Mario. *Propuesta del Protocolo MPLS para la red de la Universidad de Ciencias Informáticas.* Ciudad de La Habana : s.n., 2007.

Jaque, Sandra. Registro de direcciones de Internet para América Latina y el Caribe. [En línea] Agosto de 2005. [Citado el: 12 de Enero de 2008.] http://www.lacnic.net/ipv6tour/docs/c-lazo-aire6.pdf.

LACNIC. LACNIC anuncia el inminente agotamiento de las direcciones IPv4. [En línea] 20 de Junio de 2007. [Citado el: 12 de Febrero de 2008.] http://www.lacnic.net/ipv6/sp.

Luengo, Miguel. Redes-Linux.com. [En línea] [Citado el: 12 de Enero de 2008.] http://beta.redes-linux.com/manuales/ipv6/ipv6-UNLP.PDF.

Narten, Thomas. NIC México - Direcciones IP. [En línea] [Citado el: 2 de Marzo de 2008.] http://www.nic.mx/es/IP.Politicas_IPv6.

Núñez Oliva, Hedel. *Televisión Digital. IPTV.* Ciudad de La Habana : Universidad de Ciencias Informáticas, 2008.

Oficina para la informatización. *Estado del arte de las TIC 2007.* La Habana : s.n., 2008.

Oficina para la Informatización. *Principales resultados de Informatización al cierre 2007. Resumen ejecutivo.* Ciudad de La Habana : s.n., 2008.

Oficina para la Informatización. *Uso de estándares informáticos abiertos como parte de la estrategia para alcanzar soberanía e independencia en las TIC.* La Habana : s.n., 2007.

Palet, Jordi. Redes-Linux.com. [En línea] 2000. [Citado el: 12 de Enero de 2008.] http://beta.redes-linux.com/manuales/ipv6/principiosipv6-1.txt.

Palet, Jordi. Sitio IPv6 Cuba. [En línea] [Citado el: 13 de Abril de 2008.] http://www.cu.ipv6tf.org/pdf/sacando_partido_a_ipv6_con_redes_ipv4_v5.pdf.

Palet Martínez, Jordi. Consulintel. [En línea] [Citado el: 20 de Enero de 2008.] http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf.

PCC. *Proyecto de Resolución Económica del Partido Comunista de Cuba.* La Habana : Editorial Política, 1997.

Protocolo de Internet versión 6. **Oficina para la Informatización.** 17, Ciudad de La Habana : s.n., 2006.

Rodríguez Morales, Orestes. *Evolución a IP.* Ciudad de La Habana : Universidad de Ciencias Informáticas, 2008.

Sitio IPv6 Cuba. [En línea] [Citado el: 24 de Enero de 2008.] http://www.cu.ipv6tf.org/.

Valdés Menéndez, Ramiro. *Discurso en la Convención y Feria Internacional Informática 2007.* Ciudad de La Habana : s.n., 2007.

Wikipedia, la enciclopedia libre. [En línea] [Citado el: 20 de Enero de 2008.] http://es.wikipedia.org/wiki/Ipv4.

Wikipedia, la enciclopedia libre. [En línea] [Citado el: 20 de Enero de 2008.] http://es.wikipedia.org/wiki/Ipv6.

Zakariah bin, Zamani. Sitio IPv6 Cuba. [En línea] 2004. [Citado el: 27 de Febrero de 2008.] http://www.cu.ipv6tf.org/casos/unpan017962.pdf.

GLOSARIO DE TÉRMINOS

ADSL: Subscritor Digital Asimétrico (*Asymmetric Digital Subscriber Line*). Tipo de tecnología que permite la transmisión de información digital a una rápida velocidad por medio de la línea telefónica.

Ancho de banda: Es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bits por segundo (bps), kilobits por segundo (Kbps), o megabits por segundo (Mbps).

ARP: Protocolo de Resolución de Direcciones (*Address Resolution Protocol*), es un protocolo de nivel de red responsable de encontrar la dirección hardware que corresponde a una determinada dirección IP. Para ello se envía un paquete a la dirección de multidifusión de la red que contiene la dirección IP por la que se pregunta, y se espera a que una máquina responda con la dirección que le corresponde.

Backbone: Es usado en redes como vía principal para transportar tráfico entre otros segmentos de redes. Constituye el núcleo de la red.

DHCP: Protocolo de Configuración Dinámica de Terminales (*Dynamic Host Configuration Protocol*), es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

DNS: El Sistema de Nombres de Dominio (*Domain Name System*), es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar diferentes tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio.

FTP: Protocolo de Transferencia de Ficheros (*File Transfer Protocol*), es un protocolo sofisticado que se ocupa de la transferencia de ficheros entre sistemas.

HDTV: Televisión de Alta Definición (*High Definition TV*), es uno de los formatos que, sumados a la Televisión Digital, se caracteriza por emitir las señales televisivas en una calidad digital superior a los sistemas ya existentes (PAL, NTSC y SECAM).

***Host* o terminal**: Aparato capaz de realizar operaciones de diálogo con un servidor. También se le llama cliente. Puede ser una computadora, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, impresora, entre otros.

ICMP: El Protocolo de Mensajes de Control de Internet (*Internet Control Message Protocol*), es el subprotocolo de control y notificación de errores del Protocolo de Internet. Se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un enrutador o terminal no puede ser localizado.

IETF: Grupo de Trabajo en Ingeniería de Internet (*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, tales como transporte, encaminamiento y seguridad.

IP: Internet Protocol, Protocolo de Internet, es un protocolo no orientado a conexión, usado tanto por el origen como por el destino para el intercambio de datos a través de una red de paquetes conmutados.

IPSec: Protocolo de Seguridad de Internet (*Internet Protocol Security*), protocolo que brinda seguridad de transmisión de información sensible a través de redes públicas.

IS-IS: Sistema intermedio a sistema intermedio. Protocolo de enrutamiento jerárquico de estado de enlace OSI, en el cual los enrutadores intercambian información de enrutamiento en base a una métrica única para determinar la topología de la red.

Modelo OSI: Modelo de referencia de Interconexión de Sistemas Abiertos (*Open System Interconnection*), es el modelo de red descriptivo creado por ISO; esto es, un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones. Este modelo está dividido en siete capas: (Físico, Enlace, Red, Transporte, Sesión, Presentación y Aplicación)

Moodle: Es un sistema de gestión de cursos de libre distribución que ayuda a los educadores a crear comunidades de aprendizaje en línea.

MPLS: Intercambio de Etiquetas Multiprotocolo (*Multiprotocol Label Switching*), es un mecanismo de transporte de datos que opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

MRU: Unidad Máxima de Recepción (*Maximun Receive Unit*), indica el tamaño máximo (en octetos) del campo de datos de una trama (en el nivel de enlace) que una determinada terminal es capaz de recibir en una red. En la mayoría de los casos es un parámetro que coincide con la MTU por lo que, al igual que ésta, acaba siendo dependiente de la red física.

MTU: La Unidad Máxima de Transferencia (*Maximum Transfer Unit*), es el tamaño en bytes del datagrama más grande que puede pasar por una capa de un protocolo de comunicaciones.

NAT: Traducción de Dirección de Red (*Network Address Translator*), es un mecanismo utilizado por enrutadores IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo. Su uso más común es permitir utilizar direcciones privadas y aún así proveer conectividad con el resto de Internet.

ND Protocol: Conjunto de mensajes y procesos ICMPv6 que determinan las relaciones entre nuevos 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.

OSPF: (*Open Shortest Path First*), es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (*Interior Gateway Protocol*), que usa el algoritmo enlace-estado para calcular la ruta más corta posible. Usa *cost* (costo) como su medida de métrica. Además, construye una base de datos enlace-estado idéntica en todos los enrutadores de la zona.

PDU: Unidades de Datos de Protocolo (*Protocol Data Units*), se utiliza para el intercambio entre unidades parejas, dentro una capa del modelo OSI.

QoS: Calidad de servicio (*Quality Of Service*), medida de desempeño para un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

RFC: Petición de Comentarios (*Request For Comments*), 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.

RIP: Protocolo de Enrutamiento de Información (*Routing Internet Protocol*), es un protocolo de vector de distancia perteneciente a la arquitectura TCP/IP, que busca la ruta mas corta entre dos puntos en una red a partir del análisis de las direcciones origen y destino.

Router: Enrutador, encaminador. Dispositivo de hardware para interconexión de redes de las computadoras que opera en la capa tres (nivel de red) del modelo OSI.

RSVP: Protocolo de Reserva de Recursos (*Resource Reservation Protocol*), es un protocolo de nivel de red en la estructura de capas de Internet y OSI, que permite reservar los canales o rutas en redes Internet para la transmisión por unidifusión y multidifusión.

SDTV: Definición Estándar de Televisión (*Standard Definition TV*), son las señales de televisión que no se pueden considerar señales de alta definición (HDTV) ni de señales de televisión de definición mejorada.

SMS: Servicio de mensajes cortos (*Short Message Service*), es un servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos (también conocidos como mensajes de texto) entre teléfonos móviles, teléfonos fijos y otros dispositivos de mano.

Streaming: Término que se refiere a ver u oír un archivo directamente en una página Web sin necesidad de descargarlo antes a la computadoras. Describe una estrategia sobre demanda para la distribución de contenido multimedia a través de Internet.

TCP: Protocolo de Control de Transmisión (*Transmission Control Protocol*), es uno de los protocolos fundamentales en Internet. Utilizado dentro de una red de datos compuesta por computadoras para crear conexiones entre ellos a través de las cuales enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron.

También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través de los puertos.

UIT: Unión Internacional de Telecomunicaciones, es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras.

VoIP: Voz sobre IP o telefonía IP, es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP. Esto significa que se envía la señal de voz en forma digital en paquetes en lugar de enviarla (en forma digital o analógica) a través de circuitos utilizables sólo para telefonía como una compañía telefónica convencional.