UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

EVOLUCIÓN DE REDES FIJAS DEL PROTOCOLO IPv4 A IPv6 EN GUATEMALA

ROBERTO ALEJANDRO SANTIZO GARCÍA

ASESORADO POR EL ING. MANUEL FERNANDO LÓPEZ FERNÁNDEZ

GUATEMALA, SEPTIEMBRE DE 2003

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

EVOLUCIÓN DE REDES FIJAS DEL PROTOCOLO IPv4 A IPv6 EN GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA FACULTAD DE INGENIERÍA

POR

ROBERTO ALEJANDRO SANTIZO GARCÍA
ASESORADO POR: ING. MANUEL FERNANDO LÓPEZ FERNÁNDEZ

AL CONFERÍRSELE EL TÍTULO DE
INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, SEPTIEMBRE DE 2003

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Sydney Alexander Samuels Milson
VOCAL I	Ing. Murphy Olympo Paiz Recinos
VOCAL II	Lic. Amahán Sánchez Álvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Keneth Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Ing. Ricardo Alfredo Girón Solórzano
EXAMINADOR	Ing. Edgar Estuardo Santos Sutuj
EXAMINADOR	Ing. César Augusto Fernández Cáceres
SECRETARIA	Ing. Pedro Antonio Aguilar Polanco

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado

EVOLUCION DE REDES FIJAS DEL PROTOCOLO IPv4 A IPv6 EN GUATEMALA

Tema que me fuera asignado por la Coordinación de la Carrera de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería con fecha 11 de febrero de 2003.

Roberto Alejandro Santizo García

DEDICATORIA

A DIOS TODOPODEROSO, por haberme dado la fe y la fortaleza para continuar en los momentos difíciles de mi carrera.

A MIS PADRES VICTOR MANUEL SANTIZO ALÍA Y ZONIA LETICIA GARCÍA TORRE, por darme la vida y guiarme a través de ella, por su apoyo incondicional y comprensión que me brindaron en todo momento a lo largo de mi carrera.

A MI ABUELITA ADA MERCEDES TORRE MONTERO, por sus consejos y cariño brindado.

A MIS HERMANOS ANDREA MARISOL, ANA LUISA, ANDRÉS ESTUARDO, por su comprensión y apoyo en todo momento.

A MIS TÍOS, PRIMOS Y FAMILIA EN GENERAL, por sus consejos y cariño.

A MIS AMIGOS Y COMPAÑEROS DE ESTUDIO, en especial a Christian Barneónd, Erick López, Carlos Villatoro, Rene Monroy, Rene Alvarado, Roberto Arreaga, Edward Ayau, Arnulfo Hernández, Ronald Morales, Ricardo Morales.

A LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA, por la formación académica recibida.

AGRADECIMIENTOS

Al Ingeniero Manuel López Fernández, por la desinteresada colaboración para la realización del presente trabajo de graduación.

A la escuela de Ingeniería en Ciencias y Sistemas de la Universidad de San Carlos de Guatemala por darme la oportunidad de brindar mis conocimientos a otros estudiantes.

A todos mis catedráticos por el tiempo y dedicación que invirtieron en mi formación.

Al colegio Salesiano Don Bosco, por sus principios y conocimiento dados hacia mi persona.

ÍNDICE GENERAL

4. MIGRACIÓN DE REDES EXISTENTES EN GUATEMALA

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

3G	Redes móviles de tercera generación
AND	Operación lógica para el control de bits
DHCPv6	Protocolo de configuración dinámica de nodo en su versión 6
IP	Protocolo de Internet
IPv4	Protocolo IP en su versión 4
IPv6	Protocolo IP en su versión 6
UDP	Protocolo de datagramas de usuario
VoIP	Voz sobre IP

TCP	Protocolo de control de transporte

GLOSARIO

Autoconfiguración	Proceso por el cual un nodo obtiene las direcciones IPv6 para sus interfaces.
Backbone	Infraestructura que constituye la base de la Internet. Nivel más alto en la jerarquía de ISPs que brindan conexión a Internet.
BIND	Implementación del servicio DNS para los sistemas operativos de UNIX.
BOOTP	Protocolo de arranque que utilizan las estaciones de trabajo sin disco para solicitar una dirección IP y otros parámetros.
Descencapsular	Proceso por el cual se remueve una cabecera que fue agregada previamente a un paquete.
Descubrimiento de vecindad	Mecanismos que utilizan los nodos tanto para publicar su presencia a otros nodos como para determinar los parámetros de ubicación de nodos.
Dirección privada	Dirección utilizada por un nodo para la comunicación interna dentro de la red.

Dirección pública	Dirección única asignada por InterNIC utilizada para comunicarse a través de Internet.
Dispositivo móvil	Dispositivo no conectado a una red de computadoras que puede ser utilizado para conectarse a Internet.
DNS	Conjunto de servicios para resolver los nombres de nodos y sus direcciones IP.
Encapsular	Proceso por el cual se agrega una cabecera extra a la que contiene un paquete.
Enlace	Es el medio por el cual se transporta información en formato IPv6.
Infraestructura	Denominación para la versión del protocolo IP utilizado por una o más redes de computadoras.
Interfaz	Conexión con un medio de transmisión por la que se envían los paquetes IPv6.
IPsec	Familia de protocolos y servicios que se utilizan para proporcionar seguridad adicional a los datagramas de IP.
ISP	Compañía que provee acceso a Internet a otras compañías.

Multihomming	Mecanismo encargado de la replicación de conectividad a Internet.
Nodo	Dispositivo con capacidad de procesamiento y es comúnmente denominado computadora.
Nodo IPv4	Nodo que solamente utiliza el protocolo IPv4 para la comunicación.
Nodo IPv6	Nodo que solamente utiliza el protocolo IPv4 para la comunicación.
Nodo IPv6/IPv4	Nodo que puede utilizar tanto el protocolo IPv4 como el IPv6 para la comunicación.
Paquete	Unidad de transmisión de la capa de red del modelo OSI.
Qos	Conjunto de estándares para asegurar la calidad en la transmisión de datos. También es denominado calidad de servicio.
RARP	Protocolo por el cual se obtiene una dirección IP de la dirección del nivel de interfaz de red.
Registro A	Registro utilizado por un servidor de DNS para almacenar una dirección IPv4 de un nodo.

Registro AAAA	Registro utilizado por un servidor de DNS para almacenar una dirección IPv6 de un nodo.
Resolución	Proceso que realiza un servidor de DNS a petición de un nodo para conocer datos como la dirección IP, nombre, etc de otro nodo.
RFC	Documento formal o estándar, desarrollado por una persona, el IEFT o un grupo de trabajo del IETF que define parte de los protocolos de Internet.
Router	Dispositivo encargado de reenviar paquetes que no están dirigidos a él.
***Router* IPv6/IPv4**	*Router* con capacidad de reenviar tanto paquetes en formato IPv4 como en IPv6.
Ruteo	Proceso de recibir y reenviar paquetes a un destinatario por la ruta mas eficiente de un conjunto de rutas.
Tabla de mapeo	Componente utilizado para mantener el vinculo de una dirección IPv4 con una IPv6.
Tabla de ruteo	Información útil que se utiliza en el ruteo para determinar la ruta de un destinatario.
Túnel	Conexión lógica sobre la cual viaja la información encapsulada.

VPN	Red privada virtual que conecta una red o, a través de una red intermedia, normalmente Internet.

RESUMEN

Los 32 bits con que cuenta una dirección IP en su cuarta versión no permite asignar a cada uno de los usuarios actuales que desean conectarse a Internet una dirección propia para lograr dicho objetivo. Aunque actualmente aún existen direcciones IP sin asignar y mecanismos como NAT las utilizan para cubrir el problema de escasez de direcciones, dichos mecanismos dejarán de ser funcionales cuando todas estas direcciones hayan sido asignadas.

El protocolo IP en su sexta versión permite resolver este problema de escasez de direcciones y proporcionar un número prácticamente infinito de direcciones IP. Además proporciona una serie de beneficios e incorpora la serie de modificaciones que se le han hecho a la cuarta versión para alargar su tiempo de vida.

Debido a la utilización de la Internet en las tareas diarias de cada persona o compañía, la adopción de la nueva versión no se realizará de un día a otro. Más bien dicha transición se realizará de manera progresiva por lo que existirá un entorno mixto de redes formando Internet.

Para lograr dicha transición se han creado una serie de mecanismos que puede adoptar una organización que le permitirán realizar cambios progresivos y no radicales en sus redes, lo cual también le permitirá seguir utilizando sus inversiones hechas tanto en *software* como en *hardware*.

Para las empresas guatemaltecas tanto los ISPs, como las empresas que utilizan a dichos ISP se muestran las soluciones que deben adoptar en el corto, mediano y largo plazo para la adopción del nuevo protocolo. Además se describe el alto grado de adopción del protocolo que se ha hecho en Latinoamérica en relación a Guatemala.

OBJETIVOS

- General

Mostrar los diferentes mecanismos de transición que existen actualmente que puede adoptar una organización guatemalteca que posee una red con infraestructura IPv4 y desea comunicarse con redes que poseen infraestructura IPv6.

- Específicos

1. Mostrar los beneficios que ofrece el protocolo IPv6 sobre el IPv4
2. Mostrar el estado actual del acceso a Internet a través de redes IPv4
3. Mostrar el probable acceso a Internet a través de una red con infraestructura que soporta IPv6
4. Mostrar ejemplos de escenarios de transición que puede adoptar una organización guatemalteca
5. Mostrar los componentes que se deben tomar en cuenta para realizar la transición hacia el protocolo IPv6

6. Mostrar el grado de desarrollo hasta el 2002 del protocolo IPv6 en Latinoamérica en relación del resto del mundo

INTRODUCCIÓN

El número de usuarios que utilizan Internet ha crecido exponencialmente y el número de direcciones IP que aún no han sido asignadas es cada vez menor. Los mecanismos utilizados actualmente para cubrir el problema de escasez de direcciones pronto dejarán de ser funcionales. Agregado a ello, la meta de lograr conectividad a Internet a través de dispositivos distintos de una computadora no es posible realizarla con el protocolo IP en la versión cuatro. Esto se logrará si se cuenta con un protocolo que garantice una cantidad infinita de direcciones.

Por tales razones, el estudio del protocolo IP en su versión seis y su adopción por parte de las organizaciones merece especial atención, ya que permitirá conocer cuales son los componentes involucrados en la transición, la forma de proceder en la transición y su coexistencia con el protocolo en su cuarta versión para la obtención de los beneficios brindados por ambos protocolos.

Al conocer la forma de proceder y los diferentes mecanismos de transición, el objetivo del presente trabajo de graduación consiste en brindar las soluciones que pueden adoptar las empresas guatemaltecas en el corto, mediano y largo plazo para permitir la coexistencia de ambos protocolos, y así, poder obtener la mayor cantidad de beneficios de ambos protocolos.

1. CONCEPTOS DE IPv6

1.1 Conexión a Internet en la actualidad

El protocolo actual de Internet IPv4 lleva cerca de 20 años funcionando, desde que el 1ro de enero de 1983 se convirtió en el protocolo oficial de la ARPANET (actualmente Internet). En sus orígenes dicho protocolo fue creado principalmente pesando en la comunicación entre entidades de investigación y organizaciones militares. Los creadores de IPv4 no predijeron en ningún momento el gran impacto que este iba a tener en diferentes campos distintos de los educativos y científicos y por lo tanto, ignoraban el crecimiento que este tendría.

Dicho crecimiento desde mediados de la década de los 80 hasta la fecha ha presentado una forma exponencial, con lo cual el protocolo IPv4 presenta ya limitaciones con respecto de los requerimientos de las tecnologías de información actual.

Una de dichas limitaciones que presenta el protocolo IPv4 es la incapacidad de brindarle a cada usuario de cada parte del planeta que desee comunicarse en Internet una dirección pública en dicha red. Esta incapacidad se debe al formato de las direcciones IPv4. La cantidad de bits que posee una dirección IPv4 es de 32, con lo cual la cantidad máxima de direcciones

disponibles es de 4,294,967,296 lo cual es mucho menor del número de usuarios que actualmente requieren una dirección para acceder a Internet.

Por esta razón, se tiene el problema de la escasez de direcciones IPv4 ya que el número de usuarios que desean conectarse a Internet crece exponencialmente y el número de direcciones disponibles sigue igual. Dichas direcciones públicas son asignadas por la *Internet Network Information Center* (*InterNIC*). Por lo tanto, para comunicarse en Internet, un usuario debe usar una dirección IP valida, esto es, que haya sido asignada por la *InterNIC*.

La asignación de direcciones IP publicas, se realiza a proveedores de servicios de Internet (ISP's). Un proveedor de servicios de Internet es una compañía que provee a usuarios individuales u otra compañía acceso a Internet. A cada ISP se le asigna un rango de direcciones públicas. Así cada a cada compañía o empresa que desee conectarse a Internet, el *ISP* le asigna una dirección pública de este rango.

Para el caso de las compañías, estas manejan direcciones privadas dentro de sus redes locales, las cuales son diferentes de las direcciones públicas de Internet. Con dichas direcciones privadas, ningún usuario podrá lograr conectividad a Internet. Por lo tanto para solucionar el problema de escasez de direcciones IPv4 y lograr que todos los usuarios puedan lograr conectividad hacia Internet, ya sea que estos formen parte o no de una red local, se han creado temporalmente mecanismos que solucionen este problema crítico de IPv4.

Uno de los métodos mas comunes es el llamado *Network Address Translator (NAT).* Este NAT es un *router* que es colocado entre la red local que usa direcciones privadas e Internet. El trabajo de *NAT* es traducir direcciones privadas a direcciones públicas y viceversa.

De esta forma los paquetes que salen de la red local tienen su dirección privada que es traducida por *NAT* a una dirección pública y los paquetes que entran desde Internet tienen una su dirección pública que es traducida por *NAT* a una dirección privada. *NAT* rompe el modelo original de conexión entre extremos. Originalmente la red ARPANET fue diseñada para funcionar como *end-to-end* (E2E), es decir, a través de este modelo se permitía la conexión directa entre dos computadores sin intervención de ningún mecanismo.

1.2 Historia del IPv6

Debido al interés publico por la Internet que comenzó a mediados de la década de los 90 y observando el crecimiento exponencial de usuarios en Internet y los avances acelerados en las tecnologías de información, el IEFT (*Internet Engineering Task Force*) empezó a trabajar en 1990 en una nueva versión del IP, la cual sería denominada IP N*ext Generation.* Esta nueva versión nunca tendría problemas de escasez de direcciones, resolvería varios otros problemas y además sería mas flexible y eficiente. Los requerimientos a cumplir por el próximo protocolo eran:

- Manejar miles de millones de estaciones o *hosts*.

- Reducir las tablas de ruteo.

- Simplificación de la cabecera, para permitir el procesamiento más rápido de los paquetes.

- Proporcionar mayor seguridad en los datos que el IPv4.

- Prestar mayor atención al tipo de servicio, especialmente con datos en tiempo real.

- Ayudar al *multicast*, en la cual se pueda especificar alcances.

- Posibilitar que una estación sea móvil sin necesidad de cambiar su dirección.

- Permitir que el protocolo evolucione.

- Permitir que el IPv4 pueda coexistir con el nuevo protocolo.

La IETF hizo una convocatoria solicitando propuestas y estudios. Se recibieron 21 respuestas, dentro de las cuales, no fueron todas completas. En 1992, una propuesta denominada TUBA fue implementar mecanismos para emplear TCP y UDP sobre direcciones más grandes, eliminando con ello las direcciones IPv4 de 32 bits. Estas direcciones mas grandes eran gracias a ISO CLNP (*Connection-Less Network Protocol*), el cual, con sus 160 bits habría proporcionado suficiente espacio de direcciones para siempre. Sin embargo, se pensó que esto habría sido una aceptación de que algunas cosas en el mundo OSI en realidad estaban bien hechas, algo considerado políticamente incorrecto en los círculos de Internet. El CLNP se creó tomando como modelo al IP, por lo que los dos no son realmente tan diferentes. Otra consideración era el pobre

manejo de tipos de servicio de CLNP, algo requerido para transmitir multimedia eficientemente, así que fue descartado.

En 1993, surge un nuevo proyecto denominado SIPP (*Simple Internet Protocol Plus*), el cual es una mezcla de dos tentativas anteriores, las cuales fueron creadas en ese mismo año, por sustituir IPv4. Dichos proyectos eran SIP y PIP, cuyos creadores fueron Deering y Francis respectivamente. Una característica de este nuevo proyecto es que en el se utilizarían direcciones de 64 bits.

Finalmente, en julio de 1994, tras muchos análisis, revisiones e intrigas, el IPng *Area* elige el proyecto SIPP como una implementación adecuada para el nuevo protocolo IP, variando el tamaño de las direcciones de SIPP de 64 a 128 bits. Este nuevo protocolo cambia su nombre como originalmente había sido establecido de IP *Next Generation* (IPng) a IPv6 para no causar confusión con IPng *Area*.

1.3 Motivaciones para cambiar a IPv6

1.3.1 Motivaciones Tecnológicas

Escasez de direcciones web IPv4. Debido al formato de las direcciones IPv4, las cuales constan de 32 bits, el número de direcciones IPv4 de aproximadamente 4 mil 300 millones (2^{32} = 4,294, 967,296), establece un límite

para el número de nodos de Internet, y sumado a que este número desde finales de los 80 ha crecido exponencialmente, supone el agotamiento de las direcciones IPv4. Esta falta de direcciones disponibles limita el crecimiento de Internet, obstaculiza el uso de Internet a nuevos usuarios, y obliga que los usuarios usen métodos de traducción de direcciones llamados NAT, en los cuales deben usar una sola IP pública para toda una red privada, y por lo tanto, evitan la conectividad directa entre nodos que están tras el traductor.

IPv6 resuelve este problema, ya que aporta direcciones prácticamente infinitas de 128 bits, aproximadamente 10^{38} lo cual es más que el número de estrellas en el universo (10^{20}).

Crecimiento de las tablas de enrutamiento. Debido al aumento en forma exponencial del número de prefijos que los *routers* de los *backbones* deben mantener en sus tablas de ruteo, provoca una saturación en dichos *routers.*

Con ello, se puede llegar a alcanzar los límites físicos impuestos por la capacidad de memoria y de proceso. Dicho hecho llevó a la creación de un método llamado CIDR (*Classless Inter-Domain Routing*) que consiste en la agregación de prefijos que son adyacentes para dar lugar a prefijos menores, con lo que se reduce el número de entradas en las tablas de los *routers*. Tanto CIDR como las políticas restrictivas de asignación de direcciones son sólo medidas temporales, que no resuelven los problemas crónicos detectados en Internet.

IPv6 a través de su direccionamiento jerárquico (TLA, NLA), permite a los *routers* el procesamiento más rápido de los paquetes, debido a que estos solo se deben observar una pequeña parte de las direcciones para tomar una decisión de ruteo. Con dicho direccionamiento jerárquico se obtienen menos espacios en las tablas de ruteo y algoritmos de ruteo más simples. Además se obtiene una configuración automática de los *routers* más viable, gracias a dicho direccionamiento.

Tecnologías que necesitan direcciones permanentes para conectarse a Internet. Dispositivos móviles como teléfonos celulares, agendas personales, y otros dispositivos electrónicos, necesitan usar una dirección IP en cada punto de conexión nuevo a Internet, y con IPv4 no siempre es posible obtenerla. Debido a que no hay suficientes direcciones públicas IPv4 disponibles para todos los dispositivos móviles conectados a Internet, el Proyecto de Asociación para la 3G (3GPP/3G *Partnership Project*) ha especificado IPv6 como el protocolo IP obligatorio en la prestación de servicios multimedia en redes de telefonía móvil.

Crecimiento de aplicaciones que requieren direcciones IP públicas, únicas, globales, válidas para conexiones extremo a extremo y por lo tanto enrutables: videoconferencias, voz sobre IP (VoIP), seguridad.

Futuros sistemas con dirección IP. En el futuro, dispositivos como refrigeradoras, televisores, electrodomésticos en el hogar, parquímetros, automóviles y cualquier otra máquina que pretenda intercambiar información a

través de Internet, necesitará una dirección IP pública para conectarse a Internet.

El protocolo IPv4, es simplemente incapaz de soportar el impacto en el crecimiento del número de dispositivos electrónicos a Internet, pues no cuenta con la estructura física de datos para proveer todas las direcciones requeridas.

Necesidad de incluir en el protocolo IP los sucesivos “parches” que se le han ido añadiendo de forma adicional a lo largo de su historia. Debido a la multitud de nuevas aplicaciones en las que ha sido utilizado el protocolo IPv4, se han ido agregando funcionalidades adicionales al protocolo básico. Entre los parches más conocidos se encuentran: Calidad de servicio (QoS), Seguridad (IPsec), movilidad (Mobile IP) y *Multihomming*. En el protocolo IPv4, IPsec es una funcionalidad optativa y por lo tanto todos los nodos no tienen porque implementarla, lo cual implica un limitación en el crecimiento de IPsec. En IPv6 es obligatorio que todos los nodos tengan soporte para IPsec, por lo cual es posible mantener una conexión segura a nivel de IP. En IPv4 se tienen procedimientos complejos de marcado para la calidad de servicio ya sean agregados (*Intserv*) o bien de flujos (*Diffserv*) . IPv6 facilita esta tarea mediante la inclusión del campo TC (*Traffic Class*) en las cabeceras.

En el protocolo IPv4, *Mobile* IP es optativo, al contrario de IPv6. Para garantizar la conectividad a las organizaciones en todo momento, se han creado los servicios *multihomming*, los cuales son mecanismos de replicación de la conectividad.

Obtención de un protocolo IP que sea más flexible y que reduzca complejidad y costos. A través de IPv6 la configuración de redes será más ágil y simple a través de aspectos como la autoconfiguración.

1.3.2 Motivaciones políticas

Lucha por el predominio mundial en Internet entre USA y Europa. La falta de direcciones no afecta por igual a todos los puntos de la red mundial Internet. Actualmente en USA y Canadá poseen cerca del 55% de las direcciones IPv4 existentes. Sin embargo en zonas geográficas como Asia y Europa el problema es creciente. Del total de los 4 mil millones de direcciones, Europa solo tiene asignado 80 millones, para una población de más de 300 millones actualmente. En Asia, por ejemplo, China, solo le han correspondido 9 millones de direcciones, para una población con más de mil millones de ciudadanos. Al lado contrario, en Norte América, por ejemplo, esta la Universidad de *Stanford*, la cual tiene asignados más de 17 millones de direcciones.

A continuación se muestran los datos del número de usuarios y de direcciones IPv4 por región que se espera alcanzar en los próximos años:

Tabla I. Núm. estimado de usuarios contra núm. de direcciones IPv4 disponibles

Región	Número estimado de Usuarios en el 2010	Direcciones IPv4 disponibles

Continuación

África	800,000,000	3,000,000
Norte América	500,000,000	125,000,000
América Central y Sudamérica	500,000,000	10,000,000
Europa Occidental	250,000,000	50,000,000
Asia	2500,000,000	50,000,000

En esta tabla se muestra la justificación mas clara de la necesidad de pasar a IPv6. Incluso en Norte América donde existe el número mas grande de direcciones IPv4 disponibles también se ve reflejado dicha necesidad, ya que la relación de direcciones IPv4 a usuarios es de 1:4, y por lo tanto no existe una dirección IPv4 propia para cada usuario de Norte América. En Centro América y Sudamérica la relación es de 1:50, lo que hace mas cuestionable la vigencia del protocolo IPv4.

1.3.3 Motivaciones económicas

Extensión del mercado hacia los productos de tecnología celular. En los últimos años los nuevos servicios demandados por los usuarios consisten en una conexión a Internet por medio de dispositivos móviles. Este hecho implica que dichos dispositivos estén conectados ininterrumpidamente y por lo tanto necesiten, al menos, una dirección IP pública. Además, supone una revolución tanto desde el punto de vista económico, ya que para las organizaciones se abren muchas posibilidades a explotar, como desde el punto de vista tecnológico debido a la participación de dispositivos móviles en Internet cada

uno con su dirección propia para acceder a Internet, hecho que no se puede conseguir con el protocolo IPv4.

Intención de muchos países de implantar Internet a un porcentaje mayoritario de la población, con el fin de acelerar el proceso de crecimiento económico.

1.4 Beneficios de IPv6

IPv6 ofrece una serie de beneficios que se pueden obtener de resumir las razones por las que se debe cambiar hacia IPv6. Dichos beneficios se muestran a continuación:

Espacio de direcciones. A través de los 128 bits que conforman las direcciones IPv6, es posible obtener un número infinito de direcciones disponibles para cualquier usuario que desee conectarse a Internet. Esto permite a las nuevas tecnologías como la tecnología celular UMTS, la cual exige emplear un gran número de direcciones IP que no cambien si el usuario cambia de ubicación, así como otras tecnologías que permitan acceder a Internet desde cualquier dispositivo electrónico poder crecer y ponerse en práctica.

Seguridad. IPv6 hace uso de IPsec, por lo cual es posible mantener una conexión segura a nivel de IP y proporcionar una verificación de autenticidad y

confidencialidad. En IPv6 es obligatorio que todos los nodos tengan soporte para IPsec.

Móvil. Capacidad de habilitar para que un nodo sea móvil sin cambiar su dirección, esto es, permitirle comunicación desde cualquier punto donde este acceda a la red. Se ha especificado IPv6 como el protocolo IP obligatorio en la prestación de servicios en redes de telefonía móvil.

Direccionamiento jerárquico. A través del direccionamiento jerárquico, se tiene una reducción de las tablas de ruteo de los *backbones* de Internet. En IPv6 las direcciones se van agregando en niveles superiores (TLAs, NLAs), lo cual evita que dichas tablas crezcan indefinidamente.

Cabecera IPv6 simplificada. A través de la simplificación del protocolo, permite a los *routers* el procesamiento más rápido de los paquetes.

1.5 Características de IPv6

El protocolo IPv6 presenta una serie de características básicas:

- Espacio de direcciones prácticamente infinito, a través de sus 128 bits, permite un total de 2^{128} direcciones disponibles, o sea, 2^{96} (2^{128-32}) veces el número de direcciones de IPv4.

- Arquitectura jerárquica de direcciones. Debido a esto se obtiene un ruteo más eficiente en el *backbone* de Internet ya que se reducen las tablas de ruteo.

- Autoconfiguración de direcciones. Se refiere al conjunto de pasos por los cuales un host decide como autoconfigurar sus interfaces IPv6.

- Movilidad. A través de IPv6 se facilita todo el proceso de movilidad, como la detección de movimientos, autenticación de mensajes, etc

- Seguridad e integridad de datos. IPv6 provee extensiones para soportar autenticación, integridad y confidencialidad en los datos. El soporte de seguridad no es obligatorio en IPv4, en IPv6 sí lo es.

- Calidad de servicio (QoS). En IPv6 se introduce la capacidad de control de flujo, lo que permite marcar los paquetes que pertenezcan a un determinado tipo de tráfico, con lo cual se permite manejar QoS y la administración de ancho de banda sin necesidad de analizar cabeceras de TCP ni de UDP.

- Paquetes IP eficientes y extensibles. A través de la simplificación de la cabecera, algunos campos de la cabecera de los paquetes del IPv4 son eliminados o pasan a ser opcionales, tanto para reducir el costo de procesamiento como el tamaño de la cabecera. La eficiencia de ruteo se logra a través de cabeceras de extensión, las cuales son cabeceras separadas que, no son examinadas en ningún *host* en la ruta desde el origen hasta el destino. Debido a que en IPv6 no existe un campo opciones, la gestión de opciones se realiza a través de esta cabecera de

extensión, con lo cual se elimina así las limitaciones del tamaño de la cabecera y permite la flexibilidad en el desarrollo de nuevas opciones.

- *Multicast*. Se refiere al envío de un mismo paquete a un grupo de receptores. Al contrario que en IPv4, donde el soporte de *multicast* se añadió a posteriori y no es obligatorio, en IPv6 sí es obligatorio.

- *Anycast*. Envío de un paquete a un receptor dentro de un grupo.

- Renumeración y *multi-homming*. A través de esta característica se facilita el cambio de un proveedor de servicios.

- Posibilidad de paquetes con carga útil de más de 65,535 bytes.

- Soporte a tráfico multimedia en tiempo real.

- Recupera el modelo original *end-to-end* (E2E) perdido por IPv4. IPv6 erradica el problema de uso de NAT.

Se debe tomar en cuenta que estas son las características básicas del protocolo IPv6, ya que la propia estructura del protocolo permite que este crezca, gracias a su característica de escalabilidad, según las nuevas necesidades y aplicaciones o servicios lo requieran. Por lo demás, IPv6 mantiene la filosofía de IPv4 en cuanto a que ofrece un servicio de datos basado en datagramas no fiable, no orientado a conexión, etc.

1.6 Comparación entre IPv4 e IPv6

Tabla II. Direcciones IPv6 vs. direcciones IPv6

IPv6	IPv4
Direcciones de 128 bits (16 bytes)	Direcciones de 32 bits (4 bytes)
Arquitectura jerárquica	Arquitectura plana
Configuración automática	Configuración manual
Multicast y anycast	Broadcast
Seguridad obligatoria	Seguridad opcional
Identificación de clase de servicio	Sin identificación de clase de servicio

En esta tabla comparativa se puede observar la gran ventaja de usar el protocolo IPv6 en lugar del protocolo IPv4. Se puede observar que la escasez de direcciones que genera el protocolo IPv4 es solucionada con IPv6 a través de sus direcciones de 16 *bytes*. A través de IPv6 se genera un espacio de direcciones prácticamente infinito.

El tiempo de procesamiento de los paquetes dentro de los *routers* es resuelto con la arquitectura jerárquica del protocolo IPv6, con esto se resuelve el problema generado por el protocolo IPv4 que consiste en el crecimiento exponencial de las tablas de ruteo dentro de los *routers* debido a su arquitectura plana, la cual genera un retardo en el proceso dentro del *router* para encontrar la ruta destino del paquete especifico.

En el protocolo IPv6, se evita la configuración manual de los dispositivos antes de su conexión a la red, mediante mecanismos de autoconfiguración de direcciones, como el sin estado, mientras que en el protocolo IPv4 la configuración debe realizarse manualmente.

En IPv6 no hay direcciones *broadcast*. IPv6 codifica un alcance, estableciendo el dominio de alcance de un paquete *multicast*, algo que no es posible con el protocolo IPv4.

En IPv6 la seguridad es un aspecto obligatorio y no adicional como en IPv4. En IPv6 se tienen una total integración de los mecanismos de seguridad, autenticación y confidencialidad, dentro del núcleo del protocolo.

En IPv6 se introduce un mecanismo poderoso de control de flujo, asignación de prioridades diferenciadas según los tipos de servicios. En IPv4 dicha identificación de clase de servicio no es obligatoria.

1.7 Tipos de direcciones IPv6

Las direcciones IPv6 se clasifican en tres tipos:

Unicast. Identifica a solo una interfaz. Un paquete se envía a una dirección *unicast* que es entregado solo a la interfaz identificada con dicha dirección.

Multicast. Identifica a un conjunto de interfaces, que por lo general son pertenecientes a diferentes nodos. Un paquete enviado a una dirección multi*cast* es entregado a todas las interfaces identificadas con dicha dirección.

Anycast. Identifica a un conjunto de interfaces, que por lo general son pertenecientes a diferentes nodos. Un paquete enviado a una dirección *anycast* es entregado a una de las interfaces identificadas con dicha dirección, la cual debe ser la más cercana al origen, de acuerdo a las medidas de distancia del protocolo de ruteo.

1.8 Características de las direcciones IPv6

- Las direcciones IPv6 son identificadores de 128 bits para interfaces y conjunto de interfaces, no para los nodos, ya que, las direcciones IPv6 independientemente de su tipo son asignadas a interfaces, y no precisamente a los nodos.

- Una interfaz puede tener asignadas muchas direcciones de cualquier tipo.

- Las direcciones IPv6 tienen ámbito de acción, el cual puede ser de enlace local, de sitio local y global.

1.9 Autoconfiguración en IPv6

La autoconfiguración se refiere al conjunto de pasos por los cuales un host decide como autoconfigurar sus interfaces en IPv6.

El proceso incluye la creación de una dirección de enlace local, verificación de que no se encuentra duplicada en dicho enlace y determinación de la información que ha de ser configurada.

Las direcciones pueden obtenerse de forma totalmente manual, mediante DHCPv6, o de forma automática (sin estado).

La autoconfiguración sin estado no requiere ninguna configuración manual del host, configuración mínima de routers y no necesita servidores adicionales como podría ser un servidor de DHCP. Este método permite generar a un host su propia dirección mediante una combinación de información localmente disponible e información anunciada por *routers*. Los routers anuncian los prefijos que identifican a la subred, mientras el host genera un identificador de interfaz, que identifica de manera única la interfaz en la subred. La dirección se compone de la combinación de ambos campos. En ausencia de un *router*, el host solo puede generar la dirección de enlace local, lo cual es suficiente para permitir la comunicación de los nodos conectados en el mismo enlace.

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

El mecanismo de autoconfiguración sin estado, se emplea cuando no importa la dirección exacta que se asigna a un host, sino tan solo asegurarse que es única y correctamente enrutable.

El mecanismo de autoconfiguración mediante DHCPv6, asegura que cada *host* tienen una dirección asignada manualmente.

Cada dirección es dada a una interfaz durante un tiempo predefinido. Las direcciones tienen asociado un tiempo de vida, que indican durante cuanto tiempo se encuentra vinculada dicha dirección a una determinada interfaz. Cuando dicho tiempo termina, la vinculación se invalida y la dirección puede ser asignada a otra interfaz en cualquier punto de Internet.

Para manipular la expiración de vínculos, una dirección pasa a través de dos fases diferentes mientras se encuentre asignada a una interfaz. Inicialmente una dirección es *preferred*, lo que indica que su uso es arbitrario y no se encuentra restringido. Posteriormente, la dirección se encuentra en estado de *deprecated*, lo que indica que su vínculo actual con la interfaz será anulado.

Mientras una dirección se encuentra en estado de *deprecated*, su uso no es aconsejable, aunque no es prohibido. Cualquier nueva comunicación debe usar una dirección *preferred*, siempre que sea posible. Una dirección *deprecated*, debería ser utilizada solo por las aplicaciones que ya la estaban utilizando y que les es muy difícil cambiar a una nueva dirección sin provocar una interrupción de servicio.

Para asegurar que todas las direcciones configuradas son únicas, en un determinado enlace, los nodos ejecutan un algoritmo de detección de direcciones duplicadas, antes de asignarlas a una interfaz. Dicho algoritmo es ejecutado para todas las direcciones, independientemente si han sido obtenidas mediante autoconfiguración sin estado o mediante DHCPv6.

La autoconfiguración está diseñada para *hosts*, no para *routers*, lo cual no implica que parte de la configuración de los routers también pueda ser realizada automáticamente. Además lo *routers*, también deben de realizar el algoritmo de detección de direcciones duplicadas.

1.9.1 Autoconfiguración sin estado

Los pasos para la autoconfiguración, cuando la interfaz del nodo ha sido activada son los siguientes:

1. Generación de la posible dirección de enlace local.

2. Verificación de que dicha dirección no esta duplicada en el mismo enlace.

3. Si la dirección esta duplicada, se detiene la autoconfiguración y se requiere un procedimiento manual.

4. Si la dirección no esta duplicada, la conectividad a nivel IP se ha logrado, al asignarse definitivamente dicha posible dirección a la interfaz.

5. Si es un *host*, se interroga a los posibles *routers* para indicar al *host* lo que debe hacer a continuación.

6. Si no hay *routers*, se invoca el procedimiento de autoconfiguración mediante DHCPv6.

7. Si hay *routers*, estos contestarán indicando, como obtener las direcciones si se ha de utilizar el mecanismo mediante DHCPv6 u otra información.

1.9.2 Autoconfiguración mediante DHCPv6

El protocolo DHCPv6 es un protocolo UDP cliente/servidor, diseñado para reducir el costo del manejo de nodos IPv6 en ambientes donde los administradores requieren un control sobre la asignación de recursos de la red, superior al brindado por el mecanismo de autoconfiguración sin estado.

Para lograr este control, se centraliza el manejo de los recursos de la red como direcciones IP, información de ruteo, información de servicios de directorios sobre uno o varios servidores DHCP, en lugar de distribuir dicha información en archivos de configuración locales de cada nodo.

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

Los cambios fundamentales entre DHCPv4 y DHCPv6, están basados en el soporte inherente del formato de direccionamiento y autoconfiguración IPv6, ellos son:

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

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

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

- La autoconfiguración mediante DHCPv6 ha de coexistir e integrarse con la autoconfiguración sin estado, soportando la detección de direcciones

duplicadas y los dos tiempos de vida de IPv6, para facilitar la renumeración automática de direcciones y su manejo.

- Se soportan múltiples direcciones por cada interfaz.

- Algunas opciones del DCHPv4 ya no son precisas, debido a que los parámetros de configuración se obtienen a través de ND o del protocolo de localización de servicios.

Al utilizar estos cambios, las nuevas funciones que presta el protocolo DHCPv6 son:

- Configuración de actualizaciones dinámicas de DNS.

- Desaprobación de direcciones, para renumeración dinámica.

- Autenticación.

- Los clientes pueden pedir múltiples direcciones IP.

- Las direcciones pueden ser reclamadas mediante el mensaje “iniciar-reconfiguración”.

- Integración entre autoconfiguración de direcciones sin estado y mediante DHCPv6.

- Permitir relés para localizar servidores fuera de alcance.

- Relés preconfigurados, con direcciones de servidores, mediante *multicast*.

1.10 Representación de direcciones IPv6

A diferencia de IPv4 que utiliza una notación decimal con puntos (.) para representar las direcciones IP, IPv6 utiliza por defecto una notación hexadecimal con dos puntos (:) para representar textualmente las direcciones IP, y en otros casos también parte de dichas direcciones IP pueden ser representadas utilizando una notación decimal con puntos (.). Las 3 notaciones comunes de representar textualmente direcciones IPv6 son:

- La representación textual por defecto, en la cual, las direcciones son ocho secciones con notación hexadecimal de 16 bits, separadas por dos puntos (:), es decir, direcciones de la forma: x:x:x:x:x:x:x:x, en donde cada "x" representa una sección en formato hexadecimal. Por ejemplo, una dirección IPv6 para una interfaz podría ser:
  3ffe:3328:41:3:250:4ff:fe5c:b3f4.

- La representación textual eliminando secciones contiguas de ceros, en la cual una o mas secciones que posean valores de 0, pueden ser omitidas utilizando el sustituto "::". Es una abreviatura que sirve para hacer más cómodo el uso de algunas direcciones. Este sustituto es posible utilizarlo para representar más de una sección contigua con bits a cero, pero no se puede utilizar más de una vez en una dirección. Por ejemplo, la dirección 3234:328:0:0:0:7f8:fb8c:d2f4, se podría representar así:

3234:328::7f8:fb8c:d2f4, pero la dirección 3234:0:0:45:23:0:0:d2f4, no se podría representar así: 3234::45:23::d2f4 ya que se utiliza el sustituto dos veces y sólo es posible utilizarlo una vez, y se utilizaría en el caso que sea conveniente.

- La representación textual para direcciones compatibles con IPv4, en la cual las direcciones en las seis secciones de mayor orden (las de la izquierda) de la dirección, utilizan notación hexadecimal separadas por dos puntos (:) y el resto utiliza notación decimal con puntos (.), es decir, direcciones de la forma: x:x:x:x:x:d.d.d.d, en donde cada "x" representa una sección de 16 bits en formato hexadecimal, y cada representa "d" representa una sección de 8 bits en formato decimal. Esta forma es a veces más conveniente cuando se deben manejar entornos mixtos IPv6 e IPv4. Por ejemplo, una dirección podría aparecer así: 0:0:0:0:0:FFFF:192.168.0.1 y en su forma abreviada sería ::FFFF:192.168.0.1.

1.10.1 Representación de los prefijos de direcciones IPv6

La representación de los prefijos de direcciones IPv6 es parecida a la que se tiene en CIDR con IPv4, es decir, de la forma, dirección-IPv6/tamaño-prefijo, donde dirección-IPv6 representa alguna de las 3 notaciones descritas en la sección 1.9 y tamaño-prefijo es un valor decimal que representa la cantidad de bits de mayor orden (los de la izquierda) de la dirección que corresponden con el prefijo. Por ejemplo, en la dirección: 3ffe:3328:0041:0:0:0:fe5c:b3f4/48, en la cual al eliminar los ceros es: 3ffe:3328:41::fe5c:b3f4/48, se muestra que la dirección-IPv6 es: 3ffe:3328:41::fe5c:b3f4 y tamaño-prefijo es: 48. En dicha

dirección los 48 bits de mayor orden corresponden a: 3ffe:3328:41, por lo tanto el prefijo de dicha es: 3ffe:3328:41.

1.10.2 Representación de los tipos de direcciones IPv6

Cada tipo de dirección IPv6 (*unicast*, *anycast*, *multicast*) se identifica por los bits de mayor orden (los de la izquierda) de cada dirección, dentro del campo denominado prefijo de formato (FP, *format prefix*). El tamaño de dicho campo es variable. Por ejemplo, un valor de 11111111 para el campo FP identifica a una dirección, como una dirección *multicast*. Las direcciones unicast se identifican por el valor del octeto de mayor orden, el cual debe ser distinto de 1. Las direcciones *anycast* se asignan dentro del espacio de las unicast y no son identificables entre si observando sus bits. La asignación de los prefijos se muestra a continuación:

Tabla III. Prefijos asignados a direcciones IPv6

Asignación	Prefijo
Reservado	0000 0000
Reservado para asignación NSAP	0000 001
Reservado para asignación IPX	0000 010
Direcciones Unicast Globales Agregables	001
Direcciones Unicast Enlace Local	1111 1110 10
Direcciones Unicast Sitio Local	1111 1111 11
Direcciones Multicast	1111 1111

1.10.2.1 Direcciones *unicast*

Una dirección unicast específica que un paquete se debe enviar a una interfaz concreta. Las direcciones *unicast* se refieren a una única interfaz de un nodo de un enlace; sin embargo una dirección unicast puede estar asignada a múltiples interfaces de dicho nodo, siempre que dichas interfaces aparezcan a los protocolos de nivel superior como una única entidad. Existen varios tipos de direcciones unicast en IPv6, entre ellas las globales agregables, local al sitio, de enlace local, IPX jerárquicas, la NSAP, y las compatibles con IPv4.

1.10.2.1.1 Direcciones *unicast* reservadas

Actualmente, se tienen dos direcciones *unicast* reservadas utilizadas para usos especiales, las cuales son: la dirección no especifica, y la dirección de retorno (*loopback address)*.

1.10.2.1.1.1 La dirección no específica

Con este nombre se le denomina a la dirección 0:0:0:0:0:0:0:0, o en forma abreviada "::". Esta dirección nunca puede ser asignada a ningún nodo, ni se puede utilizar como dirección de origen en paquetes de IPv6 ni en las cabeceras de los *routers*. Solo se permite su uso en escasos casos, como en el campo dirección origen de un paquete IPv6 cuando una interfaz no conoce todavía su propia dirección IP.

1.10.2.1.1.2 La dirección de retorno

Con este nombre se le denomina a la dirección 0:0:0:0:0:0:0:1, o en forma abreviada "::1". Se le conoce como dirección de retorno (*loopback address*) y su equivalente en IPv4 es 127.0.0.1. Con esta dirección no se debe enviar un paquete IPv6 tanto como dirección de origen como de destino sobre un medio físico. Esta dirección la utiliza un nodo para enviarse paquetes a sí mismo, y por lo tanto, dicha dirección no se puede asignar a interfaces reales, sino solo a interfaces virtuales, aquellas en la que los paquetes que no salen del nodo que los envía, como es el caso de la interfaz de *loopback*.

1.10.2.1.2 Direcciones *unicast* globales agregables

En la actualidad se emplea este tipo este tipo de direcciones, basadas en la agregación por parte de los proveedores del troncal de Internet. Además se incorpora un mecanismo de agregación basado en intercambios. La combinación de ambos es lo que permite un enrutamiento mas eficiente, para dar dos opciones de conectividad a unas u otras entidades de agregación.

Una dirección agregable se organiza en una estructura jerárquica de 3 niveles, los cuales son:

- Topología pública
- Topología del sitio

- Identificador de interfaz

El nivel de topología pública, es el nivel superior de la jerarquía, y se refiere a un espacio de direcciones que es administrado por un conjunto de proveedores e intercambiadores que proporcionan servicios públicos de tránsito de Internet. Este conjunto de proveedores e intercambiadores es el encargado de proporcionar el enrutamiento que exista fuera de la red interna de la organización.

El nivel de topología del sitio, se refiere a redes de organizaciones que no proporcionan servicios públicos de tránsito a nodos fuera de su propio sitio, es decir, es la parte de la dirección que se utiliza para el enrutamiento interno de la organización. La renumeración y *multi-homming* brindados por el protocolo IPv6, es decir, el cambio de un proveedor y la facilidad de que una organización posea varios proveedores de topología pública, son manejados fácilmente por este nivel de topología de sitio, ya que por ejemplo, si una organización decide cambiar de proveedor de topología pública, dicha organización no necesitará una reasignación del nivel de topología del sitio, y esta quedará igual y solo cambiará el nivel de topología pública. Si una organización utiliza varios proveedores, lo hará a través de un intercambiador, sin necesidad de tener prefijos de cada uno de los proveedores. En IPv4 el nivel de topología de sitio sería análogo al ID de red de la dirección.

El nivel de identificador de interfaz, se refiere a la parte que identifica las interfaces reales individuales de los enlaces físicos de la organización. En IPv4

el nivel de identificador de interfaz sería análogo al ID de *host* de la dirección. El formato de las direcciones *unicast* globales agregables es el siguiente:

Figura 1. Formato de direcciones *unicast* globales agregables

FP	TLA ID	RES	NLA ID	SLA ID	ID de la interfaz
001	13 bits	8 bits	24 bits	16 bits	64 bits

Cada uno de los campos se muestra a continuación:

Tabla IV. Campos de una dirección *unicast* global agregable

Campo	Tamaño
FP (*Format Prefix*) Prefijo del formato	3 bits
TLA ID (*Top Level Aggregation*) ID de agregación de nivel superior	13 bits
Res (*Reserved*) Reservado	8 bits
NLA ID (*Next Level Aggregation*) ID de agregación del siguiente nivel	24 bits
SLA ID (*Site Level Aggregation*) ID de agregación del nivel del sitio	16 bits
ID de la interfaz	64 bits

El campo prefijo del formato con valor 001 específica que es una dirección unicast global agregable.

El campo ID de agregación de nivel superior (TLA), se trata del nivel superior de la estructura jerárquica de enrutamiento. Los *routers* que se encuentran situados en este nivel, tienen en su tabla de ruteo una entrada para cada TLA y probablemente entradas adicionales al propio TLA donde se encuentren físicamente situados. Con esta estructura de direccionamiento se permite 8,192 identificadores de TLA.

El campo reservado consiste en bits reservados para la expansión de los campos TLA y NLA, para necesidades futuras.

El campo ID de agregación del siguiente nivel (NLA), es utilizado por organizaciones que tienen asignado un TLA, y desean tener una estructura interna jerárquica de direccionamiento, dentro de su propia red, y para organizar e identificar los sitios u organizaciones que de ellas dependen. Debido a que una organización con un TLA, tiene disponibles 24 bits en este campo, puede proporcionar servicio aproximadamente al numero de direcciones IPv4 direccionables actualmente, lo cual se denomina estructura plana. Además las organizaciones que tienen asignado un TLA pueden soportar varios NLA en su espacio de direccionamiento, lo cual permite que den servicio tanto a clientes directos, como a organizaciones que prestan servicios públicos de transito, lo cual se denomina estructura de varios niveles.

El campo ID de agregación del nivel del sitio (SLA), es utilizado por organizaciones para crear su propia estructura interna jerárquica de direcciones e identificar subredes, para realizar el enrutamiento interno independiente del

que se realiza externamente a ellas. Posee el mismo concepto en IPv4 de subredes pero se diferencia en que se puede dar soporte a unas 65,535 subredes internas a través de los 16 bits de este campo. Al igual que el campo NLA, se puede tener una estructura plana de direccionamiento o una estructura de varios niveles

El campo ID de la interfaz, se refiere a las interfaces de los nodos, los cuales deben ser únicos en el enlace físico donde se encuentren. Frecuentemente, este campo suele suceder con la dirección del nivel del enlace, y este podría estar asignado a varias interfaces del mismo nodo para poder realizar un balance de carga por varias interfaces.

1.10.2.1.3 Direcciones *unicast* locales

Las direcciones unicast locales se utilizan para la comunicación en el mismo enlace. Se han definido dos tipos de direcciones unicast de uso local: de enlace local (l*ink-local*), local al sitio (s*ite-local*).

1.10.2.1.3.1 Dirección *unicast* de enlace local

Estas direcciones se han creado para su utilización en un ámbito de enlace local, en donde no existen *routers* para el reenvío de paquetes, o para otros propósitos como el descubrimiento de vecindad, método que utiliza un nodo para encontrar otros nodos dentro de un enlace, y la autoconfiguración de

una dirección, método por el que un nodo consigue su dirección IPv6. El formato de las direcciones unicast de enlace local se muestra en la figura 5.

Figura 2. Formato de una dirección *unicast* de enlace local

10 bits	54 bits	64 bits
1111111010	0	ID de la interfaz

Los *routers* no pueden retransmitir ningún paquete, con una dirección de este tipo, en el campo dirección origen o destino, debido al ámbito de estas direcciones. En forma abreviada una dirección de enlace local seria: FE80::<ID de interfaz> /64.

1.10.2.1.3.2 Dirección *unicast* local al sitio

Estas direcciones también se han creado para su utilización en un ámbito de sitio local, sin la necesidad de un prefijo global. Son equivalentes a las direcciones privadas de IPv4 que se utilizan para el direccionamiento y comunicación dentro de una organización privada.

Se configuran mediante un identificador de subred de 16 bits. Al igual que las direcciones de enlace local, los *routers* no pueden retransmitir fuera del sitio de la organización ningún paquete con una dirección de este tipo, en el campo dirección origen o destino, debido al ámbito que esta limitado a la red

local o de la organización. El formato de las direcciones unicast locales al sitio es el siguiente:

Figura 3. Formato de una dirección *unicast* al sitio

10 bits	38 bits	16 bits	64 bits
1111111011	0	ID de subred	ID de la interfaz

En forma abreviada una dirección de sitio local seria: FEC0:: <ID de subred>:<ID de interfaz> /10.

1.10.2.1.4 Direcciones IPv6 con direcciones IPv4 incluidas

Dentro de los mecanismos de transición de IPv4 a IPv6, existe un mecanismo que permite a *hosts* y a *routers* crear túneles dinámicamente para el envío transparente de paquetes IPv6 sobre una infraestructura IPv4 existente. Para la realización de ello, se han definido dos tipos de direcciones IPv6 que incluyen direcciones IPv4, las cuales son: direcciones IPv6 compatibles con IPv4 y las direcciones IPv6 mapeadas desde IPv4.

1.10.2.1.4.1 Direcciones IPv6 compatibles con IPv4

Los nodos que utilicen el mecanismo de creación de túneles para el envío transparente de paquetes recibirán una dirección *unicast* especial IPv6 en donde los bits de menor orden (los de la derecha) serán la dirección IPv4. El formato de las direcciones IPv6 compatibles con IPv4 es el siguiente:

Figura 4. Formato de una dirección IPv6 compatible con IPv4

80 bits	16 bits	32 bits
000000000.... 000000000	0000	Dirección IPv4

En forma abreviada una dirección IPv6 compatible con IPv4 seria: :: <Dirección IPv4>.

1.10.2.1.4.2 Direcciones IPv6 mapeadas desde IPv4

Dentro del mecanismo de transición, estas direcciones serán utilizadas por nodos que solo disponen de una pila IPv4, es decir, no utilizan IPv6. Al igual que las direcciones IPv6 compatibles con IPv4 los bits de menor orden (los de la derecha) serán la dirección IPv4, pero la dirección IPv4 esta precedida con FFFF y no con 0000. El formato de las direcciones IPv6 mapeadas desde IPv4 es el siguiente:

Figura 5. Formato de una dirección IPv6 mapeada desde IPv4

80 bits	16 bits	32 bits
000000000.... 000000000	FFFF	Dirección IPv4

En forma abreviada una dirección IPv6 mapeada desde IPv4 seria: :: FFFF:<Dirección IPv4>.

1.10.2.1 Direcciones *anycast*

Una dirección *anycast* específica que un paquete se puede enviar a distintas interfaces de uno o varios nodos, pero dicho paquete es entregado a una y solo una de las interfaces identificadas con dicha dirección, la cual debe ser la más cercana al origen, de acuerdo a las medidas de distancia del protocolo de ruteo.

Estructuralmente las direcciones *anycast* no se pueden distinguir de las direcciones *unicast*, por lo tanto, las interfaces (generalmente los routers del sitio) que tienen asignada una dirección de *anycast* se le debe decir expresamente, es decir, deben ser explícitamente configuradas para que reconozcan que se trata de una dirección *anycast*.

Al momento que un nodo desea enviar un paquete a una dirección *anycast* que fue previamente asignada a un conjunto de nodos o interfaces, se utiliza un mecanismo de descubrimiento del nodo o interfaz mas cercano, por lo tanto, para el nodo origen es independiente si se trata o no de una dirección de destino *anycast;* y la comunicación que después sucede sólo ocurre entre el nodo origen y el nodo destino. Si se asignara por ejemplo, una dirección *anycast* a los routers del sitio, la comunicación ocurriría entre el nodo origen y el *router* más cercano.

Existe una dirección *anycast* necesaria para cada *subred*, denominada "dirección *anycast* del *router* de la *subred*", por lo tanto, todos los *routers* deben soportar dicha dirección para las subredes a las que están conectados, y al momento de un nodo enviar un paquete a dicha dirección, el paquete será enviado a un *router* de la *subred*.

Actualmente, las direcciones *anycast* tienen una serie de restricciones, las cuales son:

- No se puede enviar ningún paquete de IPv6 que posea una dirección de origen que sea de tipo *anycast*.

- Una dirección *anycast* solo puede ser asignada a los routers, pero no a los hosts.

- Los routers deben soportar la “dirección *anycast* del *router* de la subred”, para asegurar que un *router* local recibirá el paquete enviado a una dirección *anycast* de dicha subred.

1.10.2.3 Direcciones *multicast*

Una dirección *multicast* identifica a un grupo de nodos o interfaces, y tiene la particularidad que un nodo puede pertenecer a varios grupos *multicast*. Estas direcciones se utilizan para el tráfico de IPv6, y sustituyen a las direcciones de *broadcast* en IPv4. Cuando un paquete se envía a una dirección *multicast,* es entregado a todas las interfaces configuradas con dicha dirección *multicast*, caso contrario si fuera una dirección *anycast* en la que solo se entregaría a un nodo o interfaz.

Las direcciones *multicast* tienen una serie de restricciones, las cuales son:

- No se puede enviar ningún paquete de IPv6 que posea una dirección de origen que sea de tipo *multicast*.

- No se puede usar una dirección *multicast* en las cabeceras de enrutamiento.

El formato de las direcciones *multicast* es el siguiente:

Figura 6. Formato de una dirección *multicast*

8 bits	4 bits	4 bits	112 bits
11111111	000T	ámbito	Id de grupo

El campo prefijo del formato con valor 11111111 especifica que es una dirección de *multicast*.

En el campo indicadores actualmente los 3 primeros bits están fijados a cero, y reservados para futuras actualizaciones. Si el valor del *bit* "T" es 0, se trata de una dirección *multicast* permanente, asignada por la autoridad de numeración global de Internet (IANA), en caso contrario, es decir, si el valor es 1, se trata de una dirección *multicast* temporal.

El campo ámbito establece un límite de acción de los grupos de *multicast*, es decir, limita el ámbito de dichos grupos. Los valores para dicho campo, son:

Tabla V. Valores para el campo ámbito de una dirección *multicast*

0	Reservado
1	Ámbito local de nodo
2	Ámbito local de enlace
5	Ámbito local de sitio
8	Ámbito local de organización

Continuación

E	Ámbito global
F	Reservado
Resto Valores	No asignado

El campo identificador de grupo, identifica el grupo de *multicast* que aceptará paquetes enviados a esta dirección.

1.11 Equipos potenciales para Internet

Hasta hace unos años se pensó que el acceso a Internet podría ser únicamente a través de una computadora. Actualmente el acceso a Internet esta limitado a computadoras personales, computadoras portátiles y en los últimos años se ha evolucionado a teléfonos celulares, agendas electrónicas y televisores. En la actualidad la meta principal consiste brindar conexión a Internet sin necesidad de una computadora. Con esto se busca poder brindar conexión a cualquier dispositivo creado por el hombre. Se dice que la verdadera masificación de Internet se producirá cuando se consiga esta meta.

Con la meta anterior existe una gran cantidad de dispositivos potenciales que se pueden utilizar para acceder a Internet sin necesidad de una computadora. Entre los dispositivos potenciales se pueden mencionar los siguientes:

- Teléfonos celulares
- Agendas electrónicas
- Dispositivos del hogar (lavadoras y secadoras de ropa, estufas, refrigeradoras, hornos microondas, radios, televisores, teléfonos)
- Dispositivos industriales (alarmas contra robos de casas, autos, etc)
- Dispositivos musicales (mp3 *player*, pianos, etc)
- Medios de transporte (carros, motos, bicicletas, etc)
- Dispositivos para juegos (juegos de videos, etc)

Un usuario con un horno microondas conectado a Internet podría bajar recetas y el dispositivo podría conocer los tiempos exactos de cocción del alimento y brindarle al usuario una Interfaz gráfica en donde se mostrará dicho tiempo.

Una refrigeradora conectada a Internet podría enviar una orden automática de hacia un supermercado, cuando por ejemplo, este por quedarse sin reservas de alimentos.

A través de una televisión conectada a Internet un usuario podría ver su programa favorito y a la vez consultar su cuenta de correo. Un automóvil conectado a Internet podría conocer la ruta exacta para llegar a un lugar determinado, el tiempo de llegada, etc.

Para lograr la meta, es necesario disponer de suficientes direcciones IP y no hacer que los dispositivos se encuentren conectados obligatoriamente a una red. Con el protocolo IPv4 no es posible brindar una conexión a Internet permanente, ya que la cantidad de direcciones IPv4 públicas son muy limitadas. IPv6 es un protocolo que brinda un número de direcciones ilimitadas para todos los dispositivos que desean conectarse a Internet. Con IPv6 cada persona del mundo puede disponer de su propia dirección IP. Por lo tanto, para poder brindar una conexión a todos los dispositivos potenciales de Internet es necesario hacer uso del protocolo IPv6.

1.12 Próxima generación de acceso a Internet

Actualmente existen varios medios de transmisión que se utilizan en una red para lograr una conexión a Internet. Existen medios como los cables trenzados, cables coaxiales y fibra óptica. Un medio de comunicación inalámbrico puede ser el microondas.

En la actualidad ya se posee de un sistema de transmisión a través de la luz. Este sistema puede ser utilizado para la conexión a Internet. Con un medio de transmisión como la luz eléctrica la velocidad de conexión podría aumentar

considerablemente. Para la utilización de los diferentes equipos potenciales para la conexión a Internet dentro de una casa, oficina podría ser un buen medio comunicación y no basarse en un medio de transmisión como lo sería cualquier tipo de cableado. Además un medio como el cableado puede ser complicado para su mantenimiento.

1.13 El hogar y el acceso a Internet con tecnología IPv6

Actualmente el acceso a Internet dentro de un hogar se hace a través de una computadora que posee un *modem* y se conecta con un proveedor de Internet que utiliza un mecanismo como lo es NAT. Dicha conexión se hace a través de una línea telefónica. Con un protocolo como lo es el IPv4 no es posible brindar conexión a todos los dispositivos potenciales de Internet y por lo tanto la meta de lograr conexión sin la utilización de una computadora no es posible cumplirla.

Para la utilización de los equipos potenciales para Internet dentro del hogar el protocolo IPv6 es el ideal. Dicha conexión se podría lograr con un *router* con soporte para IPv6 y formar dentro del hogar una de red. Gracias a la gran cantidad de direcciones disponibles con el protocolo IPv6, se podría asignar una dirección IPv6 a cada hogar y conectar los dispositivos a dicho al *router* con soporte para IPV6.

2. TRANSICIÓN AL IPv6

La transición total de Internet de IPv4 a IPv6 de un momento a otro es imposible debido al tamaño de Internet y al gran número de usuarios que actualmente utilizan IPv4. Además muchas organizaciones son cada día más dependientes en sus actividades diarias de Internet, y por lo tanto, un tiempo determinado para realizar la transición total de Internet hacia IPv6 es impensable.

Sin embargo, no existe ningún problema en que la transición no se realice de un momento a otro, ya que los dos protocolos (IPv4 e IPv6) pueden coexistir sin ningún problema. Mas bien se ha pensado que dicha transición debe realizarse de forma progresiva y eficiente, en donde en la fase inicial los nodos tengan soporte para ambos protocolos al mismo tiempo, para luego con el paso del tiempo, tener una infraestructura de Internet en IPv6 y dejando por un lado el protocolo IPv4.

2.1 El papel del IETF

El papel que desempeña “La fuerza de trabajo de Investigación sobre Internet (Internet *Engineering Task Force*, IETF) “ es fundamental para el crecimiento del protocolo IPv6. A través de ella, además de estandarizar protocolos para la arquitectura de Internet, se publican especificaciones para dicho protocolo, como mecanismos de transición hacia IPv6, inspecciones de direcciones IPv4 actuales en normas IETF, etc.

La mayoría de estos documentos son presentados en forma de RFC (*Request for comments*) y también existen documentos en forma de *Internet drafts*.

2.2 Metas de la transición

Las metas de la transición de Internet del protocolo IPv4 al IPv6 son:

- La meta principal del proceso de transición es la coexistencia de IPv4 e IPv6 hasta que IPv4 desaparezca completamente en algún momento.

- El uso de *hosts* y *routers* con soporte de IPv6 debe ser distribuido sobre Internet en una forma simple y progresiva.

- Reducir las interdependencias durante la transición.

- La transición para los administradores de red y los usuarios finales debe ser fácil de implantar.

2.3 Transición simple de Internet (SIT)

Un conjunto de mecanismos denominado “Transición simple de Internet (SIT)“ fue implantado, el cual incluye protocolos y reglas de manejo para simplificar la transición.

2.3.1 Características del SIT

Las principales características del “SIT (Transición simple de Internet) “ son:

- Posibilidad de una transición progresiva y no traumática. Los *hosts* y *routers* con protocolo IPv4 pueden ser actualizados a IPv6 uno a la vez, sin necesidad de actualizar todos al mismo tiempo.

- Mínimo de requerimientos para realizar la actualización a IPv6. El único requerimiento para actualizar los *hosts* a IPv6 es tener un servidor DNS para manejar direcciones IPv6 y tener un soporte a nivel de sistema operativo del *host*.

- Simplicidad en el direccionamiento. Cuando un *router* o *host* es actualizado a IPv6, puede continuar con el uso del protocolo IPv4.

- Costo inicial bajo. No se necesita un trabajo preparatorio para iniciar la transición a IPv6.

2.3.2 Requerimientos del SIT

Los requerimientos del “SIT (Transición simple de Internet) “ son:

- Una estructura de direcciones IPv6 que permita la derivación de direcciones IPv6 desde direcciones IPv4.

- La disponibilidad de una pila doble con los protocolos IPv4 e IPv6 durante la transición. Esto significa la presencia de las pilas de los protocolos IPv4 e IPv6 al mismo tiempo, para que exista comunicación con nodos que solo trabajen con el protocolo IPv4 o solo IPv6 o ambos protocolos.

- Una técnica para encapsular paquetes IPv6 dentro de paquetes IPv4, esto es, la creación de túneles dinámicamente para permitir el envío de paquetes IPv6 a través de infraestructuras que todavía no fueron actualizadas a IPv6.

- Una técnica opcional que consiste en la traducción de cabeceras IPv6 en cabeceras IPv4 y viceversa, para permitir en una fase avanzada de la transición que nodos que solo tengan soporte para IPv4 se puedan comunicar con nodos que solo tengan soporte para IPv6.

El SIT garantiza que los *hosts* con IPv6 pueden interactuar con *hosts* IPv4 inicialmente en el entorno completo de Internet. Cuando la migración sea completa en dicho entorno, esta interacción será localmente garantizada por un periodo muy largo. Esta capacidad permite la protección de las inversiones de dinero realizadas, por cada organización, en IPv4.

Esto debido a que existen actualmente dispositivos (impresoras de red, terminales, etc) con el protocolo IPv4 implantado que no se pueden actualizar a

IPv6. Por lo tanto, continuará la interacción, con el protocolo IPv4 e IPv6 hasta que estos dispositivos ya no se utilicen más.

La posibilidad de una transición en forma progresiva y eficiente permite a organizaciones integrar el protocolo IPv6 en *routers*, sistemas operativos, software de red, etc, cuando ellos piensen que la transición se encuentre en un estado estable.

2.4 Características de la transición

Las características de la transición son:

- Los protocolos IPv4 e IPv6 son incompatibles a nivel de paquete. Los nodos finales actuales de Internet no generan ni reconocen IPv6. Los *routers* IP actuales de Internet descartan los paquetes IPv6.

- La principal dificultad consiste en migrar la infraestructura de la Internet actual. Durante la etapa de la transición de la Internet actual, existirán redes con infraestructura IPv4 y otras con infraestructura IPv6, esto es, la Internet tendrá un entorno mixto.

2.5 Requerimientos para una transición suave

Para una suave e independiente transición un conjunto de mecanismos han sido diseñados. Dichos mecanismos fueron diseñados para un mapeo de direcciones fácil, coexistencia de los protocolos IPv4 e IPv6, y una transición para el nombre del servicio.

El proceso actual de transición puede ser comparado con los cambios en sistemas operativos y en los ambientes de desarrollo de aplicaciones que se construyen dentro de una organización. Los esfuerzos tomados en la transición hacia el protocolo IPv6 deberían ser los mismos que se tomarían en la transición de un proyecto de escala menor.

Los requerimientos para realizar una transición suave hacia IPv6 son:

- Minimizar la resistencia
- Esfuerzos

2.5.1 Minimizar la resistencia

La actitud general de la mayoría de las organizaciones está en desacuerdo que el IPv6 sea útil. Los puntos de vista de la IETF y de las organizaciones son diferentes, lo cual significa que existe una gran resistencia

en adoptar la nueva tecnología. Las organizaciones miran el mundo desde un punto de vista de negocios, en donde la tecnología es una herramienta para hacer negocios, las técnicas usadas nunca son el factor principal a tomar en cuenta.

El factor importante para que la transición se pueda completar en la totalidad de Internet es que los mecanismos de transición sean aceptados por la mayoría de los usuarios de Internet.

2.5.2 Esfuerzos

Los esfuerzos que se deben realizar se resumen en 4 los cuales son:

2.5.2.1 Transición progresiva

Se esta conciente de que la transición total de Internet al protocolo IPv6 tomará un periodo de tiempo, y no hay forma de sincronizar el proceso de transición de los diferentes sitios. Presumiblemente solo las organizaciones pequeñas podrán adoptar IPv6 en un simple paso.

La otra parte de las organizaciones deberían realizar su propio plan de transición, y realizarlo con las menores interdependencias posibles.

El equipo de red con IPv4 e IPv6 puede coexistir e interactuar sin ningún problema. Además, se debe tomar en cuenta que actualmente existen dispositivos de toda clase utilizando el protocolo IPv4 que nunca podrán ser actualizados hacia IPv6, y por lo tanto la interacción entre los 2 protocolos debe existir sin ningún problema, hasta que dichos dispositivos no se utilicen mas.

2.5.2.2 Coexistencia e interacción

La independencia de la transición significa que la adopción de nuevo equipo con soporte integrado para IPv6, no esta vinculado con la actualización de dispositivos de la red, los cuales pueden seguir operando con el protocolo IPv4.

El equipo y *software* antiguos se pueden seguir utilizando mientras transcurre el periodo de tiempo para llevar a cabo la transición total de Internet al nuevo protocolo. Los sistemas antiguos deben seguir ejecutándose de la misma forma y deben ser capaces de comunicarse con el equipo nuevo y el antiguo, es decir, que debe haber soporte para IPv4 e IPv6 en todos los nuevos sistemas y equipos.

2.5.2.3 Esquema flexible de mapeo de direcciones

IPv6 a través de largo espacio de direccionamiento puede asignar incluso múltiples direcciones IPv6 a cada *host*.

Para hacer el proceso de transición más fácil, un mapeo simple desde direcciones IPv4 es necesario. No es posible asumir que todas las direcciones IPv4 son globalmente únicas, el mapeo debe realizarse en un sitio específico.

2.5.2.4 Herramientas de manejo inteligentes

Durante la transición y la existencia de ambos protocolos de red, se tendrá demanda por un conjunto de herramientas de manejo de los protocolos IPv4 e IPv6. Las nuevas herramientas deben ser lo suficientemente inteligentes para separar las características de IP4 e IPv6 en múltiples niveles. La detección de posibles rutas y diferentes puntos de traducción deberían ser implantados en dichas herramientas.

Un mecanismo para la revisión de la capacidad de IPv6 en *hosts* remotos y dispositivos, es esencial.

2.6 Componentes de la transición

Los componentes involucrados en la transición hacia el protocolo IPv6 son:

- Nodos clientes
- *Routers* y protocolos de ruteo

- Sistema de nombres del dominio (DNS)

- Dependencias de componentes.

2.6.1 *Hosts*

En la práctica el concepto de una transición progresiva significa que por un tiempo la Internet contendrá *hosts* de 2 tipos, los que tengan soporte solo para IPv4 y los que tengan soporte para IPv4 e IPv6. Para que exista una interacción transparente entre dichos tipos de *hosts*, todos los *hosts* utilizando IPv6 deben ser capaces de comunicarse con la tecnología antigua.

En el nivel de aplicación, *software* diseñado para IPv4 utiliza por ejemplo, la API antigua, mientras que las nuevas aplicaciones con soporte para IPv6, utilizan la nueva API. La IPv4 API y aplicaciones estándar deben ser capaces de ejecutarse en *hosts* con soporte para IPv6.

2.6.2 Routers y protocolos de ruteo

Los nuevos dispositivos no pueden asumir que todos los nodos con los que están interactuando tienen soporte para IPv6. Los protocolos de ruteo deben permitir en detalle un ruteo basado en el tráfico fuente y destino.

2.6.3 Sistemas de nombres del dominio (DNS)

Durante la fase de transición pueden existir nodos con direcciones de ambos tipos, es decir, nodos con una dirección IPv4 y una IPv6, pero también existirán otros que tengan soporte solo para IPv4. Sin embargo, una dirección IPv6 pudo ser asignada a algún nodo. DNS tiene que trabajar con ambas direcciones para que estos nodos puedan realizar consultas. En nodos con ambos protocolos deben decidir al momento de una comunicación que protocolo utilizarán.

Una condición especial ocurre cuando una dirección IPv6 ha sido asignada a un nodo en el DNS, pero dicho nodo no tiene todavía soporte para IPv6. Esto es denominado Agujero negro (*Black Hole*) en el espacio de direcciones del protocolo IPv6 y el *software* del protocolo en dicho nodo debe tratar con dicho error en una forma aceptable.

2.6.4 Dependencias de componentes

Servidores DNS son los primeros dispositivos físicos a actualizar después de una previa asignación de espacio de direcciones IPv6 y que un esquema de direccionamiento esté disponible. Esto permite a los nuevos nodos con soporte IPv6, averiguar el nombre del servicio para direcciones IPv6. La transición del *software* de los *hosts* y *routers* es menos critica. El concepto del protocolo dual permite a sistemas basados en IPv4 continuar su funcionalidad, sin sufrir ninguna modificación.

2.7 Actores de Internet

Los principales actores involucrados en la transición del protocolo IPv4 a IP6 son los siguientes:

- Mecanismos de transición. Los mecanismos deben cumplir con el mecanismo de realizar una transición de una manera suave y progresiva. Estos permitirán la coexistencia entre los protocolos IPv4 e IPV6.

- Crecimiento de la tecnología móvil. Tecnologías como UMTS que requieren un gran número de direcciones IP harán uso del protocolo IPv6 para lograr la comunicación. Al momento de esta tecnología causar un gran impacto el protocolo IPv6 también causará un gran impacto.

2.8 Interoperabilidad IPv4/IPv6

Por un largo período, se estará tratando con redes que utilizan ambos protocolos para la comunicación. Una estimación de dicho tiempo, es 10 años, que en el mundo de la Internet es un periodo de tiempo, verdaderamente largo. Esto debido, a la gran cantidad de *software* e infraestructura que utiliza el protocolo IPv4, para la comunicación. Toda esta infraestructura deberá ser reemplazada o actualizada al nuevo protocolo IPv6 de comunicación.

Durante el período de transición, nodos que utilicen el protocolo IPv6, se comunicarán con nodos que solo utilicen el protocolo IPv4. Además existirán redes LAN dotadas de una infraestructura IPv6, denominadas “Islas Aisladas”, mientras que otras aún con una infraestructura IPv4. Dichas islas aisladas para realizar la comunicación con otras con infraestructura IPv4, utilizarán la infraestructura IPv4 brindada por la Internet.

Para solucionar el primero de estos casos, se utilizan pilas duales IP, es decir nodos que contengan una pila de protocolos IPv4, y otra de protocolos IPv6. Y en el segundo de estos casos, se utilizan túneles para la comunicación entre redes que con infraestructura IPv4 y otras con infraestructura IPv6.

3. MECANISMOS DE TRANSICIÓN

3.1 Pilas dobles IPv4/IPv6

El camino más obvio, para que un nodo pueda comunicarse con nodos que solo utilicen el protocolo IPv4 o solo el protocolo IPv6, es el uso simultaneo en dicho nodo de ambos protocolos, en pilas separadas, esto es un nodo con ambas pilas de protocolos puede enviar y recibir información de otros nodos sin importar la versión de protocolo que dichos nodos soporten.

Los nodos con ambas pilas de protocolos se denominan “nodos IPv6/IPv4”. Al utilizar este mecanismo de pilas dobles se tiene una dirección en cada pila. Estas direcciones IPv4 e IPv6 puede que estén relacionadas entre ellas mismas, pero no es un requisito de implementación de este método, por lo que estas direcciones pueden no tener ninguna relación.

Para obtener su dirección IPv6, dichos nodos pueden utilizar los mecanismos de autoconfiguración sin estado o mediante DHCPv6, y para la obtención de su dirección IPv4 pueden utilizar los mecanismos o protocolos estándar, es decir, DHCPv4, protocolo de arranque (BOOTP), protocolo de resolución de direcciones inverso (RARP) o la configuración manual en el nodo de la dirección IPv4.

Para que estas direcciones IPv4 e IPv6 estén relacionadas de cierta forma dentro de cada nodo, se puede hacer uso de las direcciones IPv6 compatibles con IPv4. Una dirección de este tipo tiene en sus 96 bits de orden mayor (los de la izquierda) un valor de 0:0:0:0:0:0 y en los 32 bits de menor orden (los de la derecha) una dirección IPv4. Así, al utilizarlas, se podría tener en la pila de IPv6, la dirección que comprende los 96 bits con valor de 0:0:0:0:0:0 mas la dirección IPv4, y en la pila de IPv4 la dirección IPv4 que se encuentra en los 32 bits de orden menor de la dirección IPv6.

Los pasos para la obtención de una dirección IPv6 compatible con IPv4, son:

1. El nodo IPv6/IPv4 utiliza los mecanismos o protocolos estándar, para la obtención de la dirección IPv4. Entre estos mecanismos, están:
    - El protocolo de configuración dinámica del host (DHCPv4)
    - El protocolo de arranque (BOOTP)
    - El protocolo de resolución de direcciones inverso (RARP)
    - La configuración manual de la dirección IPv4 en el nodo
2. El nodo utiliza la dirección del paso 1, como su dirección IPv4.

3. El nodo antepone el prefijo de 96 bits, con valor de 0:0:0:0:0:0, a la dirección IPv4 obtenida en el paso 1. El nodo utiliza esta dirección, como su dirección IPv6.

3.1.1 DNS

El servicio de nombres de dominio (DNS), es utilizado para ambas pilas de protocolos IPv4 e IPv6. El DNS es un mecanismo para relacionar un nombre de un nodo con una dirección IP. Debido a que este mecanismo fue diseñado originalmente para trabajar con direcciones IPv4, debe ser actualizado para trabajar con direcciones IPv6. Esta actualización ha sido diseñada para ser compatible con las aplicaciones actuales que trabajan con direcciones IPv4.

Esta actualización incluye los siguientes 3 aspectos:

- El registro AAAA. Es un nuevo tipo de registro para almacenar una dirección IPv6 de un nodo. Este registro es similar al registro A para direcciones IPv4, pero con tamaño de dirección de 128 bits.

- El dominio IP6.INT. Este dominio se utiliza para realizar la búsqueda inversa para los nodos de IPv6, es decir, búsquedas basadas en direcciones IPv6. Su representación se realiza en orden inverso de la dirección IPv6, seguido de ".IP6.INT". Por ejemplo la búsqueda inversa de la dirección 4321:0:1:2:3:4:567:89ab, se representaría como: "b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.INT".

- Redefinición de consultas existentes. Todos los tipos de consultas (NS, MX, MB, etc), deben soportar tanto los registros A como los AAAA y deben realizar cualquier procesamiento asociado a cada tipo de registro.

3.1.1.1 Resolución del DNS

En el momento de asignarle a un nodo IPv6/IPv4 sus direcciones IPv6 e IPv4, estas deben ser registradas en sus respectivos registros AAAA y dentro del DNS, es decir, se deben crear dos registros para dicho nodo dentro de DNS, en los cuales, dentro del registro AAAA, se registre la dirección de 128 bits, y en el registro A la dirección IPv4 de 32 bits para dicho nodo.

Esto debido a que los nodos IPv6/IPv4 puede comunicarse con otros nodos que solo soporten direcciones IPv4 o solo direcciones IPv6. Por ejemplo, un nodo que solo soporta direcciones IPv4 hace una consulta a otro nodo IPv6/IPv4, entonces a través del registro A, que tiene la dirección IPv4 del nodo IPv6/IPv4, se puede establecer la comunicación entre los dos nodos. Al igual si se tratara de un nodo que solo soporta direcciones IPv6 y desea comunicarse con dicho nodo IPv6/IPv4, entonces a través del registro AAAA, se puede obtener la dirección IPv6 del nodo IPv6/IPv4.

En el momento que se hace una consulta a un nodo específico y el resolutor de DNS descubre que dicho nodo tiene asociado los registros AAAA y A, éste tiene 3 opciones para responder a la consulta, la cuales son:

- Retornar solo la dirección IPv4
- Retornar solo la dirección IPv6
- Retornar ambas direcciones IPv4 e IPv6.

La elección del tipo de dirección a retornar, o, si ambas direcciones son retornadas, puede afectar el tipo de tráfico IP a generarse. Si se retorna la dirección IPv6, el nodo IPv6/IPv4 se comunicará con el destino a través de paquetes IPv6. Si se retorna la dirección IPv4, la comunicación se establecerá a través de paquetes IPv4.

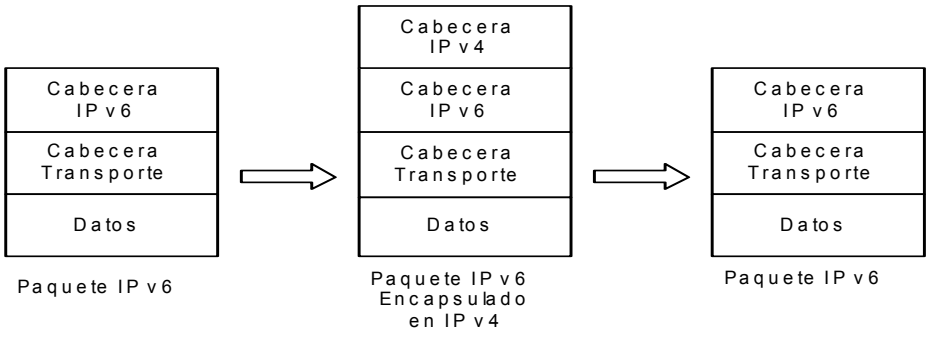
3.2 Túneles IPv6 sobre IPv4

Debido a que la transición de la infraestructura de la Internet actual al protocolo IPv6, no se hará de un día para otro, utilizar dicha infraestructura IPv4 suena lógico mientras aumenta el número de redes LAN que son actualizadas hacia el protocolo IPv6.

Al momento que un nodo ha sido actualizado al protocolo IPv6, por lógica querrá enviar información en formato IPv6 y los túneles son la solución para que este nodo pueda enviar tráfico IPv6 sin necesidad de esperar que toda la infraestructura de la Internet actual sea actualizada hacia IPv6.

Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4. Los nodos IPv6/IPv4 envían datagramas IPv6 con una cabecera IPv4, así de esta forma, un nodo IPv6 puede ser localizado mediante una infraestructura IPv4. Un nodo con soporte para IPv6, que se encuentre ubicado en una red LAN específica y desee enviar información a otro nodo, que también posea soporte para IPv6, ubicado en otra red LAN diferente puede realizarlo a través de túneles. Un paquete IPv6 encapsulado puede ser reconocido por el campo protocolo de la cabecera IPv4, ya que dicho campo es establecido a 41. Este valor es útil para un nodo, ya que al reconocer este valor extrae la cabecera IPv4, esto es, desencapsula el paquete. El encapsulado y desencapsulado de los datagramas es el siguiente:

Figura 7. Encapsulado y descencapsulado de datagramas IPv6



Además este mecanismo esta enfocado a unir redes LAN con infraestructura IPvX (islas IPvX) a través de un una infraestructura IPvY (océano IPvY). La X e Y representan las versiones 4 ó 6. Debido a que la transición se realizará de manera progresiva, durante dicha fase de transición existirán redes LAN aún con infraestructura IPv4 y otras redes LAN que tendrán infraestructura IPv6; además, la columna vertebral de la Internet actual, cambiará

gradualmente su infraestructura IPv4 a IPv6. Mientras dicho cambio es hecho a la Internet actual, la infraestructura IPv4 puede permanecer funcional y puede ser utilizada para transportar tráfico IPv6 a través de ella.

Por lo tanto, los túneles proporcionan un mecanismo para permitir la comunicación entre nodos con soporte para IPv6, para cumplir su principal objetivo que se centra en envío de tráfico IPv6 entre dichos nodos. Dicha comunicación es posible realizarla debido a 2 factores: el encapsulado de datagramas e infraestructuras basadas en el protocolo IPv4 o IPv6, esto es, los datagramas encapsulados por el nodo origen viajan, para llegar al destino, a través de varias infraestructuras que en algunos casos pueden estar basadas en el protocolo IPv4 y en otros casos en el protocolo IPv6.

Estos túneles pueden ser construidos de distintas formas, las cuales son:

- *Router a router*
- *Host a Router*
- *Host a Host*
- *Router a Host*

Para cada uno de los cuatro casos anteriores, el primer extremo del túnel, se refiere al nodo que encapsula el datagrama IPv6 en un paquete IPv4, y el segundo extremo o extremo final, se refiere al nodo que desencapsula el

paquete IPv6. A partir de las cuatro configuraciones anteriores, los túneles se dividen en:

- Túneles configurados
- Túneles automáticos
- 6over4
- Túneles 6to4
- Túnel *broker*, Túnel *Server*

3.3 Túneles configurados

Los túneles se clasifican según la forma por la cual es obtenida la dirección del nodo del extremo final del túnel, por parte del nodo origen que realiza el encapsulado de los datagramas IPv6. Los túneles configurados tienen algunas características en la forma en que el nodo origen obtiene dicha dirección del extremo final, además de otras características.

3.3.1 Características

Las características de los túneles configurados se refieren a funcionalidad y la forma de configuración de las direcciones IPv4 e IPv6, las cuales son:

- La función principal de un túnel configurado es conectar dos redes IPv4 o IPv6 para el envío de tráfico IPv6, por medio de una infraestructura IPv4. Esta característica es muy importante ya que le permite a un nodo que tenga soporte para IPv6, dentro de una red IPvX, la comunicación con otro nodo IPv6 que forma parte de otra red IPvX. Su importancia radica en que el nodo origen dentro de su red puede ser el único con soporte para IPv6, sin necesidad que los demás nodos tengan dicho soporte.

- Cada extremo del túnel es un nodo IPv6/IPv4 y en ellos se configuran las direcciones IPv4 e IPv6 tanto local como remotas.

- El datagrama IPv6 encapsulado es enviado hacía un *router*. Dicho *router,* que es el extremo final de este tipo de túnel, debe desencapsular el paquete IPv6 y reenviarlo a su destino final.

- La dirección del *router* al cual se envía la información en formato IPv6 debe ser obtenida a través de configuración que se encuentre en el nodo origen que envía el datagrama IPv6 encapsulado en IPv4.

- Debido a que dicho *router* no es el destino final para el cual se envía el paquete IPv6, la dirección en el paquete IPv6 no proporciona la dirección IPv4 del *router*, sino la dirección del nodo destino.

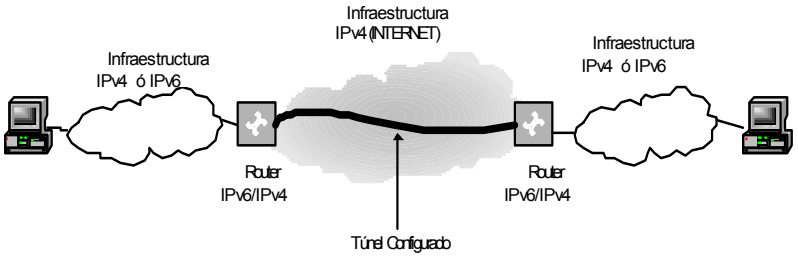
Debido a que en este tipo de túneles el datagrama IPv6 encapsulado se envía hacía un *router*, estos túneles, pueden ser construidos de 2 formas:

- *Router a router*
- *Host a Router*

3.3.2 *Router* a *router*

El objetivo de este tipo de túneles consiste en que el par de *routers* sean intermediarios entre dos nodos IPv6/IPv4, ubicados en redes diferentes, que deseen intercambiar información en formato IPv6. La forma de un túnel configurado *router* a *router* es la siguiente:

Figura 8. Túnel configurado *router* a *router*

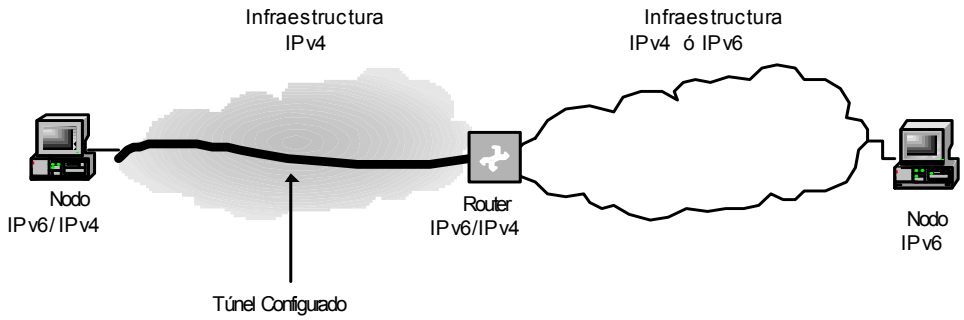


Un túnel de este tipo abarca el segmento "extremo a extremo" por el cual se unen las 2 redes, a través de la infraestructura IPv4 de la Internet actual. Cuando dos nodos ubicados en redes diferentes, que deseen intercambiar información en formato IPv6, un túnel de este tipo abarca el segmento completo por el que viaja la información en formato IPv6 a través de la Internet actual y no abarca la ruta por donde viajan la información IPv6 dentro de cualquiera de las dos redes.

3.3.3 *Host* a *router*

El objetivo de este tipo de túneles consiste en que uno o más *hosts* puedan enviar información en formato IPv6 a un *router* intermedio, dentro de la misma red, que sea alcanzable a través de una infraestructura IPv4 externa a dicha red a la que pertenecen los *hosts*. La forma de un túnel configurado *host* a *router* es la siguiente:

Figura 9. Túnel configurado *host* a *router*



Un túnel de este tipo abarca el "primer segmento" de la ruta que siguen los datagramas IPv6 encapsulados en IPv4. Cuando dos nodos, ubicados en redes diferentes, que deseen intercambiar información en formato IPv6, un túnel de este tipo abarca la ruta de la red origen por la que viajará la información en formato IPv6 para llegar al nodo destino.

3.3.4 Ventajas y desventajas los túneles configurados

Las ventajas de la utilización de túneles configurados se resumen en:

- Es un método totalmente transparente respecto a la capa IPv6 y superiores, con lo cual inversiones hechas en aplicaciones basadas en el protocolo IPv4 no se pierden, ya que estas aplicaciones no son afectadas.

- No consume excesivos recursos.

Las desventajas de la utilización de túneles configurados se resumen en:

- Por cada nodo de una red que desee enviar información en formato IPv6, se debe hacer manualmente la configuración local de la dirección IP del *router* intermedio y para el intercambio de información con nodos de otras redes, en el *router* intermedio se debe crear previamente los túneles hacia dichas redes.

- Es necesario que los *routers* tengan soporte para IPv6 e IPv4. Será una desventaja, cuando un nodo IPv6/IPv4 desee intercambiar información IPv6, y de ninguna forma sea posible que el *router* de su red pueda tener soporte para IPv6.

3.4 Túneles automáticos

3.4.1 Características

- Permiten a nodos IPv6/IPv4 comunicarse a través una infraestructura IPv4. Al igual que con los túneles configurados, esta característica es muy importante, ya que le permite a un nodo que tenga soporte para IPv6, dentro de una red la comunicación con otro nodo IPv6 que forma parte de otra red. Por lo tanto, dicho nodo puede ser el único dentro de su red que tenga soporte para IPv6.

- Cada extremo del túnel es un nodo IPv6/IPv4.

- Son necesarias las direcciones IPv6 compatibles con IPv4 para determinar los extremos del túnel. Dichas direcciones, deben tener un prefijo ::/96 + dirección IPv4 (extremo final del túnel). En la información que es destinada a estas direcciones, la dirección IPv6 origen corresponde a la dirección compatible con IPv4 del nodo origen, mientras la dirección IPv6 destino corresponde a la dirección compatible con IPv4 del nodo destino.

- Se define una interfaz virtual para la dirección IPv6 compatible con IPv4.

- El datagrama IPv6 encapsulado es enviado hacía el *host* destino. El extremo final del túnel es el nodo destino del paquete IPv6. Dicho nodo destino debe desencapsular el paquete IPv6.

- La dirección del *host* al cual se envía la información en formato IPv6 se obtiene a través de los 32 bits de orden menor (los de la derecha) de la dirección destino IPv6 compatible con IPv4.

Debido a que en este tipo de túneles el datagrama IPv6 encapsulado se envía hacía el *host* destino, estos túneles, pueden ser construidos de 2 formas:

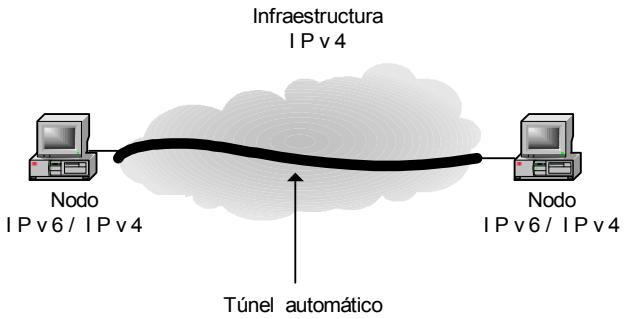
- *Host a host*

- *Router a host*

3.4.2 *Host* a h*ost*

El objetivo de este tipo de túneles, consiste en que dos nodos IPv6/IPv4, que residen dentro de la misma infraestructura IPv4, puedan intercambiar información en formato IPv6. La forma de un túnel automático *host* a *host* es la siguiente:

Figura 10. Túnel automático *host* a *host*

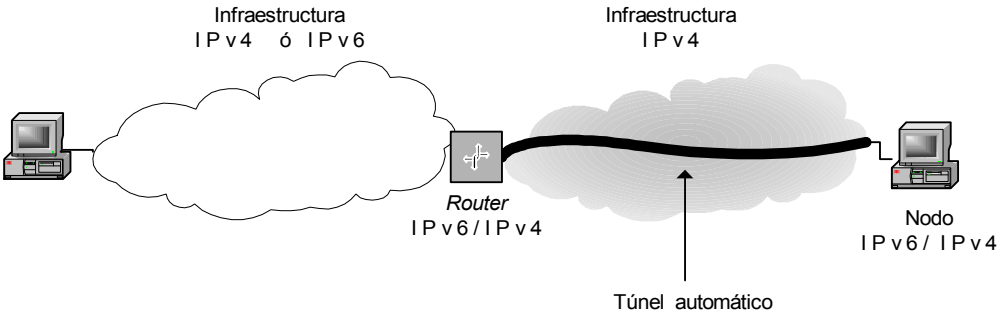


Cuando un nodo IPv6/IPv4 desee intercambiar información en formato IPv6 con otro nodo IPv6/IPv4, un túnel de este tipo abarcará la ruta completa por donde viaja la información en formato IPv6.

3.4.3 *Router* a *host*

El objetivo de este tipo de túneles, consiste en que un *router* intermedio pueda enviar información en formato IPv6, que provenga de una infraestructura IPv4 externa, a uno o mas *hosts* ubicados dentro de su misma red. La forma de un túnel automático *router* a *host* es la siguiente:

Figura 11. Túnel automático *router* a *host*



Un túnel de este tipo abarca el "último segmento" de la ruta que siguen los datagramas IPv6 encapsulados en IPv4. Cuando dos nodos, ubicados en redes diferentes, que deseen intercambiar información en formato IPv6, un túnel de este tipo abarca la ruta de la red destino por la que viajará la información en formato IPv6 para llegar al nodo destino.

3.4.4 Ventajas y desventajas los túneles automáticos

Las ventajas de la utilización de túneles configurados se resumen en:

- Es un método totalmente transparente respecto a la capa IPv6 y superiores.

- Este tipo de túneles evita la necesidad de configurar manualmente la dirección del extremo final del túnel en cada nodo que desea intercambiar información en formato IPv6.

Las desventajas de la utilización de túneles automáticos se resumen en:

- En túneles *router* a *host* es necesario que el *router* sea un *router* IPv6/IPv4. Será una desventaja, cuando de ninguna forma sea posible que el *router* de la red pueda tener soporte para IPv6.

Los túneles configurados y automáticos se diferencian principalmente en la forma en que el nodo origen determina la dirección el extremo final del túnel, pero ambos tienen similitudes las cuales son:

- El nodo del principio del túnel realiza el encapsulado del paquete, ya que, crea una cabecera IPv4 encapsulada y transmite el paquete encapsulado.

- El nodo del extremo final del túnel realiza el desencapsulado del paquete, recibe el paquete encapsulado quita la cabecera IPv4, actualiza la cabecera IPv6 y procesa el paquete IPv6 recibido.

3.5 Mecanismos de traducción

3.5.1 Mecanismo de transición de doble pila (DSTM)

Es un mecanismo que permite a nodos IPv6/IPv4, pertenecientes a redes que tengan soporte para IPv6, la comunicación con otros nodos de redes

diferentes que tengan soporte para IPv4. Este mecanismo se basa en que los nodos IPv6/IPv4 obtienen temporalmente una dirección IPv4 para el intercambio de información con nodos ubicados en redes diferentes. La utilización de este mecanismo requiere por lo menos una dirección IP4 para la red. Los componentes involucrados en este mecanismo son los siguientes:

- Nodo IPv6/IPv4. Es un componente que maneja tanto direcciones IPv4 como IPv6.

- Servidor DSTM. Es el componente encargado de proporcionar las direcciones IPv4 a los nodos IPv6/IPv4.

- Interfase *4over6*. Forma parte del nodo IPv6/IPv4 y es la encargada de encapsular los paquetes IPv4 en paquetes IPv6.

- *Router* DSTM. Es el componente encargado del intercambio de información entre los nodos IPv6/IPv4 y otros ubicados rede distintas. Realiza el proceso de descencapsulamiento de paquetes provenientes de los nodos internos de la red.

El funcionamiento de este mecanismo es el siguiente:

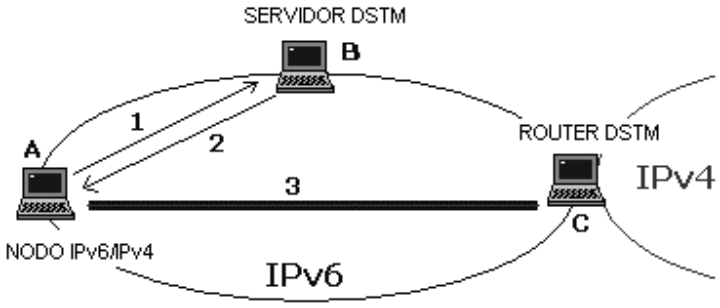
1. El nodo IPv6/IPv4 perteneciente a la red IPv6 al desear comunicarse con un nodo perteneciente a otra red, con el objetivo de intercambiar información en formato IPv4, solicita al servidor DSTM una dirección IPv4.

2. El servidor DSTM reserva una dirección IPv4 para el nodo IPv6/IPv4 tomada de su pila de direcciones IPv4 y la envía a dicho nodo. En dicha respuesta también se envía el tiempo de duración de la dirección IPv4, así como la dirección IPv6 del *router* DSTM. La respuesta a esta petición puede hacerse mediante DHCPv6, RPC u otro mecanismo. El nodo IPv6/IPv4 al obtener la dirección IPv4 la configura dentro de su pila IPv4 como su dirección.

3. Debido a que no existe una infraestructura IPv4 dentro de la red no se pueden enviar paquetes IPv4 directamente. Dichos paquetes deben encapsularse en paquetes IPv6 y enviarlos al *router* DSTM. Se envía el paquete IPv4 acompañado de una cabecera IPv6 hacía el *router* DSTM. El *router* remueve la cabecera IPv6 y lo envía hacia otra red exterior.

La siguiente figura muestra el proceso realizado por el mecanismo DSTM:

Figura 12. Proceso realizado por el DSTM



Para realizar el encapsulado y descencapsulado de paquetes IPv4 el *router* DSTM mantiene una tabla de mapeo que contiene las direcciones IPv4 e IPv6 de los nodos que pertenecen a la red interna. Además para asegurar una comunicación bidireccional se debe tomar en cuenta que todos los paquetes deben pasar por el *router* DSTM. Este mecanismo actualmente se encuentra en progreso.

3.5.1.1 Ventajas

Las ventajas de la utilización del mecanismo DSTM se resumen en:

- Es transparente a nivel de IPv6, las aplicaciones existentes pueden ejecutarse en una infraestructura IPv6 sin afectar su funcionamiento.

- La administración de la red se simplifica al tratar solo con direcciones IPv6.

- La necesidad de direcciones IPv4 es reducida. Estas direcciones son dadas temporalmente solo cuando son requeridas por los nodos de la red y no deben asignarse previamente a cada nodo de la red.

3.5.2 Traducción de dirección de red y de protocolo (NAT-PT)

Es un mecanismo que permite a nodos que tienen soporte solo para IPv6, pertenecientes a redes con soporte solo para IPv6, la comunicación con

otros nodos de redes diferentes que tengan soporte para solo para IPv4. Es un mecanismo que realiza la traducción no solamente de direcciones IP sino también de protocolo.

3.5.2.1 Características

- Permite la comunicación de nodos que solo tienen soporte para IPv6, con otros nodos que tienen soporte solo para IPv4 que se encuentran ubicados en redes distintas. Al contrario de IPv4 NAT, que provee un enrutamiento entre el dominio IPv4 interno de la red y otro dominio IPv4 externo, IPv6 NAT provee un enrutamiento entre el dominio IPv6 interno de la red y un dominio IPv4 externo.

- Utiliza un dispositivo dedicado que realiza la traducción de direcciones IPv4 a IPv6 y viceversa. El traductor de direcciones es denominado IPv6 NAT y es similar en su lógica al traductor de direcciones IPv4 NAT pero no idéntico. IPv4 NAT traduce una dirección IPv4 a otra dirección IPv4. IPv6 NAT traduce una dirección IPv4 a una dirección IPv6 y viceversa.

- El traductor de protocolo (PT), utiliza el mecanismo de traducción SITT para traducir un paquete IPv4 en un paquete equivalente en formato IPv6 y viceversa. NAT-PT reside dentro del *router* frontera de la red interna IPv6 con la red IPv4 denominada Internet.

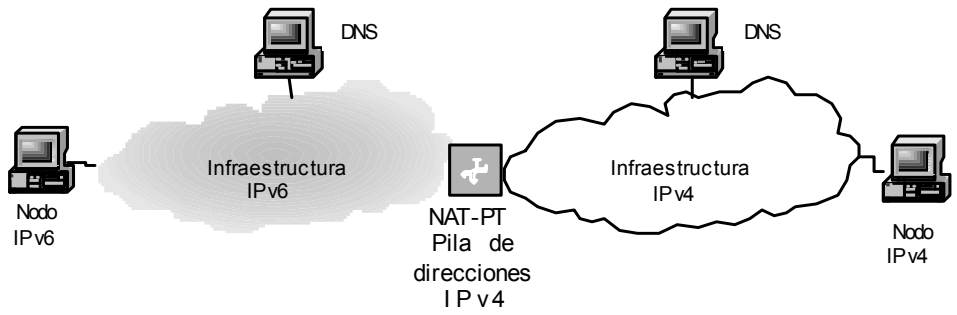
- Utiliza una pila de direcciones IPv4 para asignarlos a los nodos que tienen soporte solo para IPv6. Dichas direcciones deben ser únicas, deben ser direcciones IPv4 públicas y no privadas.

- Este mecanismo requiere por lo menos una dirección IPv4 pública para la red IPv6 que desea comunicación con redes IPv4.

- Utiliza una tabla de mapeo que contiene el vinculo de las direcciones IPv6 de los nodos internos de la red IPv6 con las direcciones IPv4 de los nodos externos a la red y viceversa para proveer un ruteo transparente.

- Este mecanismo utiliza algunas extensiones para proveer transparencia nivel de aplicación. Dichas aplicaciones son denominadas ALG y permiten a un nodo IPv6 la comunicación con un nodo IPv4 y viceversa, permite iniciar a un nodo interno la comunicación con un nodo externo y viceversa. Específicamente utiliza las aplicaciones DNS-ALG y FTP-ALG. DNS-ALG transforma peticiones DNS de registros "A" a peticiones "AAAA" y viceversa, pero cuando un nodo externo intenta iniciar la comunicación con un nodo interno y viceversa. FTP-ALG es necesario para proveer una transparencia a nivel de aplicación para el protocolo FTP. Al colocar estas extensiones hacen que este mecanismo en sus componentes básicos (NAT, PT), no sea transparente a nivel de aplicación. La siguiente figura muestra la aplicación de NAT-PT:

Figura 13. Aplicación de NAT-PT a una infraestructura IPv6



3.5.2.2 Ventajas y desventajas

Las ventajas de la utilización del mecanismo NAT-PT se resumen en:

- Actualmente muchas redes de organizaciones utilizan IPv4 NAT y se poseen mucha experiencia en su administración, por lo que se facilitaría la administración de NAT-PT.

Las desventajas de la utilización del mecanismo NAT-PT se resumen en:

- La administración de un NAT implica un alto costo.
- El proceso del NAT consume muchos mas recursos comparado con la utilización de túneles.
- Para ser transparente a nivel de aplicación es necesario agregar extensiones como DNS-ALG o FTP-ALG según sea el caso.

3.5.3 FTP-ALG

Este mecanismo es requerido para proporcionar transparencia a nivel de aplicación para el protocolo FTP durante la comunicación entre nodos que utilizan el protocolo IPv4 y los que utilizan el IPv6 . Durante la transición del protocolo IPv4 al IPv6 el protocolo FTP debe tener la habilidad de negociar el

protocolo de red que se utilizará para la transferencia de información. El nombre de este mecanismo proviene del ingles "*Application Level Gateway* (FTP-ALG)".

El protocolo FTP agrega extensiones para su utilización con el protocolo IPv6. Estas extensiones son los 2 comandos: EPRT, EPSV. El comando EPRT permite la especificación de una dirección IPv6 para la transferencia de datos. El comando EPSV solicita para que un servidor escuche a través de un puerto específico y espere por una conexión. Estas extensiones han sido diseñadas para ser utilizadas en nodos IPv6 ó IPv4. Estos comandos sustituyen a los ya existentes en su versión 4, los cuales son PORT y PASV, es decir, EPRT sustituye al PORT y EPSV al PASV. Las diferentes formas en que el mecanismo FTP-ALG realiza la traducción entre nodos IPv4 e IPv6 son las siguientes:

- Si un nodo IPv4 desea comunicarse con un nodo IPv6 y no tiene las extensiones e inicia una conexión FTP ya sea por PORT o PASV, el mecanismo FTP-ALG traducirá estos comandos en EPRT o EPSV respectivamente antes de enviar la solicitud al nodo IPv6. La respuesta del nodo IPv6 será traducida al comando específico del nodo IPv4, es decir, una respuesta de EPRT será traducida a PORT y una EPSV a PASV. Al realizar la traducción, la dirección IPv4 del nodo IPv4 es traducida a una dirección en IPv6 decidida por el mecanismo NAT-PT, además de otros parámetros.

- Si un nodo IPv4 inicia la comunicación y posee las extensiones simplemente el mecanismo FTP-ALG traduce la dirección IPv4 en IPv6, pero no se traducen los comandos ya que son los mismos.

- Sin un nodo IPv6 desea comunicarse con un nodo IPv4 que posee las extensiones EPRT o EPSV, simplemente se traduce la dirección IPv6 de acuerdo al mecanismo NAT-PT a una dirección IPv4. La desventaja de esta opción es que obliga a los nodos IPv4 a poseer las extensiones al comando FTP.

- Si un nodo IPv6 inicia la comunicación y el nodo IPv4 no posee los comandos EPRT o EPSV estos se traducen a PORT o PASV respectivamente, antes de enviarlos al nodo IPV4. Además se traduce la dirección IPv6 a una dirección IPv4.

3.5.4 DNS-ALG

Permite la comunicación entre nodos IPv6 ubicados en una infraestructura IPv6 con nodos ubicados en una infraestructura IPv4. Para permitir dicha comunicación entre ambos tipos de nodos DNS-ALG manipula registros de tipo “A” y de tipo “AAAA” ubicados en un servidor DNS. Las características de DNS-ALG son las siguientes:

- DNS-ALG se encuentra ubicado dentro del dispositivo que implementa NAT-PT en la red interna, el cual generalmente es el *router* frontera de la red que permite la comunicación con la infraestructura IPv4 de Internet.

- Debido a que los nodos internos de la red solamente implementan el protocolo IPv6, es necesario transformar los registros externos de tipo “A” a registros internos de tipo “AAAA” para permitir la comunicación

entre nodos externos e internos, así como también los registros internos de tipo “AAAA” a registros externos de tipo “A”.

El mecanismo DNS-ALG funciona para conexiones entrantes y salientes.

3.5.4.1 Conexiones entrantes

Debido a que el DNS-ALG se encuentra ubicado en el *router* frontera, todos los paquetes provenientes de nodos externos deben antes pasar por el.

Cuando un nodo externo intenta resolver dentro de su servidor de DNS, por un nodo interno en la red IPv6, la solicitud se propaga desde el servidor DNS externo al servidor DNS interno. Antes de enviar la solicitud al servidor DNS interno, el DNS-ALG intercepta el registro “A” lo transforma a un registro “AAAA” y luego lo envía a servidor DNS interno.

El servidor DNS interno responde con el registro “AAAA” del nodo interno solicitado. Este registro es interceptado por el DNS-ALG y transformado a un registro “A” y luego lo envía al nodo externo que hizo la solicitud. El vínculo entre las direcciones de los registros “AAAA” y “A” es almacenado dentro de la tabla de mapeo que posee el NAT-PT.

3.5.4.2 Conexiones salientes

Cuando un nodo interno intenta crear comunicación con un nodo externo, empieza por resolver dentro de su servidor de DNS, para obtener el registro “AAAA” del nodo externo.

Puesto que el nodo externo puede tener una dirección IPv4 o IPv6, el DNS-ALG intercepta el registro y lo envía sin transformarlo al servidor DNS externo. Si el servidor DNS externo responde con un registro “AAAA” el DNS-ALG al interceptarlo lo envía sin ninguna modificación al nodo interno. Si se responde con un registro “A” se transforma a un registro “AAAA” y se envía al nodo interno.

Para realizar la comunicación entre el servidor DNS interno de la red, que solo soporta direcciones IPv6, y una red externa IPv4, una dirección IPV4 es tomada de la pila de direcciones que posee el NAT-PT y vinculada con la dirección IPv6 del servidor DNS interno de la red. Este vínculo es almacenado en la tabla de mapeo que posee el NAT-PT.

3.5.5 Algoritmo de traducción sin estado IP/ICMP (SITT)

Permite a nodos que tienen soporte solo para IPv6 la comunicación con nodos que tienen soporte solo para IPv4, permite la comunicación a nodos pertenecientes a una red IPv6 con nodos que tienen soporte solamente para IPv4. El SIIT básicamente se basa en la traducción de la cabecera IP.

Para permitir la comunicación este mecanismo se basa en las siguientes características:

- Realiza la traducción de la cabecera IP. La traducción se puede realizar de 2 formas. Cuando el SIIT recibe un paquete IPv4 y este tiene una dirección IPv4 destino con el prefijo “0::FFFF:0:0:0/96”, traduce la cabecera IPv4 en una IPv6. Luego la cabecera IPv4 es removida y reemplazada por la IPv6. Cuando el SIIT recibe un paquete IPv6 que contiene una dirección IPv6 destino mapeada a IPv4 (0::FFFF:a.b.c.d) traduce la cabecera IPv6 a una cabecera IPv4. Luego la cabecera IPv6 es removida y reemplazada por la IPv4. En cada caso luego de ser removida y reemplazada por la nueva el paquete es enviado a su destino.

- No se realiza un control del estado, por lo que por cada paquete se debe realizar la traducción de la cabecera IP.

- Este mecanismo requiere una dirección IPv4 temporal por cada nodo. Dichas direcciones son obtenidas por la pila de direcciones IPv4 que posee el mecanismo NAT-PT. No son necesarias las direcciones compatibles con IPv4.

3.5.6 BIS (*Bump In The Stack*)

Este mecanismo permite a un nodo que solo implementa IPv4 su comunicación con otros nodos que tienen soporte solo para IPv6 o solo para IPv4. Es útil debido a que permite a aplicaciones IPv4, que de ninguna forma

pueden ser actualizadas al protocolo IPv6, su comunicación con nodos IPv4 e IPv6.

Este mecanismo se basa en 3 componentes que deben ser agregados en cada nodo que desee comunicación con nodos ya sea IPv6 o IPv4. Adicionalmente de los tres componentes, en cada nodo debe existir una pila para el protocolo IPv4 y otra para el IPv6, es decir, cada nodo debe ser un nodo dual que implementa ambas pilas de protocolos. Los 3 componentes son los siguientes:

- Traductor. Utiliza el mecanismo SIIT para traducir paquetes IPv6 en IPv4 y viceversa. Cuando este recibe un paquete IPv4 traduce la cabecera IPv4 en una IPv6 y envía el paquete modificado a la pila IPv6. Al igual un paquete IPv6 es traducido a uno IPv4.

- Extensión para resolución de nombres. Es implementado como una pila DNS dentro del nodo dual. Su función es atender las peticiones de las aplicaciones ejecutadas en el nodo dual. Debido a que pueden existir aplicaciones en el nodo dual que solo trabajan con direcciones IPv4, se supone que el servidor DNS de la red interna solamente resuelve registros “A”. Cuando la aplicación del nodo dual envía una consulta al servidor DNS de la red interna para resolver el registro “A” del nodo con el que desea la comunicación, este componente intercepta la consulta y crea otra para resolver no solamente el registro “A” del otro nodo, sino también su posible registro “AAAA” y la envía al servidor DNS de la red. Si el registro “A” es resuelto se usa la dirección IP devuelta en dicho registro para entablar la comunicación con nodo IPv4 destino.

- Si solamente el registro “AAAA” es resuelto, este componente solicita al “mapeador de direcciones “ una dirección IPv4 que represente a la dirección IPv6 devuelta en el registro “AAAA”, con la que crea un registro “A” que es devuelto a la aplicación.

- Mapeador de direcciones. Maneja un espacio de direcciones IPv4 para vincular temporalmente a direcciones IPv6 de otros nodos. Los vínculos entre las direcciones son almacenados en una tabla de mapeo. Este componente es utilizado cuando se recibe un registro “AAAA” y no tiene un vínculo con una dirección IPv4.

La ventaja de este mecanismo consiste en que permite la comunicación de aplicaciones que no pueden por ninguna forma ser actualizadas al protocolo IPv6.

La desventaja consiste en que este mecanismo es solamente útil cuando la comunicación entre los nodos es *unicast*. Una comunicación *multicast* no debe utilizar este mecanismo.

3.5.7 Socks64

Este mecanismo permite a un nodo IPv4 o IPv6 su comunicación con otros nodos IPv4 o IPv6 ubicados físicamente en redes distintas. Permite a un nodo IPv4 o IPv6 comunicarse con otros nodos IPv4 o IPv6. Es de utilidad cuando un nodo solo implementa el protocolo IPv4 o existen aplicaciones en el

que solo implementen el protocolo IPv4 y desea comunicarse con otro nodo que implementa IPv4 o IPv6.

Para permitir la comunicación, se basa en 2 componentes que deben ser agregados. Los 2 componentes son los siguientes:

- "Librería *sock*" en el cliente. Este componente debe ser agregado al nodo interno de la red, que desea la comunicación con otros nodos externos. Al agregar este componente al nodo se le denomina "nodo socksificado". Básicamente este componente es el que permite la utilización de una aplicación IPv4 en el nodo interno con otro nodo externo ya que es colocado antes de la capa de aplicación del nodo. Dentro de esta librería existe una dirección especial denominada "dirección IP falsa", así como una tabla de mapeo.

- "Servidor *sock*". Este componente es el encargado de permitir la comunicación entre el nodo interno de la red y otro nodo externo, esto es, un intermediario entre ambos nodos. Básicamente es un nodo dual que tiene una pila para el protocolo IPv4 y otra para el IPv6. Este componente permite cualquier tipo de comunicación entre nodos, por lo que estos pueden ser nodos que implementen ya sea solo el protocolo IPv4 o solo IPv6.

En este mecanismo la conexión que existe entre el nodo interno de la red y el servidor *sock*, se le denomina "conexión socksificada". La conexión que existe entre el servidor *sock* y el nodo externo es una conexión normal.

Cuando ocurre la comunicación, básicamente existe entre el nodo externo y el servidor *sock* y entre el servidor *sock* y el nodo interno.

La dirección “IP falsa” es usada como una dirección IP destino virtual por una aplicación en el nodo interno de la red. Esta dirección es brindada a la aplicación, que se ejecuta en el nodo interno por la librería *sock*, como supuesta dirección destino del nodo externo con el que desea la comunicación. Esta dirección nunca es utilizada en la comunicación real.

Dentro de la librería *sock* se mantiene un vínculo entre la dirección real y el nombre lógico del nodo externo. Dicho vínculo es almacenado en la tabla de mapeo existente dentro de la librería *sock*.

En el momento en que el nodo interno de la red establece la comunicación con el servidor *sock*, se verifica la dirección IP destino que fue brindado a la aplicación como dirección destino del nodo externo. Si dicha dirección pertenece a las direcciones previamente asignadas dentro de la librería *sock* como direcciones falsas, se manda el nombre lógico del nodo externo al servidor *sock* para que obtenga la dirección IP verdadera del nodo externo. La verdadera dirección del nodo externo es resuelta por el servidor DNS interno de la red. Con la dirección verdadera se establece la comunicación entre el servidor *sock* y el nodo externo.

3.5.7.1 Ventajas y desventajas

Las ventajas de la utilización del mecanismo socks64 se resumen en:

- Para redes en donde se desea probar el protocolo IPv6, es un mecanismo útil ya que permite a través de un solo nodo interno de la red hacer pruebas de dicho protocolo.

- Es un mecanismo que provee sistemas de autenticación adecuados para evitar resultados inesperados.

Las desventajas de la utilización del mecanismo socks64 se resumen en:

- Para cada nodo que desee una comunicación con nodos externos se debe agregar la librería *sock*.

- Es un mecanismo de traducción muy costoso respecto de los recursos en el servidor.

- La comunicación solo puede ser iniciada por un nodo interno, por lo que un nodo externo no puede iniciar una comunicación con un nodo de la red.

3.5.8 TCP/UDP *Relay* (Traductor de capa de transporte)

Este mecanismo permite a un nodo que solo implementa IPv6 el intercambio de información con nodos que tienen soporte solo para IPv4. Es un mecanismo adecuado para nodos que hayan sido actualizados hacia el protocolo IPv6 pero aún desean tener comunicación con nodos que solo soportan el protocolo IPv4. También es denominado TRT por su nombre en ingles (*Transport Relay Translator*)

Para permitir la comunicación, este mecanismo se basa en un componente que funciona como intermediario entre los nodos involucrados en la comunicación denominado “sistema de retransmisión TCP”. Cuando un nodo interno de la red IPv6 intenta iniciar la comunicación con un nodo externo a través de una conexión TCP, dicha conexión es enviada hacia el sistema de retransmisión. Debido a que el sistema de retransmisión no conoce la dirección IPv4 del nodo externo, realiza una conexión TCP con el nodo interno de la red para obtener dicha dirección. Luego de obtener la dirección IPv4 del nodo externo, el sistema de retransmisión establece una segunda conexión con el nodo externo de la red. En el momento de establecidas las 2 conexiones TCP, este componente intermediario retransmite trafico del nodo externo al interno y viceversa.

Este mecanismo se basa en un prefijo IPv6 para determinar el momento en que un nodo interno IPv6 desea comunicarse con un nodo IPv4. Se le denomina “prefijo *dummy*” y se representa como C6::/64. Los 64 bits del prefijo pueden ser sustituidos por cualquier espacio de direcciones asignados a la red interna. Si por ejemplo, el prefijo de la red es: FECO:0:0:1::/64 y la dirección del

nodo IPv4 externo es: 10.1.1.1, entonces la dirección del nodo externo se representaría como: FECO:0:0:1::10.1.1.1.

Cuando el nodo interno desea comunicarse con el externo, la conexión TCP es enviada hacia el sistema de retransmisión y capturada por este. En este punto se crea una nueva conexión TCP entre el sistema de retransmisión y el nodo interno para la obtención de la dirección IPv4 del nodo destino. Para la obtención de la dirección IPv4 del nodo externo, el sistema de retransmisión observa los 32 bits de menor orden (los de la izquierda). Luego se crean las 2 conexiones TCP para iniciar la retransmisión de información entre ambos nodos internos y externos. La dirección IPv4 del nodo externo puede ser obtenida de varias formas: guardada previamente en el nodo interno en una tabla de mapeo, una implementación especial en el DNS de la red interna, etc.

3.5.8.1 Ventajas y desventajas

La principal ventaja de la utilización de este mecanismo se resumen en que no necesita modificaciones extras en los nodos internos de la red, así como los nodos externos como sucede en otros mecanismos.

La principal desventaja de la utilización de este mecanismo se resume en que solo soporta tráfico bidireccional, esto es, una comunicación en donde ambos nodos respondan a las peticiones del otro nodo.

3.5.9 CIDR (Enrutamiento ínterdominios sin clases)

Actualmente para solucionar el problema de la escasez de direcciones IPv4 se utiliza el mecanismo CIDR. Este mecanismo trata de solucionar temporalmente el problema del desperdicio de direcciones IPv4, el cual es ocasionado por una mala asignación de redes tipo A, B o C a las organizaciones hechas a los largo de la historia del protocolo IPv4. Además este mecanismo trata solucionar el problema debido al crecimiento de las tablas de ruteo que poseen los *routers* de Internet.

En el momento de creación de este mecanismo, existían aproximadamente dos millones de redes tipo C aún sin asignar a organizaciones. El concepto de este mecanismo, es repartir clases tipo C en una forma variable basado las redes de tipo C sin asignar. Por ejemplo, si una organización necesita 2,000 direcciones IPv4, se le asigna un bloque de 2,048 direcciones IPv4, que es el equivalente a 8 redes tipo C contiguas. (2000/256 = 8 aprox). De esta forma no es necesario asignarle una red tipo B, en la cual habría un gran desperdicio de direcciones IPv4, ya que de las 65,536 solamente utilizaría 2,048. La asignación de redes tipo C, fue ordenada para tener un mejor control, sobre las direcciones IPv4. La asignación quedo de la siguiente manera:

Tabla VI. Asignación de direcciones IPv4 para las regiones del mundo

Región	Rango de direcciones IPv4
Europa	194.0.0.0 a 195.255.255.255

Continuación

Región	Rango de direcciones IPv4
Europa	194.0.0.0 a 195.255.255.255
Norteamérica	198.0.0.0 a 199.255.255.255
Centro y Sudamérica	200.0.0.0 a 201.255.255.255
Asia y el Pacífico	202.0.0.0 a 203.255.255.255
Reservadas	204.0.0.0 a 223.255.255.255

Sin un requerimiento extra, este mecanismo podría generar el problema del aumento en las tablas de *ruteo*. Debido a que cada dirección tipo C de una organización debería ser almacenada en las tablas de ruteo, se generaría un aumento en de entradas en ellas. Para solucionarlo se requiere que las direcciones tipo C sean contiguas, así para identificar una red basta con conocer el número de redes clases C asignadas y la dirección IPv4 de la primera, con lo cual se consigue el número de entradas que se deben asignar en las tablas de ruteo.

Cada dirección IPv4 tiene vinculada una mascara dentro de las tablas de ruteo. Las mascaras son útiles para el *router* para poder diferenciar las direcciones IPv4 almacenadas en dichas tablas. Cuando llega información al *router*, este verifica la dirección destino y le aplica una operación lógica AND a una máscara específica. Si el resultado es igual a la dirección IPv4 a la que esta vinculada dicha máscara entonces se puede conocer la red a la que esta dirigida dicha información, en caso contrario se sigue aplicando el método a cada máscara. Este mecanismo se utiliza para todas las direcciones, por lo que

no se necesitan la distinción entre las clases A, B y C para reenviar la información; he de ahí el nombre de este mecanismo.

CIDR no se trata de un mecanismo de transición del protocolo IPv4 hacia el IPv6, es una medida que no resuelve temporalmente los problemas crónicos detectados en Internet.

3.6 Transmisión de IPv6 sobre dominios IPv4 (Túneles 6over4)

Es un mecanismo que permite comunicar nodos IPv6 aislados dentro de una red con el resto de nodos IPv4 de la misma red. Debido a que la transición se realizará de manera progresiva este mecanismo permite a una red que no sea homogénea, respecto a la versión del protocolo IP, la comunicación entre sus nodos. Este mecanismo también es conocido como "*Ethernet* Virtual".

Este mecanismo es utilizado dentro de una red que posea un *router* sin soporte para IPv6. Esta funcionalidad permite a organizaciones que desean adquirir experiencia con IPv6 sin necesidad de cambiar toda la red hacia IPv6. Para poder brindar la comunicación, este mecanismo se basa en:

- Direcciones *unicast* de enlace local

3.6.1 Características

- Permite a nodos aislados con soporte para IPv6 la comunicación con nodos IPv4 dentro de su misma red así como a través una infraestructura IPv4.

- Se necesitan dominios IPv4 que soporten *multicast* para utilizarlos como su enlace local virtual. El enlace virtual es utilizado para mapear las direcciones IPv6 sobre los dominios que soporte *multicast*. Además dicho enlace virtual es utilizado para formar una red IPv6 virtual, esto es, para simular la existencia de una red IPv6.

- En los nodos IPv6 no son necesarias las direcciones IPv6 compatibles con IPv4, para determinar los extremos del túnel, ni túneles configurados.

- En los nodos IPv6 son necesarias las direcciones *unicast* de enlace local. Estas direcciones se forman mediante un prefijo y la dirección IPv4 de la interfaz del nodo. Este prefijo corresponde a la constante de 10 bits que en valor hexadecimal es FE. Los 32 bits menor orden (los de la derecha) de dirección *unicast* de enlace local corresponden a la dirección IPv4 de la interfaz. La unión de ambas partes forman las direcciones *unicast* de enlace local así: FE80::/64+ dirección IPv4 de la interfaz. El mecanismo para la creación de las direcciones *unicast* de enlace local es mediante la autoconfiguración sin estado.

- Los extremos finales del túnel son determinados mediante el mecanismo de descubrimiento de vecindad. Cuando un nodo desea comunicarse con otro nodo, emite una solicitud de descubrimiento de vecindad con la

dirección de multidifusión del nodo destino con el objetivo de solicitar su dirección de nivel de enlace. El nodo origen incluye su propia dirección del nivel de enlace en el paquete de solicitud de forma que el nodo destino pueda almacenar en su *caché* el resultado y, por tanto, no tenga que emitir después su propia solicitud. En respuesta, el nodo destino envía un anuncio de vecindad con su propia dirección de nivel de enlace.

3.6.2 Ventajas y desventajas

Las ventajas de la utilización de túneles 6over4 se resumen en:

- Los túneles 6over4 son establecidos dinámicamente debido a la utilización del descubrimiento de vecindad y sin configuración previa.

- Permite a nodos pertenecientes a una red experimentar con el protocolo IPv6 sin necesidad de realizar la transición de toda la red hacia el protocolo IPv6, inclusive los *routers* internos de la red.

- Son transparentes a nivel de IPv6, por lo cual no afectan a las aplicaciones existentes que trabajan con direcciones IPv4.

La desventaja de la utilización de túneles 6over4 se resumen en:

- Es un mecanismo adecuado únicamente para redes LAN.

3.7 Conexión de dominios IPv6 sobre redes IPv4 (túneles 6to4)

Es un mecanismo útil para unir redes que tengan soporte para IPv6. Para poder brindar la conexión entre dichas redes, este mecanismo se basa en 2 factores los cuales son:

- Direcciones *unicast* globales agregables
- Túneles *router* a *router*

A partir de estos 2 factores, se desprenden una serie de características que identifican a este método.

3.7.1 Características

- Permite a redes IPv6 que se encuentren aisladas la comunicación, a través una infraestructura IPv4, con otras redes IPv6 que también se encuentren aisladas.
- Utiliza un prefijo único para la red IPv6. Este prefijo corresponde a los 48 bits de la topología pública de la dirección unicast global agregable y consta de 2 partes. El prefijo para el TLA y el prefijo para el NLA. En la primera de ambas partes el prefijo es 2002::/16. Con el prefijo del TLA, se forma el prefijo para el NLA, y por lo tanto el prefijo para la red IPv6, es 2002:WWXX:YYZZ:/48. El valor de WWXX:YYZZ es la dirección IPv4

del *router,* interno de la red que se utilizará para la comunicación, representada en IPv6.

- Se utiliza túnel de tipo *router* a *router,* en donde cada extremo del túnel es un nodo IPv6/IPv4, para la conexión de dos redes que deseen intercambiar información en formato IPv6.

- Los extremos finales del túnel son identificados al observar el prefijo de la red IPv6. Al momento de enviar información en formato IPv6 y observar las direcciones IPv6 origen y destino se puede obtener los extremos del túnel. El extremo inicial corresponde a la dirección IPv4 del prefijo de la red origen y el extremo final corresponde a la dirección IPv4 del prefijo de la red destino. Dichas direcciones IPv4 corresponden a las direcciones de los *routers* que forman el túnel.

- Al igual que cualquier túnel el extremo inicial del túnel realiza el encapsulado de la información y el extremo final realiza el descencapsulado de la información con el objetivo de utilizar la infraestructura IPv4 de la Internet actual, razón por la cual se denominan a estos túneles “Conexión de dominios IPv6 sobre redes IPv4”.

3.7.2 Ventajas y desventajas

Las ventajas de la utilización de túneles 6to4 se resumen en:

- Este tipo de túneles se establecen dinámicamente debido a la utilización del prefijo para la red IPv6. El establecimiento dinámico de un túnel entre dos redes se realiza sin una configuración previa en cada uno de los *routers* involucrados.

- Solo se establecen los túneles necesarios en el momento que la conexiones se encuentran activas con una o más redes. A diferencia de los túneles configurados en donde los túneles se encuentran establecidos estáticamente, los túneles 6to4 se establecen solo en el momento en que la conexión se encuentra activa con otra red.

- Son transparentes a nivel de IPv6, por lo cual no afectan a las aplicaciones existentes que trabajan con direcciones IPv4.

Las desventajas de la utilización de túneles 6to4 se resumen en:

- Para redes que se conecten a un ISP con soporte para IPv6 en donde solo el túnel hacia dicho ISP sea necesario, puede que la utilización de un ISP gratuito que se haya más extendido por toda la Internet sea más que necesario.

- Es necesario la obtención de un prefijo único para la red.

3.8 *Tunnel Broker y Tunnel Server*

Este mecanismo permite a nodos IPv6/IPv4 aislados o redes IPv6, la comunicación con nodos IPv6 o redes IPv6. Este mecanismo puede ser visto como un ISP virtual de IPv6, que permite a usuarios que ya tienen conectividad con IPv4 la comunicación con redes IPv6. Se basa en dos componentes para su funcionamiento: *tunnel broker*, *tunnel server*.

- *Tunnel broker* es el lugar en donde un usuario se conecta para registrar y activar túneles configurados. Este componente es el encargado de dar el mantenimiento del túnel, esto es, la creación, modificación y eliminación. Es también el encargado de registrar la dirección IPv6 del usuario así como su nombre dentro del DNS del ISP virtual.

- *Tunnel server* es un *router* dual IPv6/IPv4 que es la frontera entre el ISP virtual y el nodo usuario. Recibe solicitudes del *tunnel broker* para crear, modificar o eliminar los extremos finales de los túneles de los usuarios. Mantiene estadísticas relacionadas a cada túnel activo.

El usuario que desea conectarse al ISP virtual de IPv6, es un nodo conectado hacia la infraestructura IPv4 de la Internet. Para lograr la creación del túnel configurado entre el usuario y el ISP virtual, el usuario previamente debe brindar aceptar la autorización de que desea realizar el túnel. Luego de esto, el usuario debe brindar como mínimo los siguientes parámetros:

- La dirección IPv4 del nodo. Se trata de una dirección IPv4 pública y no una IPV4 privada. En redes que utilicen NAT no funcionará este mecanismo.

- El nombre que será utilizado para registrar al nodo en el DNS del ISP virtual, el nombre para almacenar la dirección IPv6 en el registro AAAA del nodo. La dirección IPv6 será brindada por el ISP virtual al nodo usuario.

- El tipo de cliente del usuario, ya sea un nodo o un *router*. En el caso de un *router* el usuario también deberá brindar información como el número de nodos internos de la red a las cuales les brindará conexión IPv6, esto con el objetivo de asignarle un prefijo IPv6 en lugar de varias direcciones IPv6.

Los pasos de creación del túnel configurado son los siguientes:

- El *tunnel broker* designa al *tunnel server* para que sea el extremo final del túnel.

- El *tunnel broker* elige el prefijo que será asignado al nodo usuario.

- El *tunnel broker* determina el tiempo de vida del túnel. Debido a que existirán túneles que serán creados para ser utilizados por un corto tiempo y luego ya no, se asigna un tiempo de vida al túnel, el cual al cumplirse se elimina el túnel configurado.

- El *tunnel broker* registra en el DNS del ISP virtual, las direcciones IPv6 asignadas al extremo inicial y final del túnel configurado. Estas direcciones deben pertenecer al espacio manejado por el ISP virtual. El tiempo de vida de estas direcciones debe ser relativamente largo para permitir a usuarios obtener una dirección IPv6 semipermanente.

- El *tunnel broker* configura el extremo final del túnel en el ISP virtual.

- El *tunnel broker* genera la información necesaria que utilizará el cliente para generar el extremo inicial del túnel configurado, como los parámetros de configuración del túnel.

La interacción entre un usuario y el *tunnel broker* puede realizarse a través de páginas HTML. El usuario puede llenar una forma en donde ingrese los parámetros para la creación del túnel configurado. Como resultado de esto, el servidor puede responder con la información necesaria para la creación del extremo del túnel en el nodo usuario. Dicha información puede ser un *script* que el usuario simplemente tenga que ejecutar para la creación del extremo del túnel.

3.9 Otros mecanismos de transición

En la actualidad no se ha decidido aún cuál es el mecanismo de transición a utilizar, ya que todos los mecanismos presentan ventajas así como desventajas. Además actualmente se encuentran en fase de desarrollo otros

mecanismos de transición que pueden tomar ideas de los aquí expuestos o tener ideas totalmente nuevas.

4. MIGRACIÓN DE REDES EXISTENTES EN GUATEMALA

4.1 Fases de transición

En general la transición de las redes debería ser de la siguiente forma:

- Primero la transición de redes LAN de empresas.
- Segundo la transición de los proveedores de servicios de Internet (ISP).

Las redes LAN de las empresas deberían ser las primeras en hacer la transición hacia el protocolo IPv6, debido a que actualmente no existen muchas redes en el mundo que manejen el protocolo IPv6. Como consecuencia de ello la cantidad de servicios prestados actualmente basados en el protocolo IPv6 son muy pocos.

Para un ISP actualmente no tendría sentido brindar soporte para IPv6, ya que como se ha dicho, en la actualidad existen muy pocos servicios basados en el protocolo IPv6 que se puedan brindar.

Debido a que la transición se debe llevar a cabo de manera progresiva y gradual, la transición de redes LAN de empresas llevaría a un crecimiento del número de redes que manejen el protocolo IPv6 y obligaría a los proveedores

de Internet a brindar soporte para IPv6. Esto sería debido a que aumentaría la demanda de usuarios que quisieran tener comunicación con redes que manejen el protocolo IPv6 y utilizar sus servicios brindados.

Actualmente en la mayoría de las empresas de Guatemala no existe interés por el protocolo IPv6. El grado de desinterés se debe a la gran cantidad de servicios prestados por el protocolo IPv4 en contraste con la pequeña cantidad de servicios prestados por el protocolo IPv6.

Además actualmente el problema de la escasez de direcciones IP esta temporalmente salvado por *NATs* y *Proxies*. Estos mecanismos son brindados por los ISP para brindar la conexión a Internet. Con el crecimiento de redes con soporte para IPv6 en el mundo se conseguirá un mayor interés de los proveedores de servicio de Internet para realizar la transición y brindar soporte para IPv6 a las redes LAN de las empresas.

Con el crecimiento del mecanismo UMTS que brinda la oportunidad de conectarse a Internet a dispositivos móviles el protocolo IPv6 será totalmente obligatorio para todo ISP que desee brindar la oportunidad a dispositivos móviles estar siempre conectados a Internet. Un ISP deberá realizar la transición hacia IPv6 si desea brindar una clase de servicio como esta, esto es, ISPs como Comcel, Terra y otros deberán hacer la transición hacia el protocolo IPv6.

4.1.1 Fases de transición para redes LAN

Una empresa debería realizar la transición de su red LAN en las siguientes fases:

- En la primera fase seguir conectado al ISP con soporte para IPv4 y hacer uso de túneles para la transmisión de información transmitida por infraestructuras IPv4 como lo es la Internet actual. En el transcurso de esta fase debe esperar a que el ISP tenga soporte para IPv6.

- La segunda fase se da cuando el ISP ofrece soporte solamente para el protocolo IPv6, pero aún es necesario tener comunicación con otras redes que tengan solamente soporte para IPv4. En esta fase se debería hacer uso de túneles para la transmisión de la información a través de infraestructuras IPv6. En esta fase, se ofrecen una gran cantidad de servicios con IPv6 comparados con la pequeña cantidad de servicios prestados con IPv4.

4.1.2 Fases de transición para ISPs de Guatemala

- En la primera fase debería brindar conexión tanto para IPv4 como para IPv6 a sus clientes mediante el uso de túneles hacia *backbones* IPv6. El acceso que sus clientes deberían hacer a ellos (ISPs) debería hacerse mediante algún mecanismo de traducción.

- En la segunda fase debería usar conexiones nativas a *backbones* IPv6, esto es, no debería utilizar ningún mecanismo de transición para conectarse hacía *backbones* IPv6. En esta fase también el acceso que sus clientes deben hacer a ellos se debe hacer mediante algún mecanismo de traducción, ya que aunque existan clientes cuyas redes son puramente basadas en el protocolo IPv6 aún existirán servicios basados en el protocolo IPv4 que deseen ser usados.

4.2 Transición de un ISP IPv4 a IPv6

Según estimaciones, la fecha límite para la implantación del protocolo IPv6 debe ser en el 2005. Dicha estimación se basa en que esa fecha ya no existirán direcciones IPv4 disponibles debido al crecimiento exponencial del número de usuarios que utilizan Internet. Por tal razón los mecanismos NAT o Proxies utilizados por los proveedores de servicios de Internet no serán útiles debido a que dichos mecanismos utilizan una dirección IPv4 pública para brindar servicio a la red de una empresa.

En el momento del crecimiento de la demanda del protocolo IPv6 un ISP poseerá clientes que accedan a Internet por medio del protocolo IPv4. La meta principal para un ISP será brindar a sus clientes acceso a los servicios brindados por el protocolo IPv6.

Actualmente dentro del entorno guatemalteco los principales proveedores de Internet son los siguientes:

Tabla VII. ISPs de Guatemala y su vínculo con el protocolo IPv6

ISP	Utiliza IPv6
Comcel	No
Terra	No
Teléfonica	No
Telgua	No
OSI Instared	No

En la tabla anterior se puede observar que ninguno de los proveedores principales dentro del entorno guatemalteco utiliza el protocolo IPv6 para la comunicación que requieren sus clientes.

Cabe recordar que los componentes principales involucrados hacia la transición a IPv6 son *routers*, nodos cliente y el sistema DNS utilizado dentro de la red. En el entorno guatemalteco la mayoría de los ISP utilizan el mismo fabricante de *routers*, los sistemas operativos utilizados dentro de sus servidores y nodos son los más populares del mercado y el sistema de DNS utilizado es el mismo. Los componentes mas utilizados por los ISPs de Guatemala se describen a continuación:

Tabla VIII. Componentes de la transición utilizados por ISPs de Guatemala

Fabricante Router	Cisco

Continuación

Sistema operativo utilizado en nodos y servidores	Microsoft Windows ® Linux
Servidor DNS	Microsoft Windows ® Linux

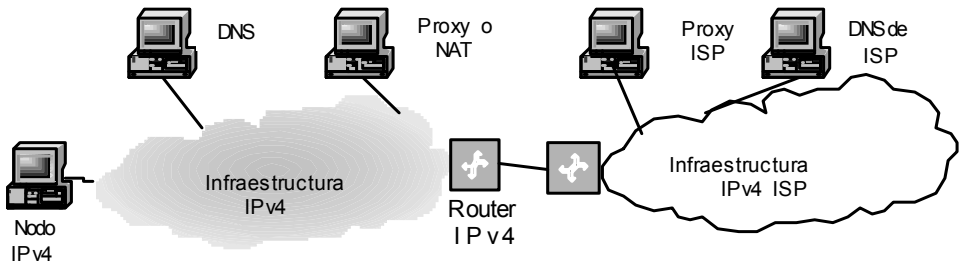
Con los datos anteriores se puede describir el procedimiento que debe realizar un ISP dentro del entorno guatemalteco para realizar la transición hacia IPv6. Dicho procedimiento se describe más adelante.

4.3 Acceso actualmente a Internet a través de IPv4

El acceso a Internet actualmente esta basado en mecanismos traductores denominados NAT o *Proxies*. Estos mecanismos se configuran en un nodo de la red, al cual se le denomina servidor *proxy*. A través de este servidor un nodo perteneciente a una red LAN se comunica con otras redes que forman la infraestructura de Internet.

Para permitir la comunicación un proveedor de servicios de Internet tiene asignado un rango de direcciones IPv4 públicas. Cada una de las direcciones pertenecientes a dicho rango es asignado a cada empresa que desee comunicarse a través de Internet, por lo tanto, cada empresa tiene asignada únicamente una dirección IPv4 pública. Dicha dirección es utilizada por el servidor *proxy*, para realizar la traducción de las direcciones IPv4 privadas de la red a la dirección IPv4 pública. El método de acceso actual que utilizan las empresas para lograr el acceso a Internet es el siguiente:

Figura 14. Acceso actual a Internet en Guatemala



A pesar de solucionar temporalmente la escasez de direcciones IPv4 con mecanismos como NAT o *Proxy*, el número de direcciones IPv4 disponibles para asignarlas a ISPs tiene una fecha límite.

4.4 Probable acceso a Internet a través de IPv6

El acceso a Internet con el protocolo IPv6 es una solución al problema de escasez de direcciones IPv4 y al cumplimiento de la meta de permitir la comunicación a través de cualquier dispositivo electrónico. Un ISP debería seguir una serie de pasos para permitir a sus clientes la conectividad a redes que utilizan IPv6 y a los servicios prestados por dicho protocolo.

4.4.1 ¿Cómo proceder a la transición en un ISP?

La serie de pasos que debería seguir un proveedor de servicios de Internet para realizar la transición del protocolo IPv4 al IPv6 son los siguientes:

- Debe obtener un rango de direcciones IPv6 que utilizará para brindarlas a sus clientes. A través de la autoridad encargada de la delegación de direcciones IPv6 a ISPs debería obtener el rango de direcciones que utilizará.

- Debe realizar la actualización de su infraestructura del DNS para soportar registros AAAA. Los servidores DNS que forman parte de la infraestructura deben ser actualizados para soportar direcciones IPv6.

- Debe actualizar los componentes de la red. Los componentes encargados de servir peticiones de los clientes que desean conectarse a redes que utilizan IPv6 deben ser actualizados. Dentro de estos componentes se encuentran los *routers*.

4.4.2 Posibles soluciones

Sin la utilización de los mecanismos de transición un ISP puede brindar conexión a redes que solamente utilizan el protocolo IPv6 con otras redes que utilizan IPv6.

Mediante la utilización de los diferentes mecanismos de transición un ISP puede brindar a sus clientes que poseen redes que utilizan IPv4 y a redes que utilizan IPv6 conectividad a redes que utilizan IPv6.

Cualquier mecanismo de transición puede ser utilizado por un ISP que desee brindar conectividad a redes que utilizan IPv6. En la presente se muestran tres soluciones que puede utilizar un ISP que desea realizar la transición.

4.4.2.1 Red IPv6 dedicada

Esta solución no utiliza ningún mecanismo de transición para brindar conectividad a sus clientes que desean utilizar los servicios prestados por el protocolo IPv6.

Básicamente es una solución en donde la infraestructura del ISP utiliza únicamente el protocolo IPv6 para la comunicación. Los *routers* solamente son capaces de retransmitir información en formato IPv6 y rechazan la que se encuentra en formato IPv4. Además sus servidores de DNS solamente utilizan direcciones IPv6.

Actualmente no es una solución apropiada para los ISPs guatemaltecos ya que el número de empresas del mercado que están interesadas en el protocolo IPv6 es casi nula. Además una solución de este tipo en términos de costos es una solución muy cara. Es una solución a largo plazo en donde en el

mercado guatemalteco existan muy pocas redes que utilicen el protocolo IPv4 para la comunicación.

4.4.2.2 Uso de túneles

Básicamente esta solución permite a redes que tienen soporte para IPv6 la comunicación con otras redes que también utilizan dicho protocolo. Se puede ver, como una interconexión de redes aisladas que utilizan el protocolo IPv6. Para interconectar las redes IPv6 se debe agregar *routers* adicionales que soporten el protocolo IPv6 a la infraestructura del ISP. Los túneles configurados son utilizados para interconectar a las redes que utilizan IPv6. Debido a que al inicio de la transición existirán pocas redes en Guatemala que utilicen el protocolo IPv6 no será necesario actualizar los servidores DNS del ISP para que soporten direcciones IPv6. Las rutas de las redes aisladas los *routers* adicionales las sabrán a través de rutas estáticas, esto es, a través de túneles configurados.

Esta solución no permite únicamente la comunicación entre redes que utilizan IPv6. Los *routers* de los que dispone el ISP que solamente manejan el protocolo IPv4 permanecen funcionales. Al permanecer estos *routers* dentro de la infraestructura, el ISP puede atender a usuarios que solamente utilizan el protocolo IPv4, los que solamente utilizan el protocolo IPv6, y los que utilizan ambos protocolos dentro de su red LAN.

Con esta solución los antiguos usuarios aún permanecen solicitando el servicio del ISP y nuevos clientes que utilizan el protocolo IPv6 son atendidos. Esta es la solución más adecuada a corto plazo para los ISPs de Guatemala, debido a que al principio existirán pocas redes que utilicen el protocolo IPv6. Es una solución barata comparada con una solución de un ISP con una red IPv6 dedicada.

4.4.2.3 Redes con pila doble

Esta solución en el sentido lógico brinda los mismos beneficios de la solución mediante el uso de túneles. Permite a un ISP atender a las redes LAN que solamente utilizan el protocolo IPv4, las que solamente utilizan el protocolo IPv6 y las que utilizan ambos protocolos.

Básicamente se diferencian ambas soluciones en que en esta no se agregan *routers* adicionales a la infraestructura del ISP. En esta solución el ISP debe realizar la actualización de los *routers* y del los servidores de DNS para que soporten tanto direcciones IPv4 como IPv6.

En el entorno guatemalteco la mayoría de *routers* utilizados pertenecen al mismo fabricante por lo que no existe el problema de heterogeneidad de *routers*. Los *routers* pertenecen al fabricante Cisco. Para los servidores de DNS tampoco existe el problema ya que la mayoría utiliza servidores implantados en un entorno Windows. En el entorno guatemalteco es una solución a mediano plazo para los ISPs.

4.5 Compañía y la conectividad IPv6

Actualmente dentro del entorno de las compañías en Guatemala que utilizan Internet para la comunicación con otras redes ubicadas a lo largo del mundo, el interés por el protocolo IPv6 es casi nulo. A continuación se muestra las compañías relacionadas sobre el presente tema.

Tabla IX. Compañías de Guatemala y su vínculo con el protocolo IPv6

Compañía	Utiliza IPv6
Unitel	No
Sefisa	No
Cablenet	No
New Com Communications Guatemala	No

En la tabla anterior se puede observar el grado de desinterés que existe actualmente por el protocolo IPv6 en las compañías guatemaltecas como protocolo de comunicación. En el caso de Unitelsa es una compañía que se dedica a las telecomunicaciones y brinda servicios como voz y videoconferencia sobre IP, acceso a Internet, etc. Sefisa es una compañía que se dedica a brindar servicios de seguridad en Internet. *New Com Communications* Guatemala es una empresa que se dedica a brindar conexión a Internet.

Al igual que en el caso de un ISP, las compañías en su mayoría utilizan dentro de sus redes LAN componentes del mismo fabricante, esto es, los componentes involucrados en la transición hacia IPv6 son en su mayoría del mismo fabricante.

Los componentes mas utilizados por las compañías dentro de las redes LAN se describen a continuación:

Tabla X. Componentes de la transición utilizados por las compañías de Guatemala

Router	Cisco
S.O utilizado en nodos y servidores	Microsoft Windows ® Linux
Servidor DNS	Microsoft Windows ® Linux

Según los datos anteriores se puede describir el procedimiento que debe realizar una compañía dentro del entorno guatemalteco para realizar la transición hacia IPv6. Dicho procedimiento se describe más adelante.

Al igual que un ISP una compañía debería seguir una serie de pasos para realizar la transición de su red LAN y tener conectividad con redes que utilizan el protocolo IPv6.

4.5.1 ¿Cómo proceder a la transición de una red LAN?

La serie de pasos que debería seguir una compañía guatemalteca para realizar la transición del protocolo IPv4 al IPv6 en su red LAN son los siguientes:

- Debe elegir que nodos de la red serán actualizados hacia el protocolo IPv6. Una compañía puede dentro de los nodos que pertenecen a su red LAN brindar conectividad a ciertos nodos o al total de ellos. Una compañía por ejemplo puede realizar pruebas, mediante algún mecanismo de traducción, al protocolo IPv6. Además puede ser el caso de que alguna norma de la empresa permita la conectividad solamente a ciertos nodos de la empresa.

- Debe obtener las direcciones IPv6 que utilizará para la comunicación. Las direcciones IPv6 que utilizará para la comunicación puede obtenerlas mediante un ISP que utilice IPv6.

- Debe actualizar la infraestructura de los servidores DNS de la red LAN para soportar registros del tipo “AAAA”. Los servidores de DNS que se utilicen en la empresa ya sea primarios o secundarios deben ser actualizados para soportar direcciones IPv6.

- Debe realizar la actualización de los *routers* que utilizará para la comunicación con otras redes que utilicen el protocolo IPv6. La compañía debe seleccionar los router que utilizará para la comunicación.

4.5.2 Posibles soluciones

Al igual que para los ISPs para llevar a cabo la transición de las redes LAN de las compañías guatemaltecas es posible realizarla mediante la utilización de mecanismos de transición. La utilización de alguno de los mecanismos de transición, permitirá a una red la comunicación con redes que utilizan el protocolo IPv6, así como con redes que utilizan el protocolo IPv4.

Sin la utilización de los mecanismos de transición la red LAN de una compañía solamente se podrá comunicar con redes que soporten el protocolo IPv6. A continuación se muestran tres soluciones que puede utilizar una compañía para llevar a cabo la transición de la red LAN del protocolo IPv4 al IPv6.

4.5.2.1 Red IPv6 dedicada

La idea de esta solución es que la red LAN de la compañía solamente trabaje con el protocolo IPv6 para su comunicación a través de Internet.

Esta solución implica que los componentes involucrados en la transición, manejan únicamente direcciones IPv6. El *router* de la red LAN únicamente tiene direcciones IPv6 dentro su tabla de ruteo, además cualquier información en formato IPv4 es rechazada debido a que dichos formatos no son compatibles. Los servidores DNS de la red solamente tienen soporte para registros de tipo

“AAAA”. Los nodos internos de la red solamente implementan la pila del protocolo IPv6 y no implementan la pila del protocolo IPv4.

Es una solución a largo plazo para las redes LAN de las compañías guatemaltecas ya que actualmente la cantidad de servicios prestados, aplicaciones creadas, dispositivos internos de la red se basan en el protocolo IPV4 y en el largo plazo el protocolo IPv6 será el más utilizado para la comunicación. En términos de costos es una solución muy cara.

En el largo plazo a esta solución puede ser agregado algún mecanismo de transición que le permita a redes que solamente utilizan el protocolo IPv6 su comunicación con redes que solamente utilicen el protocolo IPv4, esto debido a que aún existirán redes que solamente trabajen con el protocolo IPv4.

4.5.2.2 Uso de túneles

Es una solución que permite a la red de una compañía la comunicación con cualquier tipo de red sin cambiar todos los componentes involucrados en la transición. Los servidores DNS de la red no son cambiados para que soporte IPv6.

Para lograr la conectividad a redes IPv6, una compañía guatemalteca puede agregar por lo menos un *router* que soporte IPv6 o actualizar alguno de los que ya existan en la red.

Mediante la utilización de túneles configurados el *router* de la red puede crear rutas estáticas a redes IPv6 o a algún ISP que tenga soporte para IPv6. Actualmente existe un ISP a nivel mundial que utiliza el protocolo IPv6 denominado *6bone*.

En el corto plazo una compañía guatemalteca puede utilizar un ISP del mercado guatemalteco para lograr la conectividad con redes IPv4 y un ISP mundial para lograr la conectividad con redes IPv6.

Para permitir que un nodo interno de la red pueda intercambiar información en formato IPv6, dicho nodo debe ser actualizado para que soporte el protocolo IPv6 y se debe crear un túnel configurado entre el nodo interno y el *router* de la red que utilice dicho protocolo. Es una solución muy simple y barata comparada con una red IPv6 dedicada.

4.5.2.3 Redes con pila doble

En esta solución los nodos internos, los servidores de DNS y los *routers* de la red LAN son capaces de manejar direcciones IPv4 e IPv6.

Los *routers* utilizados para la comunicación a través de Internet pueden recibir y enviar paquetes en ambos formatos. Los servidores DNS de la empresa son capaces de manejar ambos tipos de direcciones. Además los

nodos internos de la red tienen asignadas dos direcciones para la comunicación.

Esta solución es la mas adecuada en el mediano plazo para las empresas guatemaltecas que desean tener comunicación con cualquier tipo de red. En el mediano plazo existirán proveedores de servicios de Internet en el mercado guatemalteco que brinden tanto conexión a redes IPv6 como a IPv4.

4.6 Actualización de los componentes de la transición

Dentro del entorno guatemalteco la mayoría de los componentes involucrados en la transición tienen la característica de ser los mas populares del mercado en cada una de sus áreas. Dichos componentes se refieren a *routers*, servidores de DNS y nodos internos de la red.

4.6.1 Componente *router*

Dentro del entorno guatemalteco la mayoría de los *routers* utilizados por las empresas dentro sus redes LAN pertenecen al fabricante Cisco. En un gran porcentaje las empresas a las que fue realizado el estudio utilizan *routers* de dicho fabricante.

Una empresa guatemalteca que desee tener conectividad con redes que utilizan el protocolo IPv6 puede optar por 2 opciones: adquirir un nuevo *router*

que soporte direcciones de este tipo o revisar si el actualmente utilizado dentro de su red puede ser actualizado.

Los *routers* del fabricante Cisco utilizan un sistema operativo denominado “Cisco IOS Software”. Este sistema operativo como cualquier otro tienen varias versiones, cada versión tiene varios parches y varios *releases*. Además este fabricante tiene varios modelos de *routers*. En un modelo específico pueden ejecutarse varias versiones de IOS pero otras no pueden ejecutarse.

El protocolo IPv6 no es posible utilizarlo en todos los IOS que han sido diseñados por Cisco. La nomenclatura utilizada para referirse a un IOS es la siguiente:

n1. n2(n3) en donde n1 es el numero de versión, n2 es el número de parches que posee la versión y n3 corresponde al *release* de la versión.

El protocolo IPv6 es soportado desde los siguientes IOS:

- 12.0(21) ST
- 12.0(22) S
- 12.2(2) T

La versión 12.0(22) ST fue unida con la versión 12.0(22) S por lo cual no existen nuevos *releases* para dicha versión. El protocolo IPv6 es soportado por los nuevos *releases* de las versiones 12.0(22) S y 12.2(2) T.

Los IOS anteriores pueden ejecutarse en un modelo específico de un *router*. La siguiente tabla muestra un listado de los modelos de *routers* de Cisco y las versiones de IOS que pueden ser ejecutadas en cada uno de los modelos.

Tabla XI. IOS necesarios para la utilización en *routers* Cisco del protocolo IPv6

Modelo	12.0 ST	12.0 S	12.2 T
Cisco 800	-	-	12.2(2) T
Cisco 1400	-	-	12.2(2) T
Cisco 1600	-	-	12.2(2) T
Cisco 1700	-	-	12.2(2) T
Cisco 2500	-	-	12.2(4) T
Cisco 2600	-	-	12.2(2) T
Cisco 3600	-	-	12.2(2) T
Cisco 3700	-	-	12.2(8) T
Cisco 4000	-	-	12.2(2) T
Cisco 7100	-	-	12.2(2) T
Cisco 7200	-	-	12.2(2) T
Cisco 7500	-	-	12.2(2) T
Cisco 12000	12.0(21) ST	12.0(22) S	-

Con la tabla anterior una empresa guatemalteca puede observar la versión que necesita para el modelo del *router* que utilizara para utilizar le protocolo IPv6.

La versión del IOS necesario para el *router* debe ser descargada desde el portal de Cisco. En dicho portal a las versiones se les denomina imágenes, así que se debe acudir al portal para descargar la imagen del IOS necesario. Actualmente para descargar una imagen el requisito es que debe ser una persona que posea un usuario en dicho portal. Luego de descargada la imagen el último paso consiste en actualizar la antigua versión del IOS por la nueva versión.

4.6.1.1 Activar el ruteo IPv6

Debido a que dentro del IOS el ruteo IPv6 se encuentra por defecto desactivado, el siguiente paso consiste en activar esa opción. Para activar el reenvío de tráfico IPV6 globalmente dentro del *router*, se debe utilizar el siguiente comando en el modo global de configuración:

Router(config)# **ipv6** *unicast-routing*

Las palabras que aparecen en negrita se refieren a un comando del IOS o una palabra reservada.

4.6.1.2 Configurar direcciones IPv6

Para asignar una dirección IPv6 en una interfase del *router*, se deben usar los siguientes comandos en el modo global de configuración.

Router(config)# ***interface*** tipo_de_interfase numero_interfase
Router(config-if)# **ipv6** ***address*** prefijo_dirección_IPv6/longitud_prefijo **eui-64**

En este comando se debe indicar el prefijo IPv6 asignado a la red. El parámetro "eui-64" asigna automáticamente a los 64 bits de menor orden (los de la derecha) de la dirección IPv6 el identificador de interfaz que posee dicha interfaz. Un ejemplo para activar el ruteo IPv6 y configurar una dirección en una interfase se muestra a continuación:

Router(config)# **ipv6** *unicast-routing*
Router(config)# **interface** *ethernet* 0
Router(config-if)# **ipv6** ***address*** 3ffe:c00:c18:1::/64 eui-64

4.6.1.3 Router IPv6/IPv4

Para habilitar la opción a una interfase para que maneje tanto direcciones IPv4 como IPv6, se deben ejecutar los siguientes comandos en el modo global de configuración:

Router(config)# **ipv6** *unicast-routing*

Router(config)# ***interface*** tipo_interfase-numero_interfase
Router(config-if)# **ipv6 *address*** prefijo_dirección_IPv6/longitud_prefijo
Router(config-if)# **ipv *address*** direccion_IPv4 mascara

Un ejemplo de lo anterior se muestra a continuación:

Router(config)# **ipv6** *unicast-routing*
Router(config)# **interface** *Ethernet*0
Router(config-if)# **ipv6 *address*** 3ffe:b00:c18:1::3/64
Router(config-if)# **ip *address*** 192.168.99.1 255.255.255.0

4.6.1.3 Creación de un túnel configurado r*outer* a r*outer*

Debido a que en Guatemala la solución a corto plazo consiste en la utilización de túneles configurados a continuación se muestran los comandos que se deben ejecutar en el modo global de configuración:

Router(config)# ***interface*** **tunnel** numero_tunel
Router(config-if)# **ipv6 *address*** prefijo_dirección_IPv6/longitud_prefijo
Router(config-if)# ***tunnel*** **source** tipo_interfase numero_interfase
Router(config-if)# ***tunnel destination*** direccion_IPv4
Router(config-if)# ***tunnel mode*** **ipv6ip**

Un ejemplo de lo anterior se muestra a continuación:

Router(config)# ***interface tunnel*** 0
Router(config-if)# **ipv6 *address*** 3ffe:b00:c18:1::3/127
Router(config-if)# ***tunnel source*** ethernet 0
Router(config-if)# ***tunnel destination*** 192.168.30.1
Router(config-if)# ***tunnel mode*** **ipv6ip**

4.6.2 Componente nodo

En el entorno guatemalteco la mayoría de las empresas utilizan dentro de los nodos internos de la red, así como en los servidores los sistemas operativos más populares del mercado. Los sistemas operativos más utilizados son Windows y Linux.

Una empresa guatemalteca que desee utilizar el protocolo IPv6 dentro de su red interna debe revisar los sistemas operativos que utilizan sus nodos y servidores. A partir de ello, deberá actualizarlos o no.

4.6.2.1 Nodos Linux

Para permitir a un nodo la utilización del protocolo IPv6 en cualquier tipo de Linux, debe tener como mínimo un kernel 2.2.x. El parámetro “x” indica que puede ser cualquier *release*. Si no se cuenta con la versión mínima debe descargarse desde el portal de Linux esta versión o la más actual.

Con el cumplimiento del requisito anterior el siguiente paso consiste en la compilación del nuevo kernel. Antes del proceso de compilación se deben habilitar las siguientes opciones:

 # make menuconfig

Code maturity level options

[*] *Prompt for development and/or incomplete code/drivers*

Networking options

<*> *Packet socket*

[*] *Kernel/User netlink socket*

[*] TCP/IP *networking*

<*> The IPv6 protocol (*EXPERIMENTAL*)

<*> IPv6: enable EUI-64 token format (*NEW*)

<*> IPv6: disable provider based addresses (*NEW*)

Luego de habilitadas se procede a compilar el nuevo *kernel*, a instalarlo y configurarlo dentro del cargador de Linux.

4.6.2.1 Nodos Microsoft Windows ®

Para permitir a un nodo o a un servidor de la red la utilización del protocolo IPv6 en el sistema operativo Microsoft Windows ®, debe tener como mínimo una versión 2000 o NT 4.0. Para las versiones 95, 98 este fabricante no

brinda soporte, esto es, los nodos de la red que posean dichas versiones solo pueden utilizar el protocolo IPv4 para la comunicación.

La solución que brinda Microsoft ® es denominada "*Microsoft Research IPv6 Network Protocol Stack (*MSRIPv6*)* ". Actualmente la última versión de esta solución es la 1.4 y puede ser descargada desde el url:

http://msdn.microsoft.com/downloads/sdks/platform/tpipv6/download.asp

Los pasos para la instalación del MSRIPv6 son los siguientes:

- Descomprimir el archivo descargado a un directorio (p.e. c:*IPv6Kit*)
- Ir a panel de control
- Seleccionar "Conexiones de red"
- Dar *click* derecho sobre "conexión de red local" y seleccionar propiedades
- Oprimir el botón "Instalar"
- Seleccionar protocolo y oprimir el botón "Agregar"
- Seleccionar del listado el protocolo "MSR IPv6 *Protocol*" y oprimir el botón "H*ave disk*".

- Escribir la ruta completa en donde fue descomprimido el archivo (p.e. p.e. c:*IPv6Kit*) y oprimir el botón “Ok”

- En este punto el archivo es instalado.

Al instalar este *software* se agrega una pila que es encargada de manejar el protocolo IPv6 y la pila IPv4 queda aún funcional, esto es, el nodo se convierte en un nodo IPv6/IPv4 capaz de manejar ambos protocolos.

El *software* crea 2 interfaces obligatorias para el nodo, una por cada dirección IPv4 asignada al nodo y una por cada adaptador de red que posea el nodo. Para cada interfase automáticamente asigna la dirección IPv6 correspondiente. A continuación se muestra un nodo con una dirección IPv4 y un adaptador de red:

- Interfase 1, contiene la dirección IPv6 de retorno (*loopback adress*)

- Interfase 2, para la creación de túneles configurados, automáticos, 6to4

- Interfase 3, contiene la dirección IPv6 de enlace local que representa a una dirección IPv4 asignada al nodo

- Interfase 4, contiene la dirección IPv6 de enlace local del adaptador de red. Dicha dirección se obtiene automáticamente de la dirección MAC del adaptador de red.

En la versión XP el funcionamiento es el mismo que en la versión 2000 y el soporte para IPv6 ya viene incorporado, solamente se debe ejecutar el siguiente comando para activarlo:

IPv6 install.

4.6.3 Componente DNS

El tercer componente que debe ser actualizado por una empresa guatemalteca que desea utilizar el protocolo IPv6 es el DNS. En la mayoría de las empresas guatemaltecas e ISPs de Guatemala los servidores de DNS se encuentran implantados en los sistemas operativos Microsoft Windows ® o Linux. Se debe observar la versión del servidor de DNS utilizado para decidir si debe ser actualizada o no.

4.6.3.1 DNS de BIND de Linux

Para permitir a un servidor de DNS de BIND en Linux la utilización de los registros “AAAA”, esto es, el manejo de direcciones IPv6, debe contar como mínimo con una versión 8.1.x , 4.9.5 ó Bind9. Sino se tiene ninguna de las versiones se debe descargar desde el portal de Linux la versión mas actualizada de dicho servidor de DNS, compilarla e instalarla.

Para el soporte de las direcciones IPv6 en el servidor DNS de BIND debe iniciar por el archivo de configuración named.conf. A través de este archivo se indica el dominio IPv6 de la red de la empresa. La configuración es parecida a las direcciones IPv4. A continuación se muestra un ejemplo en donde el prefijo asignado a la red es 3FFE:8070::/28 y el dominio es ipv6.usac.edu.gt.

```
zone "7.0.8.e.f.f.3.ip6.int" {
        type master;
        file "named.3ffe.807";
};
```

Además se debe manipular los archivos e dominio en donde se almacenan los registros “AAAA” de los nodos internos. Dicho archivo es de la forma:

```
uv.ipv6.usac.edu.gt. IN AAAA 3ffe:8070:2:0:260:8ff:feab:0091
```

Para las zonas inversas se debe configurar en el archivo indicado en el archivo named.conf para el dominio de la red IPv6, en este caso named.3ffe.807. Dicho archivo es de la forma:

```
1.9.0.0.b.a.e.f.f.f.8.0.0.6.2.0.0.0.0.0.0.2.0.0.0.0 IN PTR uv.ipv6.usac.edu.gt.
```

Actualmente Microsoft Windows ® no brinda soporte para el manejo de direcciones IPv6 dentro de sus servidores DNS y una solución podría ser la utilización dentro de la red de un servidor implantado en Linux. Debido a que en Guatemala la solución corto plazo consiste en la utilización de túneles no es necesario un servidor de DNS que soporte direcciones IPv6, por lo cual la falta de soporte por este fabricante no debe ser un problema.

5. EJEMPLOS DE ESCENARIOS DE TRANSICIÓN

5.1 Acceso a Internet

El objetivo principal de los mecanismos de transición es permitir a una red la comunicación con redes que utilicen el protocolo IPv6. Para realizar dicha comunicación es necesario observar cual será la forma en que se accesará a Internet para el intercambio de información en dicho formato. A continuación se muestran diferentes formas que han utilizado para cumplir con dicho objetivo.

5.1.1 *Proxy* de aplicación y túnel configurado

Básicamente en esta forma de acceder a Internet es por medio de túneles configurados. Es una solución igual a que para las empresas guatemaltecas en el corto plazo.

Dentro de este escenario, la red de la empresa posee un *router* que maneja tanto el protocolo IPv6 como el IPv4. A través de este *router* es como se logra el acceso a Internet y el intercambio de información en formato IPv6. Este componente es el encargado de reenviar el tráfico en formato IPv6 tanto dentro de la red interna como a redes externas. A través de el se forman túneles configurados a redes que utilizan dicho protocolo. Por lo tanto los nodos

internos de la red utilizan al *router* para el intercambio de información en ambos formatos.

El componente "*proxy* de aplicación" introducido es el encargado de recibir peticiones de los nodos internos que desean intercambiar información en formato IPv6 y dichas peticiones son enviadas al *router* que posee el túnel configurado. Este componente puede rechazar peticiones de nodos externos que desean tener comunicación con nodos internos. Este componente no es obligatorio para una red que desee utilizar el protocolo IPv6, solamente es utilizado cuando se desee tener un mejor control de la seguridad.

5.1.2 Filtro de paquetes, p*roxy* de aplicación, túnel configurado

En este escenario básicamente es igual que al descrito anteriormente. Utiliza túneles configurados para la comunicación con redes que utilizan el protocolo IPv6 y son creados dentro del *router* interno de la red que utiliza el protocolo. El *proxy* de aplicación es utilizado para brindar un mejor control de la seguridad sobre los nodos externos que deseen comunicarse con los internos de la red para el intercambio de información en formato IPv6.

El componente extra que se aplica a este escenario es el denominado "filtro de paquetes". A través de este componente se puede llevar un mejor control del tipo de información permitido para la comunicación. Por lo tanto, con este componente, se puede permitir el intercambio de solamente un tipo de información entre los nodos internos y los externos.

Al igual que el componente "*proxy* de aplicación" este componente no es obligatorio para una red que desee utilizar el protocolo IPv6 para la comunicación, solamente es un componente adicional para tener un mejor control del tipo de información permitido.

5.1.3 Traductor y túnel configurado

Este escenario básicamente permite al acceso a Internet, a través de la combinación de dos de ellos, un traductor y túneles configurados. La utilización de esta forma de acceso es solamente para aquellas redes en las cuales se utiliza el protocolo IPv6 para la comunicación interna y externa pero aún desean comunicarse con redes que utilizan el protocolo IPv4 para la comunicación.

En este escenario se crean túneles configurados hacia las redes que utilizan el protocolo IPv4. El componente traductor utilizado es el denominado NAT-PT el cual realiza la traducción de direcciones IPv4 a IPv6 y viceversa para la comunicación. Este componente reside dentro del *router* que se utiliza para la comunicación, por lo cual debe tener la capacidad de manejar ambos protocolos. Los túneles configurados utilizados en este escenario también deben crearse estáticamente dentro del *router*.

5.1.4 Traductor y 6to4

Este escenario es similar al descrito anteriormente. Para permitir la comunicación de una red que solo utiliza el protocolo IPv6 con otra red que usa el protocolo IPv4 se basa en dos componentes: un traductor y un túnel. La diferencia reside en que en este caso se trata de túneles 6to4.

El traductor involucrado en este escenario también es el NAT-PT y por lo tanto su función es traducir direcciones IPv6 en IPv4 y viceversa.

Para la utilización de los túneles 6to4 se debe asignar un prefijo IPv6 a la red. Dicho prefijo se forma con 2002:dirIPv4router. La dirección IPv4 del *router* debe ser una dirección IPv4 pública. Los túneles utilizados en este escenario son establecidos dinámicamente por lo cual es una mejora al escenario descrito anteriormente. El único requisito consiste en que tanto el *router* interno de la red como el externo tengan la capacidad de manejar esta clase de túneles.

5.2 Red de compañía y oficinas remotas

Este escenario es útil para las empresas que utilizan redes privadas virtuales para permitir a redes en oficinas remotas la comunicación a una red central como si estas formarán parte de ella.

La oficina remota es básicamente una red normal, por lo tanto para permitir el intercambio de información en formato IPv6 entre la oficina remota y la central se hace uso de los mecanismos de transición.

En este caso se hace uso de los túneles 6to4 y las redes manejan tanto el protocolo IPv4 como el IPv6 por lo cual no es necesario la utilización de ningún mecanismo de traducción. Debido a la utilización de túneles 6to4 el único requisito que se debe tener consiste en que tanto el *router de la* oficina remota como el de la central deben tener la capacidad de manejar túneles de este tipo y cada una debe tener asignado un prefijo IPv6.

5.3 Proveedor de servicios de Internet

Una empresa que desee utilizar el protocolo IPv6 ya sea para la utilización de los servicios brindados por dicho protocolo o para experimentar su funcionamiento puede hacer uso del mecanismo denominado "*Tunnel Broker*".

5.3.1 *Tunnel Broker*

La ventaja que posee este mecanismo consiste en que la gestión de los túneles que debe hacer una empresa dentro de su red, es hecha por otra empresa que brinda este mecanismo. A la empresa que provee este mecanismo servicio puede ser vista como un ISP virtual de IPv6 . En este escenario los túneles configurados, 6to4 de los otros escenarios descritos no

deben ser creados por la empresa. El único requisito que se debe cumplir para la utilización de este mecanismo consiste en que la dirección IPv4 brindada al ISP virtual debe ser una dirección pública. La utilización de este escenario brinda la oportunidad a uno o varios nodos de la red utilizar los servicios del protocolo IPv6.

6. IPv6 EN LA ACTUALIDAD

6.1 IPv6 en el mundo

El nivel de difusión que posee actualmente el protocolo IPv6 a lo largo del mundo se encuentra en sus niveles de inicio. El problema de la escasez de direcciones actualmente no tiene el mismo impacto a lo largo de los 5 continentes del mundo. Además las soluciones temporales que se han creado para resolver el problema hacen que el protocolo no este ampliamente difundido a lo largo del mundo y aún sea el protocolo oficial de comunicación el IPv4.

Hasta la fecha existen un total de 1064 sitios *6bone* que constituyen la columna vertebral del protocolo IPv6. El total de 6bones se encuentran implantados en 57 países y distribuidos principalmente en Europa y Norteamérica.

6.1.1 6bone

6.1.1.1 ¿Qué es el 6bone?

Es la red internacional experimental utilizada para probar los conceptos e implantaciones del protocolo IPv6.

La idea de crear una red experimental *backbone* sobre la Internet actual fue el resultado de la iniciativa de varias instituciones de investigación involucradas en las primeras experimentaciones del protocolo IPv6.

La red se creo en marzo de 1996 con el establecimiento de los primeros túneles entre los laboratorios de GI (Francia), UNI-C (Dinamarca) y WIDE de Japón.

La topología de esta red esta compuesta por varias redes aisladas a lo largo del mundo que solamente utilizan el protocolo IPv6 para la comunicación. Dichas redes aisladas se encuentran conectadas por medio de la utilización de túneles basados en la infraestructura IPv4 de la Internet actual. Actualmente se realizan grandes esfuerzos por reemplazar los túneles por enlaces IPv6 nativos.

La jerarquía de esta red esta dividida en nodos *backbone*, nodos de transito, nodos hojas, en donde los nodos *backbone* tienen el mayor nivel en la jerarquía y los nodos hojas el menor nivel.

Actualmente está compuesta de 1092 nodos, dentro de los cuales se encuentran 116 nodos *backbone*. Los nodos backbone desempeñan el papel de un TLA experimental encargado de brindar direcciones IPv6 a sitios que no son backbone. Una dirección asignada desde el 6bone es identificada por el prefijo 3FFE:/16. A cada nodo *backbone* se le asigna un prefijo que mezclado con el prefijo del 6bone forman un prefijo de 24 bits denominado “prefijo pTLA”. El url oficial de la red es: http://www.6bone.net.

6.1.1.2 Requisitos para conectarse al 6bone

Cuando una empresa decide conectarse al 6bone para experimentar con el protocolo IPv6 debe cumplir con una serie de requerimientos para poder llevar a cabo dicha actividad. La serie de requerimientos se muestran a continuación:

- Obtener un número de sistema autónomo (ASN).
- Contactar con algún pTLA para obtener el "prefijo pTLA". Actualmente el listado de pTLAs se encuentra disponible en: http://www.6bone.net/6bone_pTLA_list.html.
- Contactar a alguien para que enrute la información en formato IPv6 al 6bone.
- Tanto el *router* que se conecta al 6bone como el nodo de la red interna deben utilizar una dirección IP pública.

6.1.2 6REN

6REN es la red IPv6 para investigación y educación. En Octubre de 1998 la "*Energy Science Network (ESnet)* " creo el proyecto 6REN.

Es un proyecto de redes e investigación y educación con el objetivo de proveer servicios de transito de información en formato IPv6, con la característica de facilitar una alta calidad, alto desempeño y una operación robusta en redes que utilizan el protocolo IPv6 para la comunicación.

El primer paso de 6REN consistió en crear conexiones IPv6 nativas entre las redes de ESnet, Internet2/vBNS, Canarie, Cairn y WIDE. El portal oficial de esta red se encuentra en el url: http://www.6ren.net/.

6.1.3 6TAP

Es un proyecto cuyo objetivo principal consiste en el ruteo de la información en formato IPv6. Además este proyecto busca ayudar al desarrollo de procedimientos de operación para el protocolo IPv6.

A través de este proyecto se busca facilitar la interconexión de los participantes en el proyecto 6REN en USA, Canarie y Esnet. El portal oficial de esta red se encuentra en el url: http://www.6tap.net/.

6.1.4 IPv6 forum

En Luxemburgo el 7 de julio de 1999 fue creado el Foro de IPv6. Es un consorcio mundial de proveedores líderes de Internet, redes de investigación y

educación, con la misión de promover el protocolo IPv6 para dar como resultado un mejor reconocimiento de IPv6 en el mercado.

Además fue creado con el objetivo de crear la próxima generación de Internet con más calidad y seguridad.

El foro trabaja conjuntamente con el IETF el cual es el encargado de las especificaciones técnicas del protocolo. El IPv6 forum no desarrolla el protocolo ya que esta función es desarrollada por el IEFT. El portal oficial de esta red se encuentra en el url: http://www.ipv6forum.com/.

6.2 IPv6 en Latinoamérica

Actualmente la utilización del protocolo IPv6 en Latinoamérica es utilizado en organizaciones no lucrativas, esto es, de carácter puramente de investigación.

La mayoría de las empresas comerciales no han adoptado dicho protocolo ya que en esta región del mundo aún no se agravado el problema de escasez de direcciones, y específicamente para el área de Centroamérica el interés en dicho protocolo es por parte de organizaciones no lucrativas. Actualmente se encuentran registrados dentro del 6bone 53 sitios pertenecientes a Latinoamérica, que constituyen un 4.85 % del total de sitios

registrados. A continuación se muestra como se encuentran distribuidos dichos sitios:

Tabla XII. Número de sitios en Latinoamérica que utilizan IPv6 para la comunicación

País	Número de sitios
Argentina	12
Brasil	12
Chile	3
Colombia	4
Cuba	1
R. Dominicana	3
México	15
Perú	2
Uruguay	1

6.3 IPv6 en Guatemala

Actualmente dentro del entorno guatemalteco el interés hacia del protocolo IPv6 esta en su fase de inicio. El interés se ha hecho manifiesto por una organización no lucrativa la cual utilizará dicho protocolo para el cumplimiento de sus objetivos. Dicha organización es denominada “Red avanzada guatemalteca para investigación y educación (RAGIE)”.

RAGIE busca propiciar el intercambio de información entre instituciones científicas, académicas y de desarrollo tanto dentro del entorno guatemalteco como a nivel internacional. Para el cumplimiento de su objetivo hará uso de la próxima generación de Internet la cual esta relacionada con el protocolo IPv6.

El proyecto RAGIE contempla varias categorías de miembros las cuales son las siguientes:

- Asociados activos institucionales. Formada por instituciones educativas sin fines de lucro.
- Asociados activos benefactores. Formada por empresas privadas.
- Asociados activos individuales. Formada por cualquier persona individual.

Los miembros que actualmente forman parte de la Red avanzada guatemalteca para investigación y educación (RAGIE) son:

- Universidad de San Carlos de Guatemala
- Universidad del Valle de Guatemala
- Universidad Francisco Marroquín

- Universidad Rafael Landivar
- Universidad Mariano Gálvez
- Universidad Galileo

La organización RAGIE esta distribuida jerárquicamente de la siguiente forma:

- Asamblea general de asociados. Es la jerarquía más alta y esta formada por todos los miembros del proyecto.
- Consejo directivo. Encargado de la dirección y representación de la asociación. Está integrado por los representantes de cada una de las universidades participantes.

La creación de la organización RAGIE dentro del entorno guatemalteco es útil ya que se promoverá la utilización del protocolo IPv6 así como los beneficios implicados con la utilización de dicho protocolo e Internet2.

CONCLUSIONES

1. Los beneficios que aporta el protocolo IPv6 sobre el IPv4 son:

   - Número de direcciones IP infinito. Con los 128 bits de una dirección IPv6 es posible tener 3.40282366920938463463374607431768e+38 direcciones para asignar a cada usuario de Internet y resolver el problema de escasez de direcciones IP.

   - Seguridad en los paquetes de IPv6. Se mantiene una conexión segura entre los nodos involucrados en la comunicación para asegurar autenticación, integridad y confidencialidad.

   - Garantizar permanente conexión a Internet a dispositivos móviles sin necesidad de que cambien de dirección IP.

   - Reducción en las tablas de ruteo debido al direccionamiento jerárquico de las direcciones IPv6.

2. El acceso a Internet actualmente se realiza mediante mecanismos como NAT o *Proxies*, los cuales son implantados dentro de servidores que actúan como intermediarios entre los nodos internos de la red y los servidores de Internet.

3. Una organización que desea brindar a sus clientes el acceso tanto a infraestructuras IPv4 como IPv6 puede realizarlo mediante la utilización de una infraestructura que maneje ambos protocolos, en la cual los *routers* encargados de manejar el tráfico y los servidores DNS posean soporte para manejar direcciones IPv4 e IPv6 y así sus clientes solamente utilicen un ISP y no uno para cada protocolo.

4. Una organización guatemalteca puede adoptar diferentes escenarios para realizar la transición al protocolo IPv6 de la siguiente forma:

   - En el corto plazo para el acceso a la infraestructura IPv4 de la Internet actual la utilización de ISPs guatemaltecos y para el acceso a infraestructuras IPv6 una conexión hacia un ISP IPv6 virtual mundial mediante túneles configurados.

   - En el mediano plazo se debe actualizar los nodos internos, *routers* y servidores DNS para que utilicen tanto direcciones IPv4 como IPv6 y utilizar ISPs guatemaltecos que ya brinden acceso a infraestructuras IPv6. Un ISP guatemalteco debe actualizar su infraestructura para manejar ambos protocolos y poder brindar cualquier clase de conectividad a sus clientes.

   - En el largo plazo se debe tener una infraestructura IPv6 para la red y tener conexión con ISPs que aún brinden conectividad a infraestructuras IPv4. Para un ISP la infraestructura debe ser en su mayoría IPv6 y algunos *routers* con soporte para IPv4.

5. Los componentes que se deben tomar en cuenta para realizar la transición hacia el protocolo IPv6 son:

   - Nodos internos de la red, los cuales para poder comunicarse con nodos que utilizan el protocolo IPv6 se deben actualizar para que utilicen una pila para dicho protocolo.

   - *Routers* deben ser actualizados para puedan manipular tráfico IPv6.

   - Servidores DNS se deben actualizar para que puedan manipular los registros tipo “AAAA” así como dominios de búsquedas inversas de nodos IPv6.

6. En Latinoamérica actualmente la utilización del protocolo IPv6 abarca el 4.85 por ciento del total de sitios registrados a lo largo del mundo que utilizan dicho protocolo; y se resume en organizaciones no lucrativas que buscan promover y obtener los beneficios de dicho protocolo, además dentro del entorno guatemalteco actualmente se encuentra en fase de desarrollo el proyecto de la organización RAGIE.

RECOMENDACIONES

1. Debe considerarse antes de realizar inversiones en infraestructuras la cantidad de beneficios que brinda el protocolo IPv6 sobre el actual IPv4, ya que después de un tiempo se deberán hacer inversiones extras para poder utilizar los beneficios de ambos protocolos.

2. El problema crónico de la escasez de direcciones IP debe ser ampliamente analizado así como el tiempo estimado de escasez total de direcciones en lugar de tomar el camino más simple como la utilización de mecanismos como NAT o proxy.

3. Un ISP que desee brindar conectividad a sus clientes hacía infraestructuras que utilizan el protocolo IPv6, el cual debe realizar un análisis de la demanda de dicho protocolo en el mercado local para considerar no una actualización completa de su infraestructura, sino agregar solamente algunos *routers* que tengan soporte para IPv6; y hacer uso de túneles configurados entre sus clientes y las demás infraestructuras del mundo.

4. Las empresas guatemaltecas deben iniciar la transición hacía el protocolo IPv6, ya que no solamente se previenen ante el problema cercano de la escasez de direcciones IP, sino que aumentan la demandad de dicho

protocolo dentro del país dando como resultado que los ISPs guatemaltecos también realicen la transición.

5. Los componentes involucrados en la transición deben ser ampliamente analizados para conocer si es más flexible y barato adquirir un nuevo componente que utilice el protocolo IPv6 antes de realizar una actualización en el componente y pueda producir bajas de rendimiento.

6. La utilización del protocolo IPv6 debe ser ampliamente promovida dentro de los países latinoamericanos y cooperar mutuamente entre todos los países, mediante el intercambio de información relevante al tema para lograr un mejor desarrollo del que se encuentra actualmente en esta región del mundo.

BIBLIOGRAFÍA

1. 6bone. "***How to Join the* 6bone**" http://6bone.net/6bone_hookup.html. 2002.

2. Acebes Ramos, Pablo y otros "**IPv6, el nuevo protocolo para *Internet***" http://www.consulintel.es/Html/ForoIPv6/Documentos/ipv6A.ppt. 2002.

3. Allman M. y otros "**FTP *Extensions for IPv6 and* NATs**" http://www.ietf.org/rfc/rfc2428.txt. 2002.

4. "**BIS (Bump Ithe Stack)**". http://www.eurescom.de/~public-webspace/P1000-series/P1009/doc3_2.html. 2002.

5. Bound, Jim y otros. "***Dual Stack Transition Mechanism* (DSTM)**" http://www.ipv6.rennes.enst-bretagne.fr/dstm/draft-ietf-ngtrans-dstm-08.txt. 2002.

6. Carpenter, B. y C. Jung. "***Transmission of IPv6 over IPv4 Domains without Explicit Tunnels***" http://www.ietf.org/rfc/rfc2529.txt. 2002.

7. Carpenter B. y K. Moore. "***Connection of IPv6 Domains via IPv4 Clouds***" http://www.faqs.org/rfcs/rfc3056.html. 2002.

8. Cisco Systems ®. "***Cisco IOS Sofware Releases 12.2T Start Here: Cisco IOS Software Release Specifics for IPv6 Features***" www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ipv6/ftipv6s.pdf. 2002.

9. Cisco Systems ®. "***IPv6 for Cisco IOS Software, File 2 of 3: Configuring***". www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t2/ipv6/ftipv6c.pdf. 2002.

10. Correa, David. "**IPv6 para Linux**". http://www.ipv6.itesm.mx/documentos/IPv6paraLinux.htm. 2002.

11. Durand, Alain y otros." ***IPv6 Tunnel Broker***". http://www.ietf.org/rfc/rfc3053.txt. 2002.

12. "**Estatutos de la asociación civil RAGIE**". http://www.cragie.org.gt/estatutos. 2003.

13. Fernández Alcántara, Azael. "**Red IPv6 de CUDI**". www.cudi.edu.mx/primavera2002/presentaciones/Red-IPv6_de_CUDI.pdf. 2002.

14. Gallego Gómez, Oscar y otros. "**IPv6, el nuevo protocolo de Internet**." http://www.consulintel.es/Html/ForoIPv6/Documentos/ipv6B.ppt. 2002.

15. Gilligan, R. y E. Nordmark. "**RFC1933**" http://www.faqs.org/rfcs/rfc1933.html. 2002.

16. Guardini, Ivano y otros. "***IPv6 operational experience within the 6bone***". http://carmen.cselt.it/papers/inet2000/index.htm. 2002.

17. Hagino, J. "***An IPv6-to-IPv4 Transport Relay Translator***". http://www.ietf.org/rfc/rfc3142.txt. 2002.

18. Hazeltine, Andrew. "***IPv6 Transition Scenarios***". http://www.ipv6forum.org/navbar/events/telluride00/presentations/hazeltine-asci/. 2002.

19. Hurtado, Jesús. "**Internet sin ordenador es la meta**" http://www.terra.com.ve/internet/articulo/html/int3248.htm. 2002.

20. "***Interoperability between IPv6 and IPv4***". http://ntrg.cs.tcd.ie/undergrad/4ba2.02/ipv6/interop.html. 2002.

21. Kitamura, H. "***A SOCKS-based IPv6/IPv4 Gateway Mechanism***". http://www.ietf.org/rfc/rfc3089.txt. 2002.

22. Lazo Ramírez, Christian y Fernández Alcántara, Azael. "**IPv6 El protocolo para la nueva Internet**".

23. Lee, Thomas y Davies Joseph. **Microsoft Windows ® 2000 TCP/IP Protocolos y Servicios. Referencia Técnica**. España: McGraw-Hill/Interamericana. 2000.568pp

24. Martínez Melo, Jorge Alberto. "**Cocinando un DNS para IPv6**" http://www.nic.unam.mx/documentos/DNSparaIPV6.html. 2002.

25. Medina, Octavio. "***DSTM Dual Stack Transition Mecanism***" http://www.ipv6.rennes.enst-bretagne.fr/dstm/ . 2002.

26. Microsoft Windows ®."***IPv6/IPv4 Coexistence and Migration***" www.microsoft.com/windows.netserver/docs/IPv6-IPv4.doc. 2002.

27. Microsoft Windows ®."***Microsoft IPv6 Technology Preview for Windows 2000***" http://msdn.microsoft.com/downloads/sdks/platform/tpipv6/readme.asp. 2002.

28. Microsoft Windows ®."***Getting Started with The Microsoft IPv6 Technology Preview for Windows 2000***" http://msdn.microsoft.com/downloads/sdks/platform/tpipv6/start.asp. 2002.

29. Nordmark, E. "***Stateless IP/ICMP Translation Algorithm (SIIT)***". http://www.ietf.org/rfc/rfc2765.txt. 2002.

30. Palet Martínez, Jordi. "**Tutorial de IPv6**" www.consulintel.es/Html/ForoIPv6/Documentos/ Tutorial%20de%20IPv6.pdf. 2002.

31. Parent, Florent y Régis Desmueles. "**IPv6 Tutorial**" www.viagenie.qc.ca/en/ipv6forum.pdf. 2002.

32. Peralta, Luis. "**IPv6 @ UJI - Rev : 22**" www.si.uji.es/docs/projectes/ipv6/ipv6p.pdf. 2002.

33. Ralli Ucendo, Carlos. "**IPv6: Mecanismos de Transición IPv4 – IPv6**" www.ipv6.garr.it/documenti/ipv6madrid/carlos_ralli_transitiontutoria l.pdf2002.

34. Srisuresh, P. y otros. "***DNS extensions to Network Address Translators (DNS_ALG)***". http://www.ietf.org/rfc/rfc2694.txt. 2002.

35. Tanenbaum, Andrew S. **Redes de computadoras**. 3ª ed. México: Editorial Pretince Hall Hispanoamericana, S.A, 1997. 813pp.

36. Teufel, Martin. "***IPv6@IKNnet - NAT-PT***" http://www.ikn.tuwien.ac.at/~ipv6/nat-pt.htm. 2002.

37. Tsirtsis G. y P. Srisuresh "***Network Address Translation - Protocol Translation (NAT-PT)***" http://www.ietf.org/rfc/rfc2766.txt. 2002.

38. Tsuchiya, Kazuaki. y otros "***Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)***". http://www.ietf.org/rfc/rfc2767.txt. 2002.