PROTOCOLO IPv6 Y SU IMPLEMENTACIÓN EN LAS REDES DE AVANZADA EN COLOMBIA

JOHISE ASTRID MURILLO PATERNINA

RAUMIR ALBERTO SUAREZ MILANES

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERIAS

DIRECCIÓN DE PROGRAMAS DE INGENIERÍA ELECTRICA Y ELECTRÓNICA

CARTAGENA DE INDIAS, D. T. Y C

2009

PROTOCOLO IPv6 Y SU IMPLEMENTACIÓN EN LAS REDES DE AVANZADA EN COLOMBIA

JOHISE ASTRID MURILLO PATERNINA

RAUMIR ALBERTO SUAREZ MILANES

Monografía presentada como registro de aprobación de la Especialización en Telecomunicaciones

Director

Ing. Gonzalo López

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERIAS

DIRECCIÓN DE PROGRAMAS DE INGENIERÍA ELECTRICA Y ELECTRÓNICA

CARTAGENA DE INDIAS, D. T. Y C

2009

Cartagena de Indias, D. T. H. Y C. **27 de Octubre de 2009**

Señores:

Comité de Proyectos de Grado.

Universidad Tecnológica de Bolívar.

Cartagena de Indias, D. T. H. Y C.

Respetados Señores:

Presentamos para su consideración la monografía titulada: **PROTOCOLO IPv6 Y SU IMPLEMENTACIÓN EN LAS REDES DE AVANZADA EN COLOMBIA.** Como requisito para optar el titulo de Especialistas en Telecomunicaciones.

Atentamente,

_____	_____
Johise Astrid Murillo Paternina	**Raumir Alberto Suarez Milanés**
C.C: 60.266.947 de P/na	**C.C: 92.517.422 de S/jo**
Cartagena de Indias, D. T. H. Y C.	**27 de Octubre de 2009**

Señores:

Comité de Proyectos de Grado.

Universidad Tecnológica de Bolívar.

Cartagena de Indias, D. T. H. Y C.

Respetados Señores:

Presentamos para su consideración la monografía titulada: **PROTOCOLO IPv6 Y SU IMPLEMENTACIÓN EN LAS REDES DE AVANZADA EN COLOMBIA.** Como requisito para optar el titulo de Especialistas en Telecomunicaciones.

Espero que el contenido y las normas aplicadas cumplan con los requisitos exigidos por esta dirección.

Atentamente,

_____

Ing. Gonzalo López
Director de Proyecto

Nota de Aceptación

_____

_____

_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado

Cartagena de Indias, D. T. H. Y C. 27 de Octubre de 2009

ARTICULO 105

La Universidad Tecnológica de Bolívar se reserva el derecho de propiedad intelectual de todos los trabajos de grado aprobados y no pueden ser explotados comercialmente sin autorización.

AUTORIZACIÓN

Cartagena de Indias, D. T. H. Y C. 27 de Octubre de 2009

Yo **JOHISE ASTRID MURILLO PATERNINA** identificada con la cédula de ciudadanía número 60.266.947 de Pamplona.

Autorizo a la Universidad Tecnológica de Bolívar a hacer uso de mi trabajo de grado y publicarlo en el catálogo ON LINE de la Biblioteca.

_____

JOHISE ASTRID MURILLO PATERNINA

AUTORIZACIÓN

Cartagena de Indias, D. T. H. Y C. 27 de Octubre de 2009

Yo **RAUMIR ALBERTO SUAREZ MILANES** identificada con la cédula de ciudadanía número 92.517.422 de S/jo

Autorizo a la Universidad Tecnológica de Bolívar a hacer uso de mi trabajo de grado y publicarlo en el catálogo ON LINE de la Biblioteca.

_____

RAUMIR ALBERTO SUAREZ MILANES

DEDICATORIA

A Dios primeramente, porque me ayudó siempre en mis momentos de adversidad y estuvo presente en mis momentos de gloria.

A mis padres, William Murillo López y Josefa María Paternina Ramos, por su amor, confianza y apoyo incondicional a lo largo de todo este proceso de formación profesional.

A mis hermanas, Jenny Murillo Paternina, Yumiris Murillo Paternina y hermano, Michael Murillo Paternina, quienes han sido y seguirán siendo un gran motor para luchar y seguir adelante en los años que me resten de vida.

A mi novio José Benavides Rico, por su amor, su compañía, apoyo incondicional en todos estos momentos para poder alcanzar este gran logro.

Johise Astrid Murillo Paternina.

DEDICATORIA

En primera instancia a Dios todo poderoso que me ha regalado este nuevo título.

A mis padres, que aun cosechan los resultados de su entrega y dedicación en la educación de sus hijos.

A mi bella esposa Lina que con su amor y apoyo me impulsó a lograr esta meta.

A mi hermoso hijo Samuel que me dio la fuerza y entusiasmo para mejorar como profesional y como padre.

A todos ellos les dedico este triunfo con todo mi cariño…

RAUMIR ALBERTO SUAREZ MILANES

AGRADECIMIENTOS

Los autores expresan sus agradecimientos a:

A Dios por permitirnos cumplir con éxito todo este año de estudio en la especialización.

A la Universidad Tecnológica de Bolívar y a nuestro coordinador y director, Gonzalo López por su constante colaboración y apoyo durante el desarrollo de esta monografía.

A nuestros compañeros de la Especialización en Telecomunicaciones, por haber estado en los momentos malos y bueno durante todo este año de estudio.

A todos muchas Gracias.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

GLOSARIO

6over4: Una tecnología ipv6 diseñada para favorecer la coexistencia con ipv4, que proporciona conectividad unicast y multicast a través de una infraestructura IPv4 con soporte para multicast, empleando la red IPv4 como un enlace lógico multicast.

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

AH: (Authentication Header) Ver cabecera de autenticación.

Ambito (scope): Para las direcciones IPv6, el ámbito es la porción de la red a la que se supone que se va a propagar el tráfico.

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

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

Dirección anycast: Es una dirección del rango reservado para las direcciones unicast que identifica múltiples interfaces y es empleada para la entrega de uno a

uno-entre-varios. Con un rutado apropiado, los datagramas dirigidos a una dirección de tipo anycast serán entregados en un único interfaz, el más cercano.

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

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

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

DNS: (Domain Name System.) Ver sistema de nombres de dominio.

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

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

Enlace: Uno o más segmentos de una red de área local limitados por routers.

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

Grupo Multicast: Conjunto de equipos escuchando una dirección multicast específica.

HA: Home Address, ver dirección propia.

HAA: Home Agent Address, ver dirección del agente propio.

ICMPv6 (Internet Control Message Protocol for IPv6): Protocolo para los mensajes de control de Internet para IPv6) Un protocolo que proporciona mensajes de error para el rutado y entrega de datagramas IPv6 y mensajes de información para diagnóstico, descubrimiento de vecinos, descubrimiento de receptores multicast y movilidad IPv6.

IPv6 en IPv4: Ver túneles IPv6 sobre IPv4.

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

ISATAP (Intra-site Automatic Tunneling Addressing Protocol): Protocolo de Direccionamiento de Túneles Internos Automáticos.

Llamada a procedimientos remotos (RPC): Interfaz utilizada para crear programas cliente/servidor distribuidos. Las librerías que implementan el sistema

de llamadas a procedimientos remotos o RPCs se encargan de gestionar los detalles relacionados con los protocolos de red y las comunicaciones.

Máquina 6to4: Una máquina IPv6 que está configurada con al menos una dirección 6to4 (una dirección global con el prefijo 2002::/16). Las máquinas 6to4 no requieren configuración manual y crean las direcciones 6to4 empleando mecanismos clásicos de autoconfiguración.

Máquina ISATAP: Es un equipo al que se le asigna una dirección ISATAP.

MLD: Ver descubrimiento de receptores Multicast.

Mobile IP: Ver movilidad IPv6.

Movilidad IPv6: Un conjunto de mensajes y procesos que permiten a un nodo IPv6 cambiar arbitrariamente su posición (subred de acceso a Internet IPv6) y mantener activas las conexiones establecidas previamente.

MTU: Ver unidad máxima de transmisión.

MTU IPv6. El tamaño máximo de un paquete IP que se puede enviar sobre un enlace.

NAT: Ttraductor de direcciones de red.

ND: Descubrimiento de vecinos.

NLA ID: Ver identificador de agregación de siguiente nivel.

ISATAP: El nombre resuelto por ordenadores con sistema operativo Windows XP Service Pack 1 o bien de la familia de Windows .NET Server 2003 para descubrir automáticamente la dirección del router ISATAP. Los equipos con Windows XP tratan de resolver el nombre "_ISATAP."

Protocolo de Direccionamiento de Túneles Internos Automáticos: Una tecnología de coexistencia que proporciona conectividad IPv6 unicast entre máquinas IPv6 situadas en una intranet IPv4. ISATAP, obtiene un identificador de interfaz a partir de la dirección IPv4 (pública o privada) asignada a la máquina. Este identificador se utiliza para el establecimiento de túneles automáticos a través de la infraestructura IPv4.

Protocolo del nivel superior: Protocolo que utiliza IPv6 como transporte y se sitúa en la capa inmediatamente superior a IPv6, como ICMPv6, TCP y UDP.

Protocolo Punto-a-Punto: Método de encapsulación de red punto-a-punto que proporciona delimitadores de tramas, identificación del protocolo y servicios de integridad a nivel de bit.

Protocolos de Rutado: Procedimientos y conjuntos de mensajes relativos a rutas que se intercambian entre routers para construir las tablas de rutado dinámicamente.

Red: Dos o más subredes conectadas por routers. Otro término empleado es interred.

Redireccionar: Procedimiento englobado dentro de los mecanismos de descubrimiento de vecinos por el cual se informa a un host de la dirección IPv6 de

otro que resulta más adecuado como siguiente salto hacia un determinado destino.

RPC: Llamada a procedimientos remotos (RPC).

Tabla de rutado IPv6: Conjunto de rutas empleadas para determinar la dirección e interfaz del siguiente nodo en el tráfico IPv6 enviado por un equipo o reencaminado por un router.

Túnel: Un túnel IPv6 sobre IPv4, en los que los puntos finales sin determinados por configuración manual.

Túnel automático: Un túnel IPv6 sobre IPv4 en el que los puntos finales son determinados por el empleo de interfaces lógicos de túneles, rutas y direcciones orígenes y destino IPv6.

Túneles IPv6 automáticos: Creación automática de túneles que se emplea con direcciones compatibles con IPv4.

Túneles IPv6 sobre IPv4: Consiste en enviar paquetes IPv6 con una cabecera IPv4, de forma que el tráfico IPv6 pueda enviarse sobre una infraestructura IPv4. En la cabecera IPv4, el campo de Protocolo toma el valor 41.

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

Unidad Máxima de Transmisión: Es la unidad de datos del protocolo más grande que se puede enviar. Las unidades máximas de transmisión se definen a nivel de

enlace (tamaño máximo de trama) y a nivel de red o de Internet (tamaño máximo de los paquetes IPv6).

ACRÓNIMOS

IPv6: Internet Protocol versión 6. (Protocolo de internet versión 6)

DCHPv6: Dynamic Host Configuration Protocol version 6

IEEE: Institute of Electrical and Electronics Engineers

ICMP: Internet Control Message protocol

ICMPv6: Internet Control Message protocol version 6

IGMP: Internet Group Management Protocol

Interface ID: Interface Identifier

IPv4: Internet Protocol versión 4

NAPs: Network Access Protection

IPsec: Internet Protocol security

MPLS: Multiprotocol Label Switching

SATAP: Intra-site Automatic Tunneling Addressing Protocol

TLA ID: Top-Level Aggregation Identifier

ICMPv6: Internet Control Message Protocol for IPv6

EUI: Extended Unique Identifier

R E S U M E N

El nuevo protocolo IPv6 (Internet Protocol version 6) ha sido desarrollado recientemente para responder a las necesidades planteadas por los nuevos servicios Internet. Sin embargo, aunque se trata de protocolos del nivel de red, las aplicaciones no son ajenas al cambio. Para completar la transición a IPv6 es necesario revisar las aplicaciones. El proceso de migración no se puede hacer de forma instantánea y en consecuencia, durante el período de transición surgirán escenarios donde aplicaciones IPv4 e IPv6 tendrán que coexistir e incluso interoperar. En este artículo se exponen los escenarios de aplicación que son sensibles al cambio del protocolo IP y las posibles soluciones para que las aplicaciones funcionen en entornos heterogéneos de red, con diferentes versiones de IP.

Muchos Proveedores de Servicios (ISPs) ya cuentan con sus troncales preparadas para la demanda de clientes que quieran desplegar el nuevo protocolo. Hablamos de ISPs a nivel nacional y regional que poseen esta particularidad, incluso ofreciendo tecnologías más avanzadas, como MPLS, con soporte para IPv6.

En cuanto al ambiente académico la realidad es aun mas alentadora, ya que desde hace muchos años este sector ha estado trabajando, investigando e implementando IPv6, habiéndose convertido en los primeros en demandar el servicio que hoy se ha hecho extensivo a la comunidad en general; Asimismo, distintos organismos de gobierno y entidades públicas o redes de universidades, a la hora de lanzar licitaciones para la compra de equipamientos o servicios, exigen en ellos el soporte del nuevo protocolo, preparándose de esa manera para una transición que consideran inevitable.

En cuanto al intercambio de tráfico, varios NAPs de la región han implementado el protocolo y ofrecen a quienes son sus miembros intercambiar prefijos IPv6 además de IPv4. Esto, más allá de la cuestión técnica del intercambio de prefijos, ayuda a que los ISPs y miembros de NAPs se interesen en el tema y planifiquen su implementación.

INTRODUCCIÓN

IPV6 es un protocolo diseñado por Steve Deering de Xerox PARC y Craig Mudge, cuyo diseño y desarrollo inició hacia el año 1990 por IETF (Internet Engineering Task Force, traducido en: Grupo de Trabajo en Ingeniería de Internet), está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados.

La necesidad de adoptar el nuevo protocolo debido a la falta de direcciones ha sido parcialmente aliviada por el uso de la técnica NAT. Pero NAT rompe con la idea originaria de Internet donde todos pueden conectarse con todos y hace difícil o imposible el uso de algunas aplicaciones P2P (peer-to-peer), voz sobre IP y de juegos multiusuario. Un posible factor que influya a favor de la adopción del nuevo protocolo podría ser la capacidad de ofrecer nuevos servicios, tales como la movilidad, Calidad de Servicio (QoS), privacidad, seguridad entre otros. IPv6 es la segunda versión del Protocolo de Internet que se ha adoptado para uso general; antes que éste surgiera se desarrolló un IPv5, pero no fue un sucesor de IPv4, debido a que fue un protocolo experimental orientado al flujo de streaming que intentaba soportar voz, video y audio. El nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles con sus direcciones propias y permanentes. Al día de hoy se calcula que las dos terceras partes de las direcciones que ofrece IPv4 ya están asignadas. (Se estima que faltan pocos días para que se acaben las direcciones ipv4, resta aproximadamente 492 millones por asignar).

Por otra parte, tal como sucedió en los inicios de Internet con el IPv4, el protocolo de nueva generación, IPv6, tuvo un rápido despliegue en el sector académico científico. Si nos remontamos a los inicios de la Internet, podemos ver que su desarrollo estuvo ligado a las redes de Universidades y los centros de

investigación. En lo que respecta a IPv6, se repite una experiencia similar. Su adopción temprana por la comunidad académica ha tenido como fin, por un lado la experimentación e investigación y por otro la formación de recursos humanos en el tema. A su vez, algunas necesidades propias de este sector se ven beneficiadas con características disponibles en este protocolo. Son algunos ejemplos:

La necesidad de contar con direcciones públicamente alcanzables, que permitan la interacción entre pares (en aplicaciones "peer to peer" como videoconferencia, operación remota de instrumentos, grids, etc). Características como multicast, necesario en aplicaciones como access grid y otras que requieren optimizar el uso del ancho de banda. Disponibilidad de IPSec como parte del stack, lo que facilita el despliegue de aplicaciones que requieren seguridad de extremo a extremo, como disponibilidad de recursos en malla (grids). Las nuevas posibilidades que brindan las características de QoS incorporadas al protocolo. Por todas estas razones, es amplia la experiencia existente en el ambiente académico y de investigación. En particular en la región de Latinoamérica, las Redes Nacionales de Investigación y Educación (NRENs, tal como es su sigla en ingles) y sus instituciones miembro han estado utilizando el protocolo desde hace años. Cabe destacar la experiencia disponible en RedCLARA, en donde actualmente se encuentra disponible IPv6 en forma nativa, con cerca de la totalidad de las NRENs conectadas intercambiando prefijos IPv4 e IPv6. En Colombia, la Red Nacional Académica de Tecnología Avanzada (RENATA), se ha convertido en la pionera en el uso de IPv6, alcanzando un grado de avance acorde a otras redes académicas en el mundo. Para alcanzar este hito, Telefónica, como proveedor del servicio en Colombia, culminó con éxito la implementación de la primera red nacional funcionando bajo el protocolo IPv6.

1. PLANTEAMIENTO DEL PROBLEMA

A medida que la población mundial crece, se hace necesario planificar la posibilidad de que todas las personas puedan acceder a Internet, pero cuando se diseñó el actual IPv4 en los años setenta, no se podía prever el enorme crecimiento de Internet. Y debido a esto, actualmente no existen suficientes direcciones IP para todos los habitantes del planeta, lo que ha ocasionado que muchos países, no sólo Europa que se quedó sin direcciones, sino también países como Japón y los países de África y Latinoamérica, tengan restricciones en el acceso a Internet, a los servicios y aplicaciones de nueva generación.

Otros de los problemas de IPv4 es la gran dimensión de las tablas de ruteo en el backbone de Internet, que lo hace ineficaz y perjudica los tiempos de respuesta. Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, aspectos que no fueron contemplados en el análisis inicial de IPv4, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades. Entre las más conocidas se pueden mencionar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec) y movilidad. Por ello se comenzó, en los años 90, la búsqueda de un sustituto, el cual permitirá la continua evolución de Internet, y así surgió IPv6, la versión 6 del protocolo de Internet.

Los principales problemas que aborda este proyecto es IPv4 versus IPv6, la arquitectura de direccionamiento en el protocolo IPV6, mecanismos de transición a IPV6 y las aplicaciones de este protocolo en las redes avanzadas en Latinoamérica, especialmente en Colombia.

1.1. OBJETIVOS

1.1.1. Objetivo General: Evaluar la evolución que ha tenido el protocolo IPV6 desde su inicio y su estado actual en Latinoamérica, especialmente en Colombia.

1.1.2. Objetivos Específicos:

1.1.2.1 Desarrollar un estudio comparativo de la versión IPV4 a la versión IPV6.

1.1.2.2 Explicar la arquitectura de direccionamiento en el protocolo IPV6.

1.1.2.3 Describir los mecanismos de transición a IPV6.

1.1.2.4 Realizar una descripción de las implementaciones de este protocolo en las redes avanzadas en Latinoamérica, especialmente en Colombia.

1.2. JUSTIFICACION

En estos momentos es prioritaria la divulgación sobre las ventajas de IPv6 y sobre todo que se tenga claridad acerca de la convivencia IPv4 e IPv6, remarcando que la adopción debe iniciarse y que tendrá las facilidades de una transición tecnológica.

Es urgente la inserción, el desarrollo, el fomento y la implantación del Protocolo en Colombia por lo que se requiere incluir el tema en los programas de formación para profesionales, tecnólogos y técnicos de las áreas de sistemas y afines, de tal manera que se logre en los aprendices y estudiantes las competencias para dicha implantación de este protocolo.

IPV6 es una nueva versión del protocolo de redes de datos en los que Internet está basado. La rápida evolución y crecimiento de las redes y su inter-conectividad a nivel mundial hizo necesario el desarrollo de un nuevo protocolo para acompañar y soportar este proceso de manera eficaz y eficiente.

IPV6 es la herramienta ideal para implementar las nuevas tecnologías convergentes y negocios actuales y futuros sin la estrechez y funcionalidad limitada del IPV4.

Este nuevo protocolo suple ciertas falencias que estaban fuera del alcance de IPV4 como direccionamiento escalable y mejoras en movilidad.

IPV6 es capaz de trabajar en forma paralela y/o conjunta con IPV4 lo que garantiza su interoperabilidad en el mundo actual, ya que la completa implantación del nuevo protocolo llevara varios años.

El IETF (Internet Engineering Task Force) desarrollo sus especificaciones básicas durante los años 90 y continúa sus definiciones.

La principal motivación para el diseño y despliegue de IPv6 fue la necesidad de expansión del espacio de direcciones disponible en Internet, permitiendo así que se conecten billones de nuevos dispositivos (PDAs, teléfonos móviles, etc.), nuevos usuarios y tecnologías "siempre-conectadas" (xDSL, cable, Ethernet en el

hogar, Fibra en el hogar, Comunicaciones a través de la red eléctrica, etc.) sin la necesidad del uso de traducción de direcciones.

El protocolo existente, IPv4, dispone solo de 32 bits de direcciones proporcionando un espacio teórico de 232 (aproximadamente cuatro mil millones) interfaces de red únicas globalmente direccionables.

IPv6 en cambio tiene direcciones de 128 bits y por tanto puede direccionar 2128 interfaces de red: (340.282.366.920.938.463.463.374.607.431.768.211.456).

El agotamiento de las direcciones IPv4 que aún no han sido utilizadas, implicaría que Internet no podrá seguir creciendo con la facilidad que lo ha hecho hasta ahora y que se dificultará la incorporación de nuevos usuarios, dispositivos, servicios, aplicaciones y en general la innovación en Internet.

Además incrementará el costo del desarrollo de software y por tanto el costo asociado con la utilización de Internet para nuevos servicios y aplicaciones.

El despliegue de IPv6 es la única solución que podemos calificar de permanente para la problemática del agotamiento de IPv4.

IPv6 no reemplaza IPv4, ambos protocolos co-existirán por muchos años más.

Las políticas de asignación de IPv6 y los costos asociados, facilitan la adopción de IPv6. Se requiere muchos esfuerzos de promoción para la adopción de este nuevo protocolo.

IPv6 está listo para su implementación y explotación en redes de producción para el transporte para las necesidades de tráfico actuales pero las aplicaciones vendrán en fases. Hay una oportunidad muy importante en temas de innovación a través de este protocolo. No hay nuevos servicios en IPv6 que no existan en IPv4, sino en su defecto existen más direcciones IP. Hay ventajas de no usar NAT o mejoras en movilidad, pero no son “nuevos servicios”.

La urgencia de promover la adopción del protocolo IPv6 en el país debido a la necesidad por la demanda por servicios y aplicaciones que requieran IPV6, entre los tomadores de decisión de las organizaciones que permitiría a su vez el impulso en la adopción del protocolo IPv6 en el País.

2. ANTECEDENTES DE IPv6

Básicamente han existido tres fases importantes en el desarrollo de IPv4 hasta lo que hoy conocemos como IPv6:

Primera Fase: 1.992 – TUBA

- Implementación de mecanismos para usar TCP y UDP sobre mayores direcciones.
- Se emplea ISO CLNP (Connection-Less Network Protocol, “protocolo de redes sin conexión”).
- Se descarta.

Segunda Fase: 1993– SIPP, acrónimo inglés de Single In-line Pin Package (Paquete de Pines en Línea Simple).

- Proyecto “Simple IP Plus”.
- Mezcla de SIP (Protocolo de Inicio de Sesiones) y PIP, dos tentativas anteriores para sustituir IPv4.
- Direcciones de 64 bits.

En diciembre de este mismo año, el RFC 1550 fue distribuido, titulado "IP: Next Generation (IPng)". Este RFC invitó a cualquier partido interesado que sometiera comentarios con respecto a cualesquiera requisitos específicos para el IPng o cualquier factor dominante que se deban considerar durante el proceso de selección de IPng.

Las respuestas fueron sometidas que trataron una variedad de asuntos, incluyendo: seguridad (RFC 1674), opinión de un usuario corporativo grande (RFC 1686). El área de IPng detallado en el RFC 1726, "Criterio Técnico para elegir IP, la nueva generación de direcciones IP (IPng)", para definir los sistemas de los criterios que serían utilizados en el proceso de la evaluación de IPng.

Tercera Fase: 1.994 – IPng

- Se adopta SIPP.
- Se cambia el tamaño de las direcciones a 128 bits.
- Se renombra como IPv6.

La red **6bone** era una red IPv6 de carácter experimental creada para ayudar a los vendedores y usuarios a participar en la evolución y transición a IPv6. Su enfoque original fue la prueba de estándares e implementaciones. En marzo de 1996, la red **6bone** empezó sus funciones como un proyecto de colaboración entre Norteamérica, Europa y Japón. Los primeros túneles se establecieron entre los laboratorios IPv6, G6 de Francia, UNI-C de Dinamarca y WIDE de Japón, bajo la coordinación de la IETF.

A principios de 1998 un ensayo de IPv6 en todo el mundo y pre-producción de despliegue la red, llamado el 6BONE, ya había llegado a unos 400 sitios y redes en 40 países. Existen más de 50 IPv6 implementaciones finalizadas o en marcha en todo el mundo, y más de 25 en prueba o usadas en producción.

2.1. ENTIDADES QUE FORTALECEN LA IMPLEMENTACIÓN DE IPV6

Una asociación sin ánimo de lucro, "*el Foro IPv6*", con el objetivo común de educar al mercado en las ventajas del protocolo IPv6, promover su uso, y reforzar su aplicación en el mundo. La lista de corporaciones involucradas en este proyecto es una mezcla explosiva, incluyendo fabricantes, instituciones de Investigación y Desarrollo, organizaciones de Educación, Operadores de Telecomunicaciones, y Empresas de Consultoría, entre otros. Eso implica, por supuesto, una ingente generación de esfuerzos personales y de corporaciones, presionando a las

Organizaciones de Normalización para acelerar el proceso, para culminar con la creación de una definición completa y estable del protocolo.

2.2. MIEMBROS FUNDADORES DEL FORO IPV6

Entre los miembros iníciales del Foro IPv6 se incluyen 42 de las compañías e instituciones punteras activas en la nueva tecnología Internet, un foro verdaderamente internacional desde el primer día:

Europa y Medio Este: BT, Case Technology, Consulintel, Deutsche Telekom, CSELT, DFN, Ericsson, Eurocontrol, Gigabell, IABG, Intracom, Netmedia, Nokia, Teldat, Telebit Communications, CSELT, Telia Networks Services, Thomson-CSF Detexis.

Norte America: 3Com, Advanced Systems Consulting, AT&T, Cisco, Compaq, ESNet, Hewlett-Packard, IBM, MCI WorldCom, Mentat, Microsoft, Motorola, Qwest, SGI, Sprint, Sun, The Business Internet, Viagenie-Canarie.

Asia: Centre for Wireless Communications (Singapore), Hitachi, NTT, NTT Software Corporation, Trumpet Software, WIDE Japan.

Para más detalles acerca de la Tecnología IPv6 o para inscribirse en el Foro IPv6, existe el enlace Web del FORO IPv6: http://www.ipv6forum.com

2.3. IPV6 Vs IPV4

Entre las principales diferencias que encontramos entre ambos protocolos destacamos:

- No existen direcciones de broadcast (sustituida por direcciones multicast).
- Los campos de las direcciones reciben nombres específicos, se denomina “prefijo” a la parte de la dirección hasta el nombre indicado. El prefijo nos permite conocer dónde está conectada una determinada dirección, es decir, su ruta de encaminamiento.
- Cualquier campo puede contener sólo unos o sólo ceros, salvo que explícitamente se indique lo contrario.
- Las direcciones IPv6 son asignadas a interfaces, no a nodos. Dado que cada interfaz pertenece a un único nodo, cualquiera de las direcciones Unicast de las interfaces del nodo puede ser reemplazado para referirse a dicho nodo.
- Todas las interfaces han de tener, al menos, una dirección unicast link-local (alcance local. Existen también direcciones unicast site-local).
- Una única interfaz puede tener también varias direcciones IPv6 de cualquier tipo (unicast, multicast o anycast).
- Una misma dirección o conjunto de direcciones unicast pueden ser asignados a múltiples interfaces físicas, siempre que la implementación trate dichas interfaces, desde el punto de vista de internet, como una única, lo que permite balanceo de carga entre múltiples dispositivos.
- Al igual que en IPv4, se asocia un prefijo de subred con un enlace, y se pueden asociar múltiples prefijos de subred a un mismo enlace.

- Se produce una simplificación de la cabecera. Algunos campos de la cabecera del IPv4 son eliminados o pasan a ser opcionales, tanto para reducir el coste de procesamiento como el tamaño de la cabecera.
- El tamaño de la cabecera de IPv6 es fijo (40Bytes) lo que facilita el procedo en routers y conmutadores.
- Existe mayor flexibilidad para extensiones y nuevas opciones. En IPv6 no existe un campo “opciones”, como tal. La gestión de opciones se realiza por un campo “siguiente cabecera”. Eliminando así las limitaciones de tamaño en la cabecera, e introduciendo una gran flexibilidad en el desarrollo de nuevas opciones.
- Capacidades de control de flujo. Se añaden capacidades que permiten marcar los paquetes que pertenezcan a un determinado tipo de tráfico, para el cual el remitente demanda una calidad mayor a la especificada por defecto o servicios en tiempo real.
- IPv6 provee extensiones para soportar autenticación, e integridad y confidencialidad de datos.

Tabla1. IPv6 vs IPv4

IPv6	**IPv4**
Dirección de 128 bits (16 bytes)	Dirección de 32 bits (4 bytes)
Arquitectura jerárquica	Arquitectura plana
Configuración automática	Configuración manual
Multicast y anycast	Broadcast
Seguridad obligatoria	Seguridad Opcional
Identificación QoS	Sin Identificacion QoS

3. DIRECCIONAMIENTO EN IPv6

3.1. CARACTERISTICAS DE IPv6

Un espacio de direccionamiento: Permite asequibilidad, flexibilidad, agregación, multihoming, autoconfiguración, “Plug and Play”. Esto agrega nuevas funciones, tales como mayor alcance de direccionamientos. Cada nivel puede ayudar al agregado del tráfico y realzar la función de asignación. **Una cabecera más simple:** Permite eficacia de encaminamiento, funcionamiento y escalabilidad continua. Muy pocos campos; 64 campos alineados dígito binario facilitan el proceso dotación-basado muy eficiente. Ninguna suma de comprobación, nuevo flowlabel. **Opciones de Ayuda mejorada:** Los nuevos campos en la cabecera IPv6 definen cómo se maneja y se identifica el tráfico. Trafique la identificación que usa un campo de la escritura de la etiqueta del flujo en la cabecera IPv6 permite que las rebajadoras identifiquen y que proporcionen la dirección especial para los paquetes que pertenecen a un flujo, a una serie de paquetes entre una fuente y a la destinación. Porque el tráfico se identifica en la cabecera IPv6, la ayuda para QoS es parte y paquete del protocolo de IPv6. **Seguridad asignada por mandato:** La comunicación privada sobre un medio público como el Internet requiere los servicios asegurados que protegen los datos contra ser visto o modificación mientras que en tránsito. Aunque un estándar de IPv4-based existe para proporcionar a la seguridad para los paquetes de los datos (conocidos como seguridad o IPSec del Internet Protocol), este estándar es solamente opcional, y las soluciones propietarias son frecuentes. En IPv6, la ayuda de IPSec es un requisito del protocolo. Este requisito proporciona a una solución estándar-basada para las necesidades de la seguridad de la red de dispositivos, de

aplicaciones y de servicios, y promueve interoperabilidad entre diversas puestas en práctica IPv6. **Riqueza de la transición:** Diversos mecanismos de la transición están disponibles que permiten la integración lisa de IPv4 a IPv6. Diversos mecanismos de la compatibilidad se aseguran de que los nodos IPv4 e IPv6 puedan hablar juntos. Ningún día fijo a convertir. Ninguna necesidad de convertir de una vez.

3.2. MODELOS DE DIRECCIONAMIENTO.

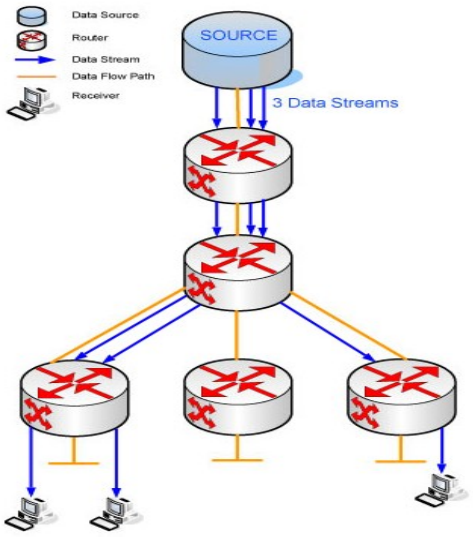
Cualquier tipo de dirección se asigna a interfaces, no nodos. Es algo importante que no haya que olvidar. Todas las interfaces han de tener, por los menos, una dirección de enlace local (Link-Local) de tipo unicast. Un mismo interfaz puede tener asignadas múltiples direcciones de cualquier tipo (unicast, anycast, multicast) o ámbito (scope). Direcciones unicast con ámbito mayor que el de enlace no son necesarias para interfaces que no son usados como origen y destino de paquetes IPv6 hacia o desde no vecinos. Esto significa que para la comunicación dentro de una LAN no nos hacen falta direcciones IPv6 globales, sino que tenemos más que suficiente con direcciones de ámbito local. De hecho, es lo aconsejable para enlaces punto a punto.

Respecto a los prefijos de subred, IPv6 sigue el mismo modelo que IPv4, es decir, un prefijo se asocia a un enlace, pudiendo haber varios prefijos en un mismo enlace. La estructura de dirección ipv6 encuentra sus raíces en la estructura Classless Inter-Domain Routing (CIDR Encaminamiento Inter-Dominios sin Clases), que incluye un prefijo de dirección, un ID de Site y un ID de Host. Para ipv6, sin embargo, habrá múltiples prefijos de direcciones, y cada uno de ellos puede tener múltiples estructuras similares a ID de Site y ID de Host. Como una

base, el documento de arquitectura de direccionamiento de ipv6, define 3 tipos diferentes de direcciones ipv6:

3.2.1. Direcciones Unicast Locales: Unicast: Un identificador para una interface simple. Un paquete enviado a una dirección unicast es entregado a la interface identificada por esa dirección.

Figura 1. Unicast



Fuente: http://www.merit.edu/services/multicast/images/multicast_unicast.jpg

Las direcciones unicast, son agregables con máscaras de bits contiguos, similares al caso de IPv4, con CIDR (Class-less Interdomain Routing). Como

hemos visto, hay varias formas de asignación de direcciones unicast, y otras pueden ser definidas en el futuro.

Los nodos IPv6 pueden no tener ningún conocimiento o mínimo de la estructura interna de las direcciones IPv6, dependiendo de su misión en la red (por ejemplo, host frente a router). Pero como mínimo, un nodo debe considerar que las direcciones unicast (incluyendo la propia), no tienen estructura:

Tabla 2. Dirección del nodo

128 bits
Node address

Un host algo más sofisticado, conocería el prefijo de la subred del enlace al que está conectado:

Tabla 3. Direcciones de prefijo de subred

N bits	128 bits –nbits
Subnet prefix	Interface ID

Dispositivos más sofisticados pueden tener un conocimiento más amplio de la jerarquía de la red, sus límites, etc., en ocasiones dependiendo de la posición misma que el dispositivo o host/router, ocupa en la propia red. El “identificador de interfaz” se emplea, por tanto, para identificar interfaces en un enlace, y deben de ser únicos en dicho enlace. En muchos casos también serán únicos en un ámbito

más amplio. Por lo general, el identificador de interfaz coincidirá con la dirección de la capa de enlace de dicha interfaz. El mismo identificador de interfaz puede ser empleado en múltiples interfaces del mismo nodo, sin afectar a su exclusividad global en el ámbito IPv6.

Se han definido dos tipos de **direcciones unicast de uso local:** Local de Enlace (Link-Local) y Local de Sitio (Site-Local). Las direcciones locales de enlace han sido diseñadas para direccionar un único enlace para propósitos de auto-configuración (mediante identificadores de interfaz), descubrimiento del vecindario, o situaciones en las que no hay routers.

Por tanto, los encaminadores no pueden retransmitir ningún paquete con direcciones fuente o destino que sean locales de enlace (su ámbito esta limitado a la red local). Tienen el siguiente formato:

Tabla 4. Direcciones Unicast, Link-Local

10 bits	54 bits	64 bits
1111111010	0	Identificador de Interfaz

Se trata de direcciones FE80::<ID de interfaz>/10.

Las direcciones locales de sitio permiten direccionar dentro de un “sitio” local u organización, sin la necesidad de un prefijo global. Se configuran mediante un

identificador de subred, de 16 bits. Los encaminadores no deben de retransmitir *fuera del sitio* ningún paquete cuya dirección fuente o destino sea “local de sitio” (su ámbito está limitado a la red local o de la organización).

Tabla 5. Direcciones Unicast, Site-Local

10 bits	38 bits	16 bits	16 bits
1111111010	0	ID de subred	Identificador de Interfaz

Se trata de direcciones FEC0::<ID de subred>:<ID de interfaz>/10.

3.2.2. **Direcciones Unicast Globales Agregables (RFC2374):** Dado que uno de los problemas que IPv6 resuelve es la mejor organización jerárquica del routing en las redes públicas (globales), es indispensable el concepto de direccionamiento “agregable”. En la actualidad ya se emplea este tipo de direcciones, basadas en la agregación por parte de los proveedores del troncal Internet, y los mecanismos adoptados para IPv6, permiten su continuidad. Pero además, se incorpora un mecanismo de agregación basado en “intercambios”. La combinación de ambos es la que permite un encaminamiento mucho más eficiente, dando dos opciones de conectividad a unas u otras entidades de agregación. Se trata de una organización basada en tres niveles:

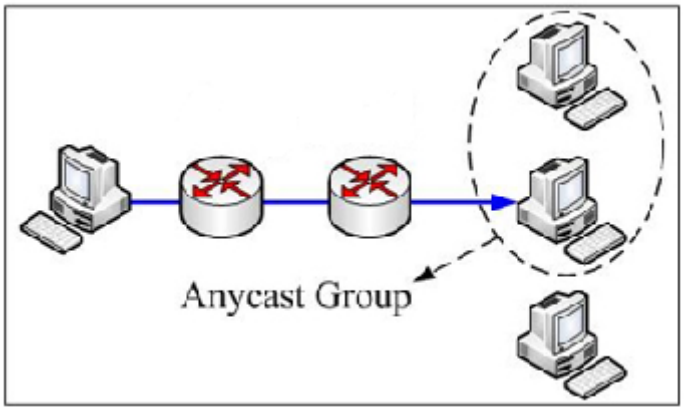
- Topología Pública: conjunto de proveedores e “intercambiadores” que proporcionan servicios públicos de tránsito Internet.

- Topología de Sitio: redes de organizaciones que no proporcionan servicios públicos de tránsito a nodos fuera de su propio “sitio”.
- Identificador de Interfaz: identifican interfaces de enlaces.

A diferencia de lo que ocurre actualmente, los intercambiadores también proporcionarán direcciones públicas IPv6. Las organizaciones conectadas a dichos intercambiadores también recibirán servicios de conectividad directos, indirectamente a través del intercambiador, de uno o varios proveedores de larga distancia. De esta forma, su direccionamiento es independiente de los proveedores de tráfico de larga distancia, y pueden, por tanto, cambiar de proveedor sin necesidad de reenumerar su organización. Este es uno de los objetivos de IPv6.

3.2.3. Direcciones Anycast (RFC2526): Anycast: Un identificador para un conjunto de interfaces (típicamente perteneciente a nodos diferentes). Un paquete enviado a una dirección anycast es entregado por una de las interfaces identificadas por esta dirección (la más cercana, según la medida de distancia del protocolo de ruteo).

Figura2. Anycast



Fuente: http://www.merit.edu/services/multicast/images/multicast_unicast.jpg

Tal y como hemos indicado antes, las direcciones anycast tienen el mismo rango de direcciones que las unicast. Cuando una dirección unicast es asignada a más de una interfaz, convirtiéndose en una dirección anycast, los nodos a los que dicha dirección ha sido asignada, deben ser explícitamente configurados para que reconozcan que se trata de una dirección anycast.

Existe una dirección anycast, requerida para cada subred, que se denomina "dirección anycast del router de la subred" (subnet-router anycast address). Su sintaxis es equivalente al prefijo que especifica el enlace correspondiente de la dirección unicast, siendo el indicador de interfaz igual a cero:

Tabla 6. Dirección anycast del router de la subred

N bits	128 bits –nbits
Subnet prefix	0000000000000000000

Todos los routers han de soportar esta dirección para las subredes a las que están conectados. Los paquetes enviados a la "dirección anycast del router de la subred", serán enviados a un router de la subred.

Una aplicación evidente de esta característica, además de la tolerancia a fallos, es la movilidad. Imaginemos nodos que necesitan comunicarse con un router entre el conjunto de los disponibles en su subred.

Dentro de cada subred, los 128 valores superiores de identificadores de interfaz están reservados para su asignación como direcciones anycast de la subred.

La construcción de una dirección reservada de anycast de subred depende del tipo de direcciones IPv6 usadas dentro de la subred.Las direcciones cuyos tres primeros bits (prefijo de formato) tienen valores entre 001 y 111 (excepto las de multicast, 1111 1111), indican con el bit "universal/ local" igual a cero, que el

identificador de interfaz tiene 64 bits, y por tanto no es globalmente único (es local).

En este caso, las direcciones reservadas anycast de subred se construyen del siguiente modo:

Tabla 7. Direcciones reservadas anycast de subred

64 bits	57 bits	7 bits
Prefijo de subred	1111110111…111	ID anycast

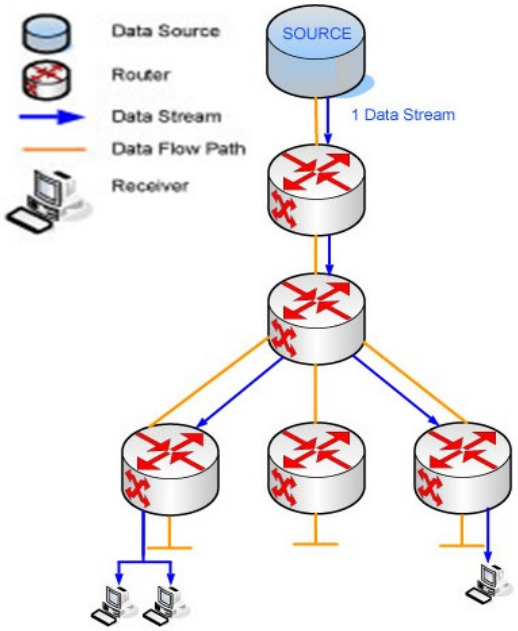
En el resto de los casos, el identificador de interfaz puede tener una longitud diferente de 64 bits, por lo que la construcción se realiza según el siguiente esquema:

Tabla 8. Direcciones reservadas anycast de subred diferente de 64 bits

n bits	121-n bits	7 bits
Prefijo de subred	1111110111…111	ID anycast

3.2.4. **Direcciones Multicast (RFC2375): Multicast,** Un identificador para un conjunto de interfases (típicamente perteneciendo a nodos diferentes). Un paquete enviado a una dirección multicast es entregado a todas las interfases identificadas por esta dirección.

Figura 3. Multicast



Fuente: http://www.merit.edu/services/multicast/images/multicast_unicast.jpg

Una dirección multicast en IPv6, puede definirse como un identificador para un grupo de nodos. Un nodo puede pertenecer a uno o varios grupos multicast.

Las direcciones multicast tienen el siguiente formato:

Tabla 9. Direcciones Multicast

8	4	4	112 bits
11111111	000T	Ámbito	Identificador de Grupo

El bit “T” indica, si su valor es cero, una dirección multicast permanente, asignada únicamente por la autoridad de numeración global de Internet. En caso contrario,

si su valor es uno, se trata de direcciones multicast temporales. Los 4 bits que le preceden, que por el momento están fijados a cero, están reservados para futuras actualizaciones.

Los bits “ámbito” tienen los siguientes significados:

Tabla 10. Identificador de grupo

0	Reservado
1	Ambito Local de Nodo
2	Ambito Local de Enlace
3	No asignado
4	No asignado
5	Ambito Local de Sitio
6	No asignado
7	No asignado
8	Ambito Local de Organización
9	No asignado
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Ambito Global
F	Reservado

El “Identificador de Grupo”, identifica, como cabe esperar, el grupo de multicast concreto al que nos referimos, bien sea permanente o temporal, dentro de un determinado ámbito.

Por ejemplo, si asignamos una dirección multicast permanente, con el identificador de grupo 101 (hexadecimal), al grupo de los servidores de tiempo (NTS), entonces: FF01::101 significa todos los NTS en el mismo nodo que el paquete origen. F02::101 significa todos los NTS en el mismo enlace que el paquete origen. FF05::101 significa todos los NTS en el mismo sitio que el paquete origen. FF0E::101 significa todos los NTS en Internet.

Las direcciones multicast no-permanentes, sólo tienen sentido en su propio ámbito. Por ejemplo, un grupo identificado por la dirección temporal multicast local de sitio FF15::101, no tiene ninguna relación con un grupo usando la misma dirección en otro grupo (en otro ámbito), ni con un grupo permanente con el mismo identificador de grupo.

Las direcciones multicast no deben ser usadas como dirección fuente en un paquete IPv6, ni aparecer en ninguna cabecera de encaminado. Las principales direcciones multicast reservadas son las incluidas en el rango FF0x:0:0:0:0:0:0:0.

Algunos ejemplos útiles de direcciones multicast, según su ámbito, serían:

FF01:0:0:0:0:0:0:1 – todos los nodos (ámbito local)
FF02:0:0:0:0:0:0:1 – todos los nodos (ámbito de enlace)
FF01:0:0:0:0:0:0:2 – todos los routers (ámbito local)
FF02:0:0:0:0:0:0:2 – todos los routers (ámbito de enlace)
FF05:0:0:0:0:0:0:2 – todos los routers (ámbito de sitio)

La dirección FF02:0:0:0:0:1:FFxx:xxxx, denominada “Solicited-Node Address”, o dirección de nodo solicitada, permite calcular la dirección multicast a partir de la unicast o anycast de un determinado nodo. Para ello, se sustituyen los 24 bits de menor peso (“x”) por los mismos bits de la dirección original. Así, la dirección 4037::01:800:200E:8C6C se convertiría en FF02::1:FF0E:8C6C.
Cada nodo debe de calcular y unirse a todas las direcciones multicast que le corresponden para cada dirección unicast y anycast que tiene asignada.

3.2.5. **Direcciones especiales en IPv6:** Se han definido también las direcciones para usos especiales como:

- Dirección de auto-retorno o Loopback (::1) – No ha de ser asignada a una interfaz física; se trata de una interfaz “virtual”, pues se trata de paquetes que no salen de la máquina que los emite; nos permite hacer un bucle para verificar la correcta inicialización del protocolo (dentro de una determinada máquina).

- Dirección no especificada (::) – Nunca debe ser asignada a ningún nodo, ya que se emplea para indicar la ausencia de dirección; por ejemplo, cuando se halla en el campo de dirección fuente, indica que se trata de un host que esta iniciándose, antes de que haya aprendido su propia dirección.

- Túneles dinámicos/automáticos de IPv6 sobre IPv4 (::<dirección IPv4>) – Se denominan direcciones IPv6 compatibles con IPv4, y permiten la retransmisión de tráfico IPv6 sobre infraestructuras IPv4, de forma transparente.

Tabla 11. Direcciones IPv6 compatibles con IPv4

80 bits	16 bits	32 bits
0000…0000	0000	Dirección IPv4

Representación automática de direcciones IPv4 sobre IPv6 (::FFFF:<dirección IPv4>) – permite que los nodos que sólo soportan IPv4, puedan seguir trabajando en redes IPv6. Se denominan “direcciones IPv6 mapeadas desde IPv4”.

Tabla12. Direcciones IPv6 mapeadas desde IPv4

80 bits	16 bits	32 bits
0000…0000	FFFF	Dirección IPv4

3.2.6. **Direcciones Requeridas para cualquier nodo:** Todos los nodos, en el proceso de identificación, al unirse a la red, deben de reconocer como mínimo, las siguientes direcciones:

- Sus direcciones locales de enlace para cada interfaz.
- Las direcciones unicast asignadas.
- La dirección de loopback.
- Las direcciones multicast de todos los nodos.
- Las direcciones multicast solicitadas para cada dirección unicast o anycast asignadas.
- Las direcciones multicast de todos los grupos a los que dicho host pertenece.

Además, en el caso de los routers, tienen que reconocer también:

- La dirección anycast del router de la subnet, para las interfaces en las que esta configurado para actuar como router.
- Todas las direcciones anycast con las que el router ha sido configurado.
- Las direcciones multicast de todos los routers.
- Las direcciones multicast de todos los grupos a los que el router pertenece.

Además, todos los dispositivos con IPv6, deben de tener, predefinidos, los prefijos siguientes:

- Dirección no especificada
- Dirección de loopback
- Prefijo de multicast (FF)
- Prefijos de uso local (local de enlace y local de sitio)
- Direcciones multicast predefinidas
- Prefijos compatibles IPv4

Se debe de asumir que todas las demás direcciones son unicast a no ser que sean específicamente configuradas (por ejemplo las direcciones anycast).

3.2.7. **Reservas de espacio de direccionamiento en IPv6:** A diferencia de las asignaciones de espacio de direccionamiento que se hicieron en IPv4, en IPv6, se ha reservado, que no “asignado”, algo más del 15%, tanto para permitir una fácil transición (caso del protocolo IPX), como para mecanismos requeridos por el propio protocolo.

Tabla13. Reservas de espacio de direccionamiento en IPv6

Estado	Prefijo (en binario)	Fracción del Espacio
Reservado	0000 0000	1/256
No Asignado	0000 0001	1/256
Reservado para NSAP	0000 001	1/128
Reservado para IPX	0000 010	1/128
No Asignado	0000 011	1/128
No Asignado	0000 1	1/32
No Asignado	0001	1/16
Direcciones Unicast Globales Agregables	001	1/8
No Asignado	010	1/8
No Asignado	011	1/8
No Asignado	100	1/8
No Asignado	101	1/8
No Asignado	110	1/8
No Asignado	1110	1/16
No Asignado	1111 0	1/32
No Asignado	1111 10	1/64
No Asignado	1111 110	1/128
No Asignado	1111 1110 0	1/512
Direcciones Unicast Locales de Enlace	1111 1110 10	1/1.024
Direcciones Unicast Locales de Sitio	1111 1110 11	1/1.024
Direcciones Multicast	1111 1111	1/256

Fuente: Facultad de Ciencia y Tecnología Escuela de Informática, Trabajo de grado presentado por

3.3. NOMENCLATURA DE LAS DIRECCIONES.

Tenemos tres formas comunes de representar direcciones IPv6 en texto:

- **x:x:x:x:x:x:x:x**, donde cada x es el valor en hexadecimal de cada grupo de 16 bits de la dirección. No es preciso escribir los ceros a la izquierda de cada campo. Ejemplos:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:0:8:800:200C:417ª

- **x:x::x,** en el caso de que haya grupos contiguos de 16 bits todos cero. Es una abreviatura que serviría para hacer más "cómodo" el uso de algunas direcciones. Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits “cero”, se permite la escritura de su abreviación, mediante el uso de “::”. Este símbolo sólo puede aparecer una vez en la dirección IPv6.

Ejemplos: Las direcciones:

1080:0:0:0:8:800:200C:417A (una dirección unicast)
FF01:0:0:0:0:0:0:101 (una dirección multicast)
0:0:0:0:0:0:0:1 (la dirección loopback)
0:0:0:0:0:0:0:0 (una dirección no especificada)

Pueden representarse como:

1080::8:800:200C:417A (una dirección unicast)

FF01::101 (una dirección multicast)

::1 (la dirección loopback)

:: (una dirección no especificada)

- **x:x:x:x:x:x:d.d.d.d,** donde las x son los seis grupos de 16 bits en hexadecimal de mayor peso de la dirección y las d son los valores decimales de los cuatro grupos de 8 bis de menor peso de la dirección. Esta forma es a veces más conveniente a la hora de manejar entornos mixtos IPv6 e IPv4. Por ejemplos:

0:0:0:0:0:0:13.1.68.3

0:0:0:0:0:FFFF:129.144.52.38

Pueden representarse como:

::13.1.68.3

::FFFF:129.144.52.38

La representación de los prefijos IPv6 se realiza del siguiente modo: dirección-IPv6/longitud del prefijo donde:

- dirección-IPv6 = una dirección IPv6 en cualquiera de las notaciones válidas.

- Longitud del prefijo = valor decimal indicando cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo. Por ejemplo, las representaciones válidas del prefijo de 60 bits 12AB00000000CD3, son:

12AB:0000:0000:CD30:0000:0000:0000:0000/60

12AB::CD30:0:0:0:0/60

12AB:0:0:CD30::/60

Por tanto, para escribir una dirección completa, indicando la subred, podríamos hacerlo como: 12AB:0:0:CD30:123:4567:89AB:CDEF/60

Tabla14. Nomenclatura de direcciones IPv6

Representación Normal	Representación Abreviada	Tipo
1080:0:0:0:8:800:200C:417A	1080::8:800:200C:417A	Unicast
FF01:0:0:0:0:0:0:101	FF01::101	Multicast
0:0:0:0:0:0:0:1	::1	Loopback
0:0:0:0:0:0:0:0	::	No Especificada

De esta forma se permite la asignación directa de direcciones de agregación, direcciones locales, y direcciones multicast, con reservas para OSI NSAP e IPX. El 85% restante queda reservado para uso futuro.

Podemos distinguir las direcciones multicast de las unicast por el valor del octeto de mayor orden de la dirección (FF, o 11111111 en binario, indica multi- cast). En cambio, en el caso de las anycast, no hay ninguna diferencia, sintácticamente hablando, y por tanto, son tomadas del espacio de direcciones unicast..

3.3.1. **Nomenclatura de Los Prefijos:** La representación de los prefijos de direcciones con IPv6 es similar a la que tenemos con CIDR con IPv4, esto es: dirección-ipv6/tamaño-prefijo. Donde dirección-ipv6 es alguna de las notaciones vistas en la sección anterior y tamaño-prefijo es un valor decimal que especifica cuantos bits de la dirección corresponden al prefijo.

Por ejemplo, el prefijo de la UJI en hexadecimal es **3FFE33300002**, que son 48 bits, lo podemos escribir como:

3FFE:3330:0002:0000:0000:0000:0000:0000/48

3FFE:3330:2:0:0:0:0:0/48

3FFE:3330:2::/48

Si queremos escribir la dirección y el prefijo, no hace falta que escribamos los dos de forma explícita. Por ejemplo, una dirección IPv6 de la misma UJI con su prefijo asociado quedará **3FFE:3330:2:1:250:BAFF:FE7A:E67E/48**.

4. REPRESENTACION DE LA CABECERA DE IPv6.

El paquete de ipv6 es cargado en un frame de red local como en ipv4; sin embargo, el encabezado de ipv6 consiste en 2 partes. Estas son el encabezado base de ipv6, más encabezado de extensión opcional. Con o sin algún encabezado de extensión opcional, un constraint de tamaño fijo en uniframe de red local debe ser respetado. Por ejemplo, la mayor cantidad de datos que puede ser cargada en un frame Ethernet es 1500 octetos. Si el encabezado de extensión es añadidos al paquete de ipv6, menos datos de aplicación pueden ser enviados. El host y/o su sistema operativo deben tener un mecanismo para manejar esto.

Figura 4. Representación de la cabecera de IPv6.

Fuente: http://www.tcpip6.com/images/index.1.gif

La cabecera de un paquete IPv6 es, sorprendentemente, más sencilla que la del paquete IPv4. Y recordemos que además la funcionalidad del protocolo IPv6 es mucho mayor.

La cabecera de un paquete IPv4 es variable, por lo que necesita un campo de tamaño o longitud. Sin embargo, para simplificar la vida de los enrutadores, IPv6

utiliza un tamaño de cabecera fijo de 40 bytes, que componen un total de ocho campos:

El campo Versión: El campo Versión es de 4 bits de largo e identifica la versión del protocolo. Para ipv6, Versión = 6. Nótese que este es el único campo con una función y posición que es consistente entre ipv4 e ipv6. Todos los demás son diferentes de alguna forma. El tener este campo al comienzo del paquete permite una rápida identificación de la versión del IP y el paso de ese paquete al protocolo de proceso apropiado: ipv4 o ipv6.

El campo Traffic Class: El campo Traffic Class es de 8 bits de largo y su intención para los nodos de origen y/o nodos de reenvío es identificar y distinguir entre diferentes clases o prioridades de paquetes ipv6. (En la primera publicación de la especificación ipv6, RFC 1883, este campo se llamaba Priority, reflejando su función. Mejoras en este trabajo lo renombraron como campo Class, con una longitud de 4 bits. Trabajo adicional en el IPNG Meeting, en el plenario de agosto 1997 de Munich expandió este campo a 8 bits y redujo el campo Flow Label de 24 bits a 20.

El nuevo término Traffic Class, definido en RFC 2460, identifica más el propósito de este campo.) Este campo reemplaza las funciones que fueron provistos por el campo Type of Service de ipv4, permitiendo la diferenciación entre categorías del servicio de transferencia de paquetes. Esta función es comúnmente referida como “Servicio de Diferenciación”. Al tiempo de este escrito, algunos experimentos están siendo conducidos en esta área de la tecnología, especialmente en soporte de transporte de señal dependiente del tiempo, como voz o video sobre IP. Estos 3 requerimientos generales para el campo Traffic Class son stated en RFC 2460:

- Para paquetes que son originados en un nodo por un protocolo de capa más alta, ese protocolo de capa más alta especificaría el valor de los bits del campo Traffic Class. El valor por default es cero.

- Nodos que soportan una función particular que usa bits de Traffic Class pueden cambiar los valores de los bits en paquetes que ellos originan, reenvían o reciban. Sin un nodo no soporta esa función particular, no debe cambiar ninguno de los bits de Traffic Class.

- Los protocolos de capa más alta no deben asumir que los valores de los bits de Traffic Class en un paquete recibido son los mismos valores que fueron originalmente transmitidos. En otras palabras, un nodo intermediario puede ser permitido a cambiar (y haber cambiado) los bits de Traffic Class en tránsito.

Dos de los otros documentos, RFC 2474 y RFC 2475, discuten el concepto e implementación de servicios de diferenciación, que tienen la intención de discriminar entre varios tipos de servicio, requiriendo el estado por carga y señalización en cualquier salto. RFC 2474 define un campo Differentiated Services que reemplaza el campo Type of Service de ipv4. RFC 2475 es más general en la naturaleza, y describe una arquitectura para servicios diferenciados y las funciones a ser provistos. Esta arquitectura es descrita en 2 componentes: uno trata con el reenvío de paquetes, y el otro trata con las políticas que determinan los parámetros usados en la ruta de reenvío. Una analogía es dibujada desde las diferencias entre reenvío de paquetes y ruteo de paquetes. El reenvío es el proceso por paquete que determina (de una tabla de ruteo) a qué interface un paquete debe ser enviado. (En otras palabras, si el encabezado de paquete identifica la subred en Kansas City, entonces envía este paquete por la interfase #5). Rutear es un proceso más complejo que determina las entradas en esa tabla

de ruteo, y (posiblemente más importante) la política que determina cómo esa tabla es construida. (Por ejemplo, si el enlace a Kansas City se cae, entonces envía el paquete vía Chicago en vez de vía Denver). Como se discutió en RFC 2474, los comportamientos de la ruta de reenvío son mejor entendidos que las políticas que configuran los parámetros que afectan la ruta de envío.

RFC 2474 se concentra en el componente de la ruta de reenvío que determina el comportamiento por saltos (PHB) de los paquetes, más que en la política y parámetros de configuración del componente. Los PHB's incluirían tratamiento específico que un paquete individual recibe, con las cosas del mensaje de que son requeridas para hacer eficiente este tratamiento especial.
Un PHB suficientemente definido debería permitir la construcción de servicios predecibles.

RFC 2474 define el formato para el campo Differentiated Services (DS) que contiene 2 subcampos. El subcampo Differentiated Services Codepoint (DSCP) selecciona el PHB que un paquete experimenta en cada nodo. El campo Currently Used (CU) es reservado para futuras definiciones. El campo Type of Service de ipv4 consiste en 3 partes: un campo Precedence de 3 bits, 3 bits que especifican banderas (Delay, Throughput y Reliability, o DTR) y 2 bits que son reservados. RFC 2474 define un grupo de puntos de código, el patrón de bits para el subcampo DSCP sería XXX000 (en binario, donde x sería cero o uno). Note que los 3 "X" bits corresponden con las mismas posiciones de los bits de DTR; sin embargo, RFC 2474 establece que ningún atento es hecho para mantener compatibilidad hacia atrás con esos bits de banderas. También, el punto de código con valor 000000 es asignado al PHB por default, que es definido como el comportamiento de envío "común, de más esfuerzo". (Nótese la comparación con el campo de precedencia, éste correspondería con el valor para precedencia de "rutina"). Otros valores de punto de código han sido agrupados en pools, con un

pool reservado para tareas basadas en estándares, y otros, para propósitos de uso local y experimental. RFC 2474 describe estas tareas en detalle más grande.

El Campo Flow Label: El campo Flow Label es de 20 bits de longitud, y puede ser usado por un host para solicitar manejo especial para ciertos paquetes, como aquellos con una calidad de servicio de no default o de tiempo real. En esta primera versión de la especificación ipv6, RFC 1883, este campo era de 24 bits de longitud, pero 4 de estos bits han sido ahora colocados en el campo Traffic Class.
Un flujo es una secuencia de paquetes enviados a un destino unicast o multicast que necesita manejo especial por los routers ipv6 que intervienen. Todos los paquetes pertenecientes a un mismo flujo debe ser enviado con la misma dirección fuente, dirección destino y etiqueta de flujo. Un ejemplo de un flujo sería paquete que soporta un servicio en tiempo real, como audio o vídeo.

Flow Label es usado por esa fuente para etiquetar esos paquetes que requieren manejo especial por el nodo ipv6. Si un host o router no soporta funciones de Flow Label, el campo es fijado a cero en el origen e ignorado en la recepción. Múltiples flujos de datos pueden existir entre una fuente y un destino, así como tráfico de datos que no es asociado con un flujo particular. Un flujo único es identificado por la combinación de una dirección fuente y una etiqueta de flujo que no sea cero. La etiqueta de flujo es un número seudo-aleatorio elegido del rango de 1 a FFFFFH (donde H denota notación hexadecimal). Esa etiqueta es usada como una clave hash por router para buscar el estado asociado con ese flujo.

RFC 1809, “Usando el Campo Flow Label en ipv6”, describe algunas de las investigaciones más tempranas en la materia, como el campo Class, Flow Label es sujeto de investigación actualmente y puede cambiar según la experiencia de la industria madura.

El campo Payload Field: El campo Payload Field es un entero no asignado de 16 bits que mide la longitud, dada en octetos, de la carga (ejemplo el balance del paquete ipv6 que sigue al encabezado base de ipv6). Nótese que los encabezados de extensión opcional son considerados parte de la carga, junto con cualquier protocolo de capa más alta, como TCP, FTP y así.

El campo Payload Length es similar al campo Total Length de ipv4, excepto que las 2 medidas operan en diferentes campos. Payload Length (ipv6) mide los datos después del encabezado, mientras Total Length (ipv4) mide los datos y el encabezado. Las cargas más grandes de 65,535 son permitidas y son llamadas Cargas Jumbo. Para indicar una carga jumbo, el valor de Payload Length está fijado en cero y la longitud de la carga actual es especificada en una opción que es cargada en la extensión del encabezado Hop-by-Hop.

El Campos de Siguiente Cabecera (Next Header Field): El campo Next Header tiene 8 bits de longitud e identifica el encabezado inmediatamente siguiente del encabezado de ipv6. Este campo usa los mismos valores que el campo Protocol de ipv4. Ejemplos:

Value	Header
0	Hop-by-Hop Options
1	ICMPv4
4	IP in IP (encapsulation)
6	TCP
17	UDP
43	Routing
44	Fragment
50	Encapsulating Security Payload
51	Authentication

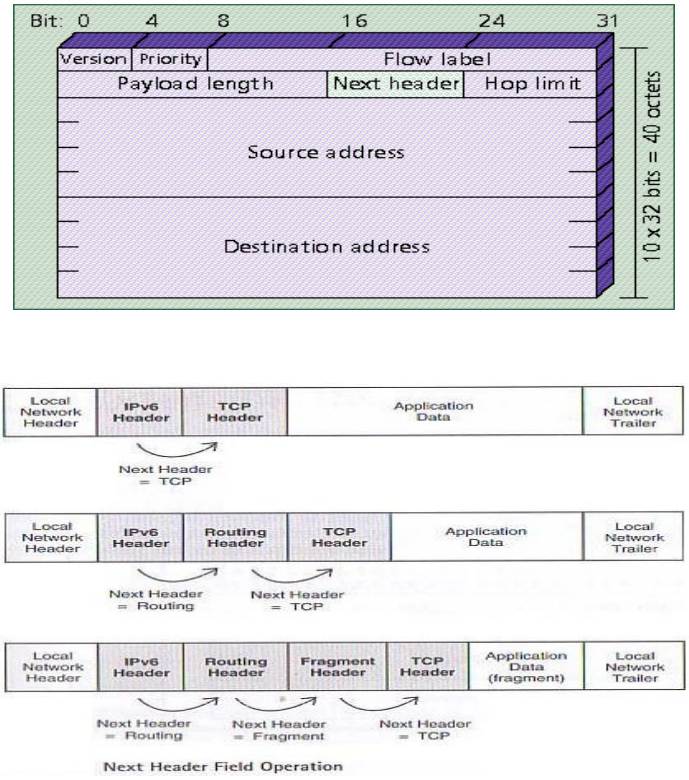
58 ICMPv6

59 None (No Next Header)

60 Destination Options

Un paquete ipv6, que consiste en un paquete de encabezado ipv6 más su carga, puede consistir de cero, uno o más encabezado de extensión. Muchos de los encabezados de extensión también emplean un campo Next Header. Note los valores de los campos Next Header en cada ejemplo mostrado en la figura 5.

Figura 5. Encabezado Next Header



Fuente: Facultad de Ciencia y Tecnología Escuela de Informática, Trabajo de grado presentado por Darwin Lamarck Santana Yunes, Santo Domingo, D.N. 2004

En el primer caso ningún encabezado de extensión es requerido, Next Header = TCP, y el encabezado TCP y cualquier protocolo de capa más alta le sigue. En el segundo ejemplo, un header Routing es requerido. Luego, Next Header de ipv6 = Routing; en el header Routing, Next Header = TCP, y el encabezado TCP y cualquier protocolo de capa más alta le sigue. En el tercer caso, tanto el header Routing como Fragment son requeridos, con los campos Next Header identificados acordemente.

El campo Hop Limit: El campo Hop Limit tiene 8 bits de longitud, y va decreciendo en 1 por cada nodo que reenvía el paquete. Cuando Hop Limit se iguala a cero, el paquete es descartado y un mensaje de error es retornado. Este campo es similar al campo Time-to-Live (TTL) encontrado en ipv4, con una excepción clave. El campo Hop Limit (ipv6) mide el máximo de saltos (hops) que pueden ocurrir mientras el paquete es enviado por varios nodos. El campo TTL (ipv4) puede ser medido en saltos o segundos. Note que con Hop Limit usada en ipv6, la base del tiempo no está disponible más.

El campo Source Address: El campo Source Address es un campo de 128 bits que identifica el originador del paquete. El formato de este campo es más ampliamente definido en RFC 2373.

El campo Destination Address: El campo Destination Address es un campo de 128 bits que identifica el destinatario que tiene la intención de recibir el paquete. Una importante distinción es la de que el destinatario que tiene la intención de recibir el paquete puede no ser el destinatario final, como el header Routing puede ser empleado para especificar la ruta que el paquete toma desde su fuente, a través de destinatario(s) intermedio(s), y así hasta su destinatario final.

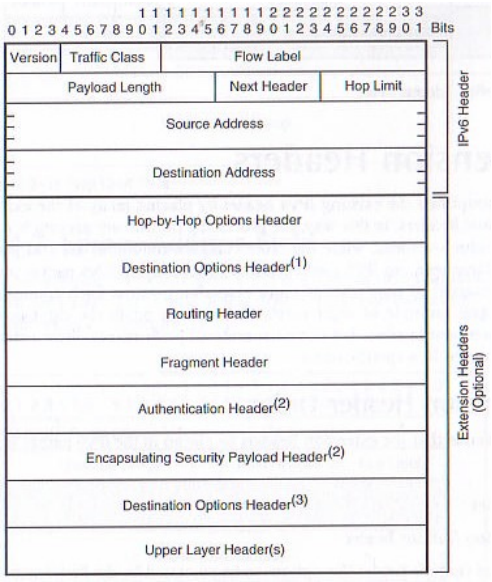
4.1. ENCABEZADOS DE EXTENSIÓN

El diseño de ipv6 simplifica el encabezado existente de ipv4 colocando muchos de los campos existentes en encabezado opcionales. De esta forma, el procesamiento de paquetes ordinarios no es complicado por uso indebido de encabezados, mientras las condiciones más complejas son todavía provistas.

Como hemos visto, un paquete ipv6, que consiste de un paquete ipv6 más su carga, puede consistir de cero, uno o más encabezados de extensión. Cada encabezado de extensión es un múltiple integral de 8 octetos de longitud para retener la alineación de 8 octetos para encabezados subsecuentes. Para óptimo desempeño del protocolo, estos encabezados de extensión son colocados en un orden específico.

4.1.1. Orden de los Encabezados de Extensión: RFC 2460 recomienda que los encabezados de extensión sean colocados en el paquete IPv6 en un orden particular:

Tabla15. Orden de los Encabezados de Extensión

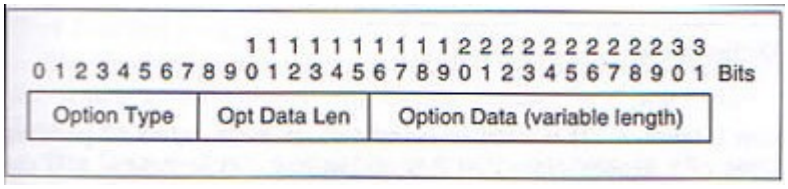


Fuente: Facultad de Ciencia y Tecnología Escuela de Informática, Trabajo de grado presentado por Darwin Lamarck Santana Yunes, Santo Domingo, D.N. 2004

- ipv6 Header
- Hop-by-Hop Options Header
- Destination Options Header (para opciones a ser procesadas por el primer destino que aparece en el campo Destination Address de ipv6, más destinos subsecuentes listados en el Routing Header)
- Routing Header
- Fragment Header
- Authentification Header (como se detalla en RFC 2402)
- Encapsulating Security Payload Header (como se detalla en RFC 2406)
- Destination Options Header (para opciones a ser procesadas por el destino final solamente)
- Upper Layer Protocol Header (TCP, etc.)

4.1.2. Opciones de los Encabezado de Extensión: Dos de los encabezados de extensión, Hop-by-Hop y Destination Options, pueden cargar una o más opciones que identifican más allá de los parámetros de operación de red. Estas opciones son codificadas usando el formato TLV (Tipo-Longitud-Valor) que es especificado por el lenguaje de descripción de mensajes Abstract Syntax Notation 1 (ASN.1) (TLV es ampliamente usado entre protocolos de comunicación, incluyendo el Simple Network Management Protocol, SNMP.) La opción formato incluye un campo Option Type de 8 bits que identifica la longitud del campo Option Data dada en octetos; y un campo Option Data de longitud variable.

Figura 6. Opciones de los Encabezados de Extensión



Fuente: Facultad de Ciencia y Tecnología Escuela de Informática, Trabajo de grado presentado por Darwin Lamarck Santana Yunes, Santo Domingo, D.N. 2004

Los dos bits de orden más alto del campo Option Type, especifican como tener opciones que son irreconocibles en el nodo de procesamiento de ipv6:

Tabla 16. Bits del campo Option Type irreconocibles en el nodo de procesamiento de ipv6

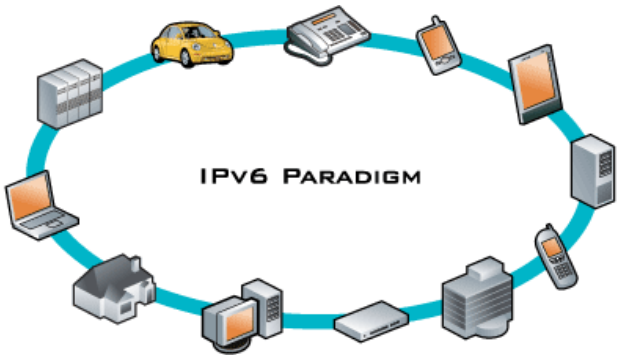
Valor	Acción
00	Salta la opción y continúa procesando el encabezado.
01	Descarta el paquete.
10	Descarta el paquete y envía un mensaje ICMP Problema de Parámetro (Tipo de Opción irreconocible) a la fuente.
11	Descarta el paquete y envía un mensaje ICMP problema de parámetro (Tipo de Opción irreconocible) a la fuente (solo si el destino no era multicast).

4.2. SEGURIDAD EN EL PROTOCOLO IPv6

En la arquitectura IPv6, tanto el encabezado de extensión Authentification (AH) como Encryption (ESP) han sido definidos y son requeridos para una implementación completa de ipv6. Los encabezados Authentification y Encryption son parte del trabajo en curso en IP Security (Ipsec), que es direccionar aplicaciones para ipv4 e IPv6. Un archivo de los estándares Ipsec está disponible desde el Virtual Private Networking Consortium.

Las funciones de autentificación y cifrado (encryption) han sido separadas de tal manera que las implementaciones individuales pueden usar una o ambas de las funciones como sean necesitadas por las aplicaciones de capa más alta. Cifrado, por ejemplo, puede ser restringida para regulación gubernamental; así, solo la autentificación está implementada en algunos casos.

Figura 7. Seguridad IPV6



Fuente: http://www.ipv6summit.com.mx/imagenes/paradigmaIPv6.jpg

4.2.1. Arquitectura de Seguridad IP (IPSEC): La meta de IP Security (Ipsec) es proveer seguridad basada en criptografia, interoperable para IPv4 e IPv6. Como estas funciones de seguridad son ofrecidas en la capa IP, la protección para tanto IP como cualquier capa más alta de protocolos es

proveída. Ipsec habilita a un sistema seleccionar los protocolos de seguridad requeridos, determinar los algoritmos que serán usados para el servicio de seguridad, e implementar cualquier clave criptográfica que sea requerida para proveer estos servicios. Ipsec puede ser usado para proteger los caminos de comunicación entre 2 hosts, entre 2 gateways de seguridad o entre un host y un gateway de seguridad. La arquitectura de seguridad para IPv6 está definida en RFC 2401. Este documento incluye las siguientes definiciones base para varios sistemas y procesos:

- **Control de Acceso**: El proceso de prevenir acceso no autorizado a un recurso de red.

- **Autentificación:** La verificación de la identidad de la fuente reclamada de los datos (también conocido como *autentificación del origen de los datos*), más la propiedad que un paquete IP individual no ha sido modificado (integridad sin conexión).

- **Integridad:** La propiedad de asegurar que los datos son transmitidos desde una fuente o destino sin modificación sin detectar. *Integridad sin conexión* es un servicio que detecta la modificación de un paquete IP individual, sin importar el orden del paquete en un stream de datos. *Integridad anti-replay* (o *integridad de secuencial parcial*) detecta la llegada de paquetes IP duplicados dentro de una ventana.

- **Confidencialidad:** La protección de los datos de acceso no autorizado.

- **Cifrado:** Un mecanismo para transformar los datos desde una forma inteligente (*plaintext*) a una forma no inteligente (*ciphertext*), así proveyendo confidencialidad.

- **Indice de Parámetros de Seguridad (SPI):** Un valor de 32 bits que es usado para distinguir entre diferentes Asociaciones de Seguridad (SAs) terminando en el mismo destino y usando el mismo protocolo IPSec.

- **Asociación de Seguridad (SA):** Una simple (unidireccional) conexión lógica, creada para propósitos de seguridad. Tanto AH como ESP hacen uso de SAs. La SA es una simple conexión lógica (de una vía) que provee servicios de seguridad a los AH o ESP pero no a ambos. Así, si tanto un AH como un ESP se les aplica el mismo stream de tráfico, 2 SA debe ser asignadas. Además, sesiones de comunicaciones bidireccionales, autentificadas entre 2 hosts tendrán 2 SA en uso – uno en cada dirección. La SA puede incluir: el algoritmo de autentificación, el modo del algoritmo y claves; el algoritmo de cifrado, el modo del algoritmo, el transform y claves; tiempo de vida de la clave, o tiempo en que la clave debe ser cambiada, y así. Dos tipos de SA son definidos: modo de transporte y modo túnel.

- **Gateway de Seguridad:** Un sistema que actúa como un sistema intermediario entre 2 redes. Los hosts o redes en el lado externo del gateway de seguridad son vistos como sistemas no confiables (o menos confiables), mientras que los hosts o redes en el lado interno son vistos como sistemas confiables (o más confiables).

- **Análisis de Tráfico:** El análisis del flujo de tráfico en la red para el propósito de deducir información que es útil para un adversario. Ejemplos de este tipo de información son la frecuencia de transmisión, las identidades de las partes que conversan, tamaño de los paquetes, identificadores de flujos usados, y así.

- **Subred Confiable:** Una red que contiene hosts y routers que se confían entre sí para no comprometerse en ataques activos o pasivos, y que confían que el canal de comunicación subyacente (ejemplo: un Ethernet) no está siendo atacado.

- **Asociación de Seguridad en Modo de Transporte***:* Una SA entre 2 hosts, primariamente proveyendo seguridad para los protocolos de capa más alta.

- **Asociación de Seguridad en Modo de Túnel***:* Una SA aplicada a un túnel de IP, primariamente proveyendo seguridad para un paquete en el túnel. Las siguientes secciones discuten las varias SA que son posibles, más la manera en que AH y ESP son implementadas dentro de estas SA.

- **Encriptación:** Encapsulated Security Payload (ESP) provee confidencialidad (cifrado), autentificación del origen de los datos, integridad sin conexión, servicio antireplay y confidencialidad de flujo de tráfico limitado (guardando contra análisis de tráfico). Tanto AH como ESP pueden ser usados para control de acceso, basado en los flujos de tráfico y distribución de claves en uso. El alcance de la autentificación ofrecido por ESP no es tan amplio como el proveído por AH. ESP está definido en RFC 2406. En modo de transporte, ESP es considerado una carga útil de extremo a extremo, así que debe ser colocado después de los encabezado hop-by-hop, routing y fragmentation. El encabezado (o los encabezados) Destination Options pueden ser colocado antes o después de ESP. Sin embargo, como ESP protege solo los campos que van después del encabezado ESP, colocar el encabezado Destination Options después de ESP es deseable.

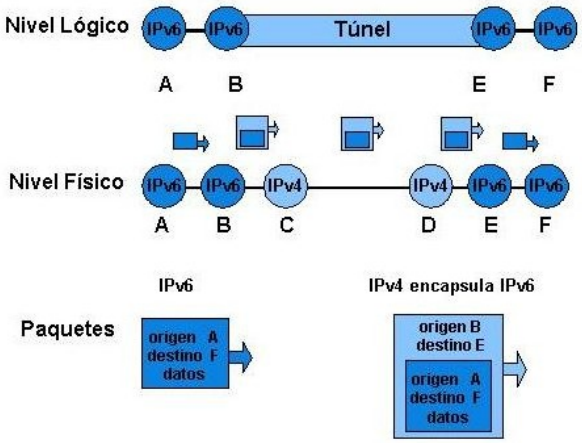
5. MECANISMOS DE TRANSICION

5.1. MECANISMOS DE TRANSICION A IPv6

El cambio de IPv4 a IPv6 ya ha comenzado, pero no puede hacerse instantáneamente, sino que la implantación de IPv6 es paulatina y durante unos 20 años se espera que convivan ambos protocolos. Existe una serie de mecanismos que permitirán la convivencia y la migración progresiva tanto de las redes como de los equipos de usuario. Estas técnicas pueden ser utilizadas incluso de forma combinada.

5.1.1. Túneles: Los **túneles** permiten conectarse a redes IPv6 "saltando" sobre redes IPv4.Estos túneles trabajan encapsulando los paquetes IPv6 en paquetes IPv4. De esta manera, los paquetes IPv6 pueden ser enviados sobre una infraestructura IPv4. Los extremos finales del túnel son siempre los encargados de realizar la operación de encapsulado del paquete/es IPv6 en IPv4.

Figura 8. Túneles



Fuente: http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/ipv6/ipv6_archivos/image021.jpg

Estos túneles pueden ser utilizados de distintas formas:

- Router a router: Routers con doble pila (IPv4/IPv6) se conectan mediante una infraestructura IPv4 y transmiten tráfico IPv6. El túnel comprende un segmento que incluye la ruta completa, extremo a extremo, que siguen los paquetes.

- Host a router: Host con doble pila se conectan a un router intermedio (también con doble pila), alcanzable mediante una infraestructura IPv4. El túnel comprende el primer segmento de la ruta seguido por los paquetes.

- Host a Host: Host con doble pila interconectados por una infraestructura IPv4.

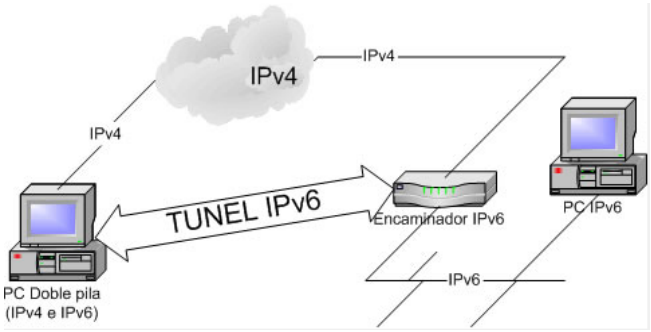
  El túnel comprende la ruta completa que siguen los paquetes.

- Router a Host: Routers con doble pila que se conectan a host también con doble pila. El túnel comprende el último segmento de la pila.

Los túneles se clasifican según el mecanismo por el que el nodo que realiza el encapsulado determina la dirección del nodo extremo del túnel. En los dos primeros casos (router a router y host a router), el paquete IPv6 es tunelizado a un router. El extremo final de este tipo de túnel, es un router intermedio que debe desencapsular el paquete IPv6 y reenviarlo a su destino final. En este caso, el extremo final del túnel es distinto del destino final del paquete, por lo que la dirección en el paquete IPv6 no proporciona la dirección IPv4 del extremo final del túnel. La dirección del extremo final del túnel ha de ser determinada a través de información de configuración en el nodo que realiza el túnel. Es lo que se denomina “túnel configurado”, describiendo aquel tipo de túnel donde el extremo final del túnel es explícitamente configurado. En los otros casos (host a host y router a host), el paquete IPv6 es tunelizado, durante todo el recorrido, a su nodo destino. El extremo final del túnel es el nodo destino del paquete, y por tanto, la dirección IPv4 está contenida en la dirección IPv6. Este caso se denomina “túnel automático”. El desencapsulado, en el extremo final del túnel, realiza la función opuesta.

5.1.2. Pila dual (RFC 2893): La pila dual hace referencia a una *solución de nivel IP con pila dual*, que implementa las pilas de ambos protocolos, IPv4 e IPv6, en cada nodo de la red. Cada nodo de pila dual en la red tendrá dos direcciones de red, una IPv4 y otra IPv6.

Figura 9. Túneles con Pila dual



Fuente: http://www.derechonntt.com/wp-content/uploads/tunelipv6.jpg

Pros: Fácil de desplegar y extensamente soportado.

Contras: La topología de red requiere dos tablas de encaminamiento y dos procesos de encaminamiento. Cada nodo en la red necesita tener actualizadas las dos pilas.

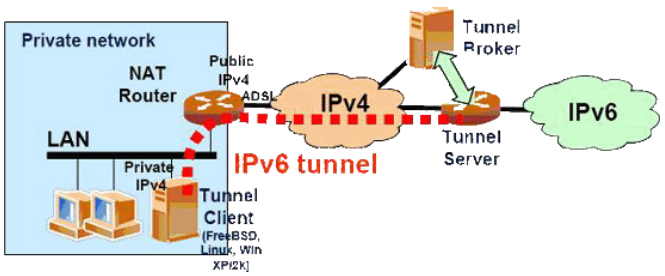
5.1.3. Over 4 (Transmisión de IP6 sobre dominios IPv4, RFC 2529): Este mecanismo permite a hosts IPv6 aislados, sin conexión directa a routers IPv6, ser totalmente funcionales como dispositivos IPv6. Para ello se emplean dominios IPv4 que soportan multicast como su enlace local virtual. Es decir, usamos multicast IPv4 como su "ethernet virtual". De esta forma, estos host IPv6 no requieren direcciones IPv4 compatibles, ni túneles configurados. Los extremos finales del túnel se determinan mediante ND. Es imprescindible que la subred IPv4 soporte multicast.

5.1.4. To 4 (Conexión de dominios IPv6 sobre redes IPv4): Es un mecanismo para asignar un prefijo de dirección IPv6 a cualquier sitio que tenga al

menos una dirección IPv4 pública. De esta forma, dominios o host IPv6 aislados, conectados a infraestructuras IPv4 (sin soporte para IPv6), pueden comunicar con otros dominios o host IPv6 con una configuración manual mínima. Este mecanismo funciona aún cuando la dirección IPv4 pública es única y se accede a la red mediante mecanismos NAT, que es el caso mas común en las redes actuales para el acceso a Internet a través de ISP's.

5.1.5. "Tunnel Server" y "Tunnel Broker": El "tunnel broker" es el lugar donde el usuario se conecta para registrar y activar "su túnel". El "broker" gestiona (crea, modifica, activa y desactiva) el túnel en nombre del usuario. El "tunnel server" es un router con pila doble (IPv4 e IPv6), conectado a Internet, que siguiendo órdenes del "broker" crea, modifica o borra los servicios asociados a un determinado túnel/usuario. El mecanismo para su configuración es tan sencillo como indicar, en un formulario Web, datos relativos al S.O. La dirección IPv4, un "apodo" para la máquina, y el país donde está conectada. El servidor de túneles crea los registros DNS, el extremo final del túnel, y genera un script para la configuración del cliente. Estos mecanismos se hacen indispensables para labores de investigación, dado que se requisen direcciones IPv6 y nombres DNS permanentes. Hemos encontrado ejemplos de estos sistemas en www.freenet6.net y carmen.cselt.it/ipv6/download.html.

Figura 10. Tunnel server



Fuente: http://www.6sos.net/images/imagen_espanol_proto-41.gif

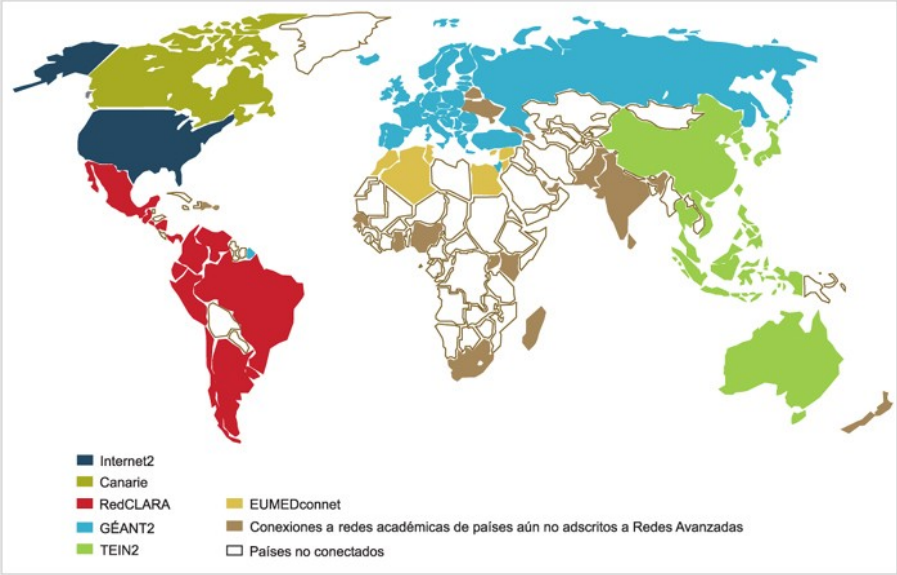
5.2. SERVICIOS DE RED BASADOS EN IPV6.

Una vez alcanzada la conectividad interna en el segmento escogido se definen e implementan servicios de red sobre IPv6, tales como son seguridad, servicios de monitoreo y publicación Web, servicio de transferencia de archivos, servicio de mensajería, etc.

6. REDES AVANZADAS EN LATINOAMERICA

En términos generales, las Redes Avanzadas se agrupan en el mundo de acuerdo a zonas geográficas. Así, las Redes Nacionales de Investigación y Educación (NREN) o Redes Avanzadas de cada país, van integrando consorcios que no son otra cosa que redes mayores, unidas en una gran troncal (*backbone*). Estas redes mayores, a su vez establecen Memorandums de Entendimiento (MoU) o asociaciones que les permiten interconectarse, permitiendo la interconexión global de las Redes Avanzadas: es el fin de las barreras para el desarrollo de la investigación, la ciencia, la educación y la innovación.

Figura 11. Redes Avanzadas



Fuente: http://www.reuna.cl/documentos/IMG2006/MAPA_REDES_AVANZADAS.jpg

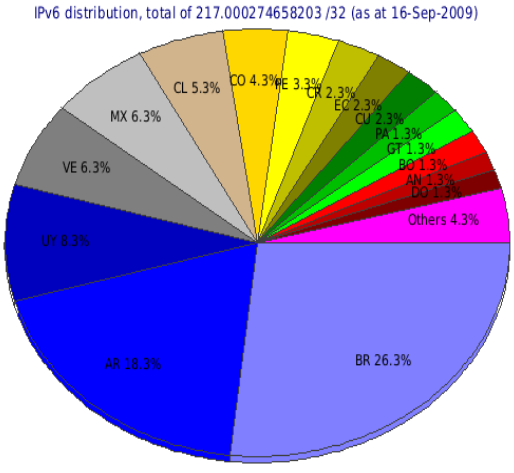
El desarrollo de Internet comercial ha llegado en la actualidad a límites fuera de lo esperado, con un nivel de tráfico que se duplica cada 4 meses. El alto consumo de

ancho de banda por parte de las aplicaciones que manejan voz, video y multimedia en general, ha logrado que Internet se convierta en una red que por su alto tráfico, no garantiza calidad de servicio, ni permite reservación de recursos como ancho de banda, lo que la convierte en una red impredecible y con poca capacidad para manejar aplicaciones o tecnologías donde el tiempo de respuesta es prioritario. Es por esta razón que nació la iniciativa de las Redes Avanzadas, lo cual implica la urgencia de diseñar redes con capacidad de transportar Gigabits de información en un segundo, y la necesidad de que a través de aplicaciones avanzadas se realice la colaboración entre personas y el acceso interactivo a la información y otros recursos en formas que no son posibles en el Internet de ahora

6.1. IMPLEMENTACION DE IPV6 EN LA REGIÓN

Entre el año 2010 y 2012, aproximadamente, se prevé que se produzca el agotamiento de las direcciones IPv4 que aún no han sido utilizadas. Por ello la trocal (Backbone) en Latinoamérica ya se encuentra lista para el despliegue y la implementación de IPv6 como se muestra a continuación.

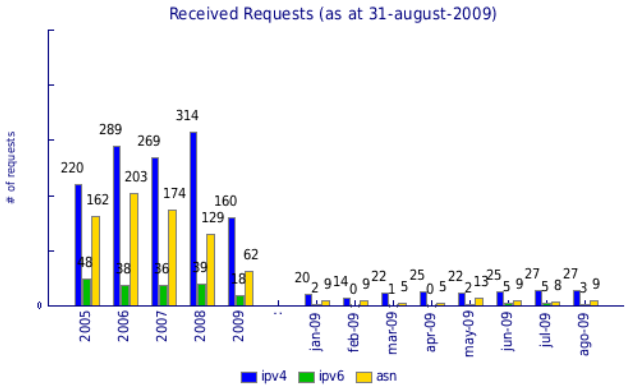
Figura 12: Distribución de IPv6 en la región de LACNIC



Fuente: http://lacnic.net/v6stat/ipv6-country.png

La Fig. 12 de torta indica como es la distribución de las direcciones IPv6, en número de /32, ya asignadas por LACNIC (Registro de Direcciones de Internet para América latina y el Caribe) entre los países de la región.

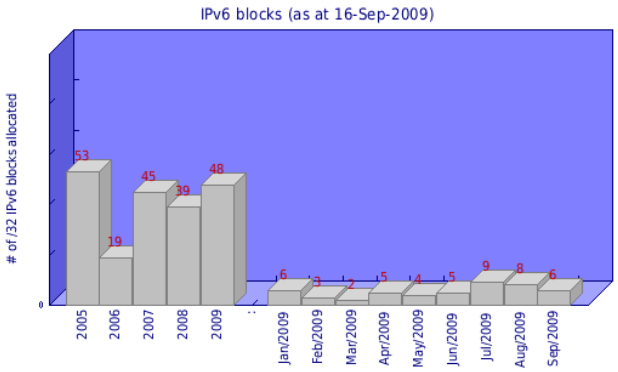
Figura13. Solicitudes



Fuente: http://portalipv6.lacnic.net/es/ipv6/estad-sticas/ipv6/solicitudes

Esta gráfica indica la cantidad de solicitudes para recursos Internet (IPv4, IPv6, ASN) recibidas por LACNIC a cada mes. Y también un comparativo con los años anteriores

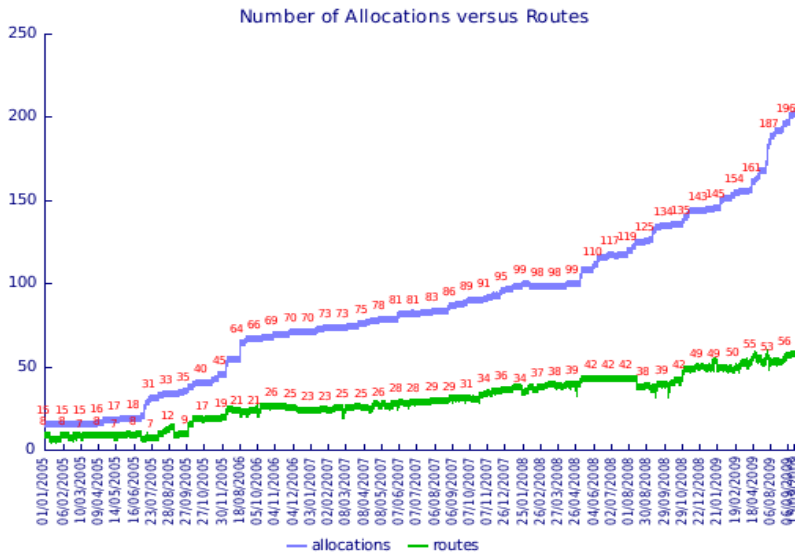
Figura14. Número de Bloques /32 de IPv6 asignados



Fuente: http://lacnic.net/v6stat/ipv6-stat.png

Esta gráfica indica la cantidad de direcciones IPv6 asignadas por LACNIC. Dichas asignaciones están representadas en bloques de prefijo /32

Figura15. Número de Asignaciones y Distribuciones

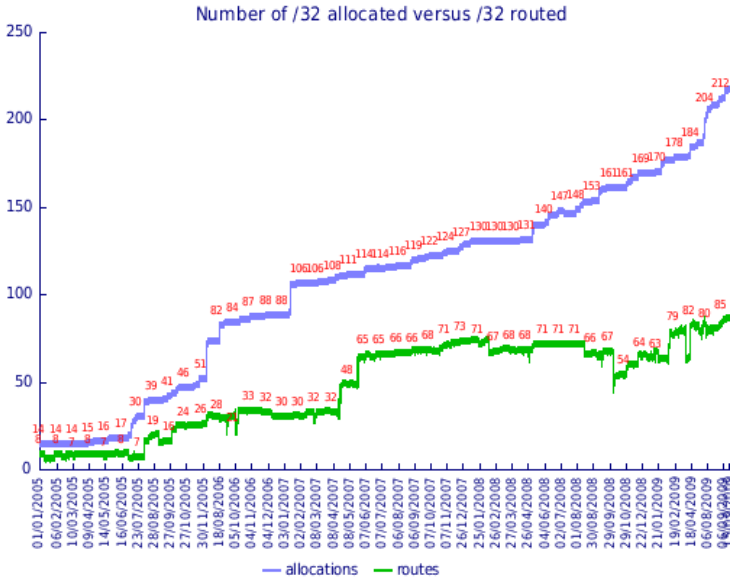


Fuente: http://lacnic.net/v6stat/stats-metrica15.png

Número de Distribuciones y Asignaciones realizadas por LACNIC: Esta métrica mide el número total de distribuciones y asignaciones IPv6 hechas por LACNIC. Se incluyen las hechas a recursos críticos, ISPS y en el futuro a usuarios finales.

Número de Distribuciones y Asignaciones realizadas por LACNIC ruteadas: Esta métrica mide del número total de distribuciones y asignaciones IPv6 hechas por LACNIC cuantas están presentes en la tabla global de direcciones. Se incluyen las hechas a recursos críticos, ISPS y posible PI en el futuro.

Figura16. Número de Direcciones Asignadas /32



Fuente: http://lacnic.net/v6stat/stats-metrica26.png

Número de bloques /32 equivalentes distribuidos y asignados por LACNIC: Esta métrica mide el número total de direcciones IPv6 distribuidas y asignadas en unidades de /32.

Número de bloques /32 equivalentes distribuidos y asignados por LACNIC ruteados: Esta métrica mide el número total de direcciones IPv6 distribuidas y asignadas en unidades de /32 que estén presentes en la tabla global de direcciones.

6.1.1. ARIU – Red de Interconexión Universitaria. Argentina: La ARIU (Asociación Redes de Interconexión Universitaria) es un emprendimiento conjunto de las universidades nacionales e institutos universitarios integrantes del CIN (Consejo Interuniversitario Nacional) con el propósito de llevar adelante la gestión de redes para facilitar la comunicación informática a nivel nacional e internacional de las universidades nacionales, promoviendo la investigación informática,

tecnológica, educativa y el desarrollo cultural en el área de las tecnologías de información y comunicaciones. En lo que respecta a la conexión internacional, RIU posee conexión en modo nativo desde el nodo central de la red hacia las redes académicas de prestaciones avanzadas de Latinoamérica y el mundo. En cuanto a la Internet comercial, se encuentra en fase de implementación y en cuanto a la conectividad interna, desde el nodo central hasta las 38 Universidades que componen la red se está trabajando con un esquema de túneles configurados / automáticos y está en fase de implementación el modo nativo en la VPN que conforma la red. Para lograr este objetivo se trabaja junto al proveedor a los fines de terminar de implementar en todo el territorio nacional.

6.1.2. BT Latinoamérica Argentina: La red MPLS de BT Latinoamérica cuenta soporte para IPv6 desde comienzos del año 2007 utilizando el "feature" 6PE. Este "feature" permite a los routers de borde operar en el modo "dual-stack" soportando IPv4 e IPv6 simultáneamente, incorporando también algunas funcionalidades nuevas en el plano de envío y de control para transportar los paquetes IPv6 en una red MPLS. La red MPLS de BT Latinoamérica es utilizada transportar el tráfico de Internet IPv4 e IPv6 de nuestros clientes. A nivel IPv6 la red cuenta con varios upstream providers conectados en el POP de Miami y con gran cantidad de peerings en varios países donde la red tiene presencia. Hasta el momento sólo tenemos clientes con IPv6 en Argentina y Venezuela, pero seguimos promoviendo el despliegue de IPv6 con nuestros clientes en toda la región para que nuestro tráfico IPv6 sea cada vez mayor. La presentación realizada en el evento LACNIC X sobre nuestra implementación general de IPv6 se encuentra en el siguiente link: http://www.lacnic.net/sp/eventos/lacnicx/flip6.html. La presentación realizada en el evento LACNIC XI sobre nuestra implementación de IPv6 en Venezuela se encuentra en el siguiente link: http://www.lacnic.net/sp/eventos/lacnicxi/flip6.html.

6.1.3. Telecom Argentina S.A. Argentina: La prueba tiene dos objetivos.
Objetivo 1: probar IPv6 hacia Internet.
Objetivo 2: probar IPv6 en una VPN, sobre la red MPLS de Telecom.
En el objetivo 1, se está implementando un túnel sobre una de las conexiones internacionales que posee Telecom Argentina S.A. desde uno de los routers de borde de la red de Telecom. En este sentido se está trabajando con uno de los providers con los cuales Telecom tiene peering IPv4 desde hace tiempo. Con respecto al objetivo 2, se está trabajando en conjunto con uno de los clientes de Telecom y ya se implementaron túneles configurados en varios puntos de la VPN de dicho cliente. Estos túneles ya están funcionando, y ya están transportando paquetes IPv6 en la red MPLS de Telecom.

6.1.4. CENIT. Venezuela: El protocolo IPv6 fue implementado en la Red Académica Nacional de Venezuela (REACCIUN) en el año 2005. Desde entonces, existe el soporte de dual-stack y se han activado sesiones IPv6 nativas unicast y multicast con las principales universidades nacionales, así como con las redes avanzadas RedCLARA e Internet2. Paralelamente, se han establecido sesiones IPv6 nativas unicast con nuestros proveedores de acceso a Internet comercial. En REACCIUN se utiliza el protocolo de enrutamiento BGP conjuntamente con las sesiones IPv6. La Fundación CENIT promociona el despliegue de IPv6 a nivel nacional, por lo que entre sus metas para el 2010 está la adopción de dicho protocolo por el resto de los miembros de la Red Académica Nacional, así como también su divulgación entre proveedores de acceso a Internet nacionales.

6.1.5. Universidad Técnica Federico Santa María (UTFSM). Chile: La UTFSM cuenta, desde Enero del 2009, con una red IPV6 funcionando en configuración "dual-stack" con la tradicional red IPv4. La red IPv6 UTFSM cuenta con una red de prefijo /32, delegada directamente por LACNIC, la cual se comunica a Internet mediante un enlace con el ISP GlobalCrossing. En la primera etapa de

implementación se realizo una actualización del "backbone" de la red IP existente, evaluando alternativas de distintos vendedores, lo que permite en la actualidad ofrecer IPv6 en toda la Casa Central de la UTFSM. La UTFSM es una Universidad en su mayoría de carreras de Ingeniería, por lo que hay muchas unidades internas interesadas en contar con IPv6 nativo y su espacio propio de direcciones. En un futuro se planea actualizar otras secciones de la red, con el fin de poder otorgar conectividad IPv6 a todas las sedes y campus de la Universidad.

6.2. REDCLARA (COOPERACIÓN LATINO AMERICANA DE REDES AVANZADAS).

RedCLARA cuenta con IPv6 nativo implementado desde Julio/2005 sobre la troncal. El enrutamiento utiliza protocolo IS-IS en modo “single topology” para IPv4 juntamente con IPv6. La cual ofrece servicios de unicast y multicast IPv6 para las NRENs conectadas (National Research and Education Networks) de América Latina.

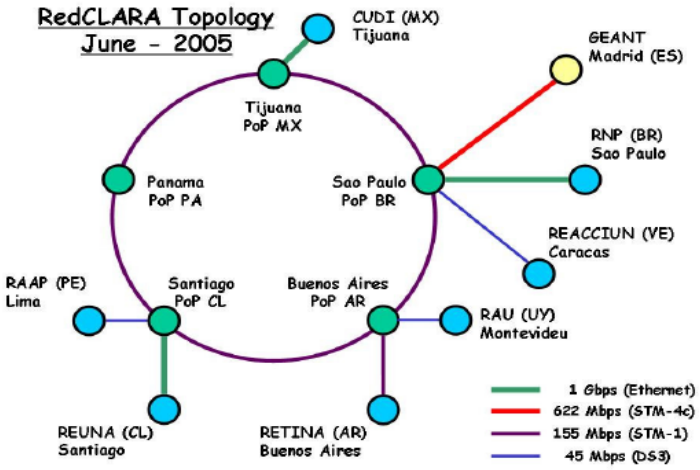
Hoy en día la troncal tiene peerings IPv6 con todas las NRENs conectadas, y también con los proveedores de tránsito académico internacional con los cuales tiene sus acuerdos (Internet2 Network, GEANT, CAnet y otros).

RedCLARA interconecta a las redes académicas avanzadas nacionales de Latinoamérica y a éstas con las redes de Europa (GÉANT2), Estados Unidos (Internet2), Asia (APAN) y el resto del mundo, otorgando a los científicos, académicose investigadores de la región, una infraestructura que les permite colaborar efectivamente con la comunidad científica global.

RedCLARA comenzó a proveer conectividad a la región el 15 de noviembre de 2004 , enlazando a las redes de investigación y educación nacionales de América Latina, mediante los Puntos de Presencia (PoPs) establecidos en Argentina, Brasil, Chile, Panamá y México, y conectándolas con GÉANT2 a 622 Mbps a través de la conexión entre São Paulo (Brasil) y Madrid (España). En 2007

RedCLARA sumó un sexto nodo (PoP) a su troncal, en Miami (Estados Unidos), al que se conectan las redes centroamericanas. Gracias al proyecto WHREN/LILA, RedCLARA se conecta también con Estados Unidos, lo que se lleva a cabo mediante los enlaces del nodo de Tijuana (México) con San Diego (Costa Pacífico de EE.UU.) y del de São Paulo con Miami.La arquitectura e ingeniería de RedCLARA, los tipos de enlaces y los procedimientos de intercambio de tráfico, están a cargo del NEG de CLARA (Grupo de Ingeniería de la Red). El centro de Operaciones de la Red (NOC) es responsable de la administración, el control, el monitoreo y la operación diaria de todas las infraestructuras físicas y lógicas que conforman la troncal de RedCLARA, asegurando altos niveles de rendimiento y de operación de la red y de sus interconexiones. RedCLARA ofrece servicios de IPv4, Multicast, IPv6, Multicast IPv6, Ancho de Banda a pedido (QoS), además de servicios especializados para proyectos, tales como Mallas Computacionales (Grids), entre otros. RedCLARA no es sólo una infraestructura ideal para el crecimiento de las redes nacionales de investigación de la zona, con una capacidad de tráfico de datos sin precedentes, lo es también para el desarrollo de colaboraciones regionales e intercontinentales. Estimulando la cooperación regional, la promoción del desarrollo científico y tecnológico, y la integración directa con las comunidades científicas del mundo, RedCLARA es fundamental para la investigación y educación en América Latina: conecta a doce países y 729 universidades (más de 671.986 académicos, 104.607 investigadores y 3.763.142 estudiantes) a través del continente, a velocidades de hasta 622Mbps.

Figura17. REDCLARA



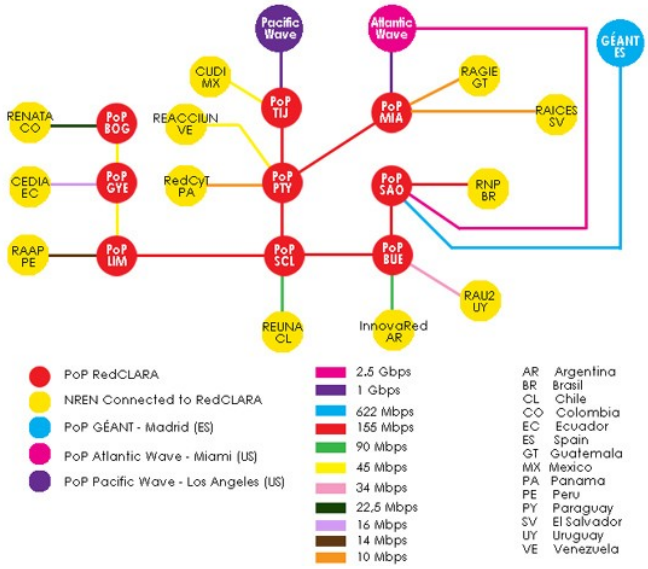
Fuente: http://www.cerider.edu.ar/images/clara_backbone.gif

Descripción técnica: CLARA es responsable de la implementación y manejo de la infraestructura de red que interconecta a las redes académicas nacionales (NREN) de América Latina. Con un gran número de universidades y centros de investigación conectados a Red CLARA, muchos proyectos que carecían de una infraestructura adecuada para sustentar los procesos de comunicación y colaboración, hoy están en posición de avanzar y lo están haciendo.

La troncal (*backbone*) de Red CLARA está compuesta por nueve nodos enrutadores principales, conectados en una topología punto-a-punto. Cada nodo principal (IP - Protocolo Internet) representa a un PoP (Punto de Presencia) para Red CLARA, ocho de ellos están ubicados en un país de América Latina -São Paulo (SAO - Brasil), Buenos Aires (BUE - Argentina), Santiago (SCL - Chile), Lima (LIM - Perú), Guayaquil (GYE - Ecuador), Bogotá (BOG - Colombia), Panamá (PTY - Panamá) y Tijuana (TIJ - México)- y el noveno, en Miami (MIA - Estados Unidos). Todas las conexiones de las redes nacionales latinoamericanas (NREN) a Red CLARA son a través de uno de estos nueve nodos. La troncal de RedCLARA está interconectada con la red paneuropea GÉANT2 a través del

enlace del PoP de CLARA en SAO con el punto de acceso de GÉANT2 en Madrid (España - ES), posibilitado por el Proyecto ALICE (finalizado en marzo de 2008), y, con Estados Unidos, mediante los enlaces establecidos en los PoP de CLARA en SAO y TIJ, el primero con el PoP de *AtlanticWave* y el segundo con el PoP de *PacificWave*, estos dos últimos accesos son posibilitados por WHREN-LILA. Cuando una NREN latinoamericana hace conexión con RedCLARA, lo hace a través de uno de los nueve nodos de la troncal de RedCLARA; esta conexión le brinda a estas NREN y a sus miembros (clientes), acceso a RedCLARA, otorgándoles un Punto de Intercambio.

Figura18. Troncal REDCLARA



Fuente: http://www.redclara.net/imag/var/clara_backbone_aug2007.gif

6.2.1. Ingeniería de Tráfico de Red CLARA:

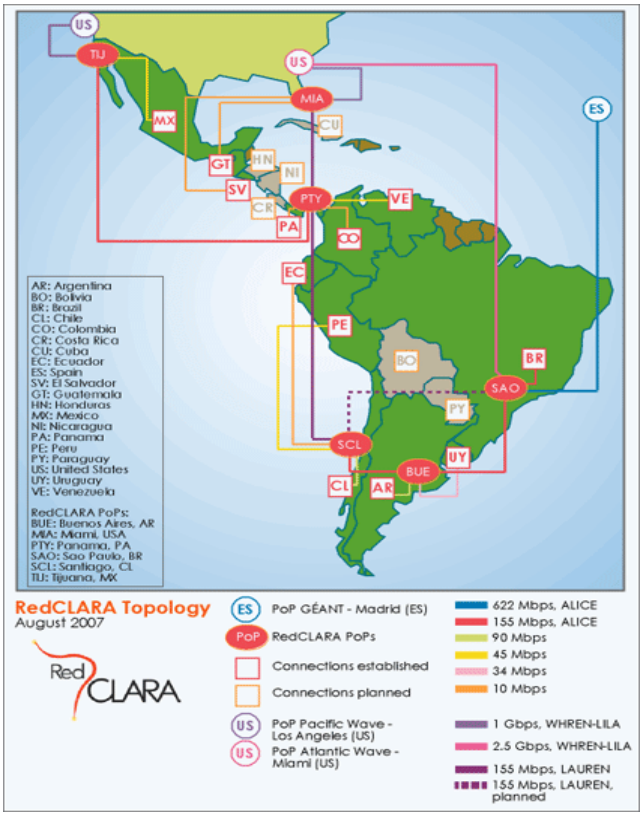
- Uso de Ingeniería de Tráfico MPLS en la troncal.
- Las aplicaciones sensitivas al retardo podrían "indicar" a la red su

requerimiento por una vía diferente.

- Los túneles definidos manualmente deberían prevalecer por sobre la decisión normal de proceso de enrutamiento IGP.

A la fecha se encuentran conectadas a RedCLARA las redes nacionales de investigación y educación (NREN) de:

Figura19. Conexión RedCLARA

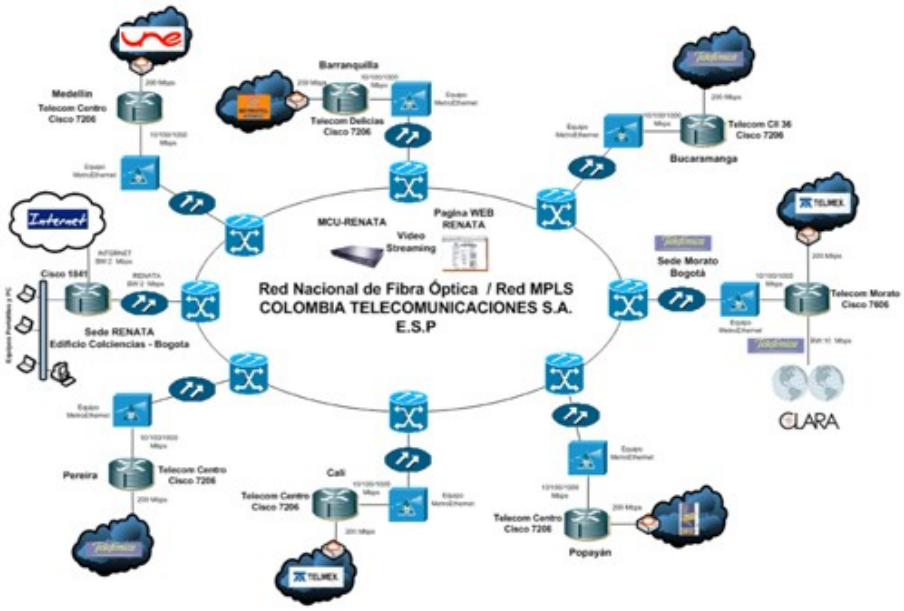


Fuente: http://www.redclara.net/imag/var/topology_RedCLARA_Aug2007.gif

6.3. RENATA, Red Nacional Académica de Tecnología Avanzada. COLOMBIA.

Es la red de tecnología avanzada que conecta, comunica y propicia la colaboración entre la comunidad académica y científica de Colombia con la comunidad académica internacional y los centros de investigación más desarrollados del mundo. Es administrada por la Corporación RENATA, de la cual son miembros las Redes Académicas Regionales, el Ministerio de Educación, el Ministerio de Tecnologías de la Información y las Comunicaciones y Colciencias.
Al momento de configurar los enlaces cada Router utiliza una interface Loopback la cual es publicada por OSPFv3. Cada una de estas interfaces tiene una IPv6 y es utilizada como PEER MBGP, es decir, a través de ésta se establecen las sesiones MBPG. Asimismo es utilizada una Ipv4 como Router ID de cada proceso Dinámico OSPFv3 o MBGP.

Figura 20. RENATA, Red Nacional Académica de Tecnología Avanzada.



Fuente: http://www.renata.edu.co/images/stories/renata/inf_renata.jpg

Las conexiones IPv6 son establecidas entre los concentradores de la red RENATA (Cisco 7206 y 7606) utilizando la red mallada MPLS a través de VLL's configuradas en los PE's Alcatel 7750. De esta manera el router principal de la red RENATA y Gateway contra Internet2 establece una sesión MBGP contra cada uno de los routers concentradores de la red RENATA y realiza el papel de Route-Reflector constituyendo una red Full-mesh IPv6. Este equipo está encargado de agregar todos los sub-prefijos IPv6 asignados a RENATA publicando la sumarización de la red 2001:13f8::0/32

El direccionamiento utilizado en el CORE RENATA para establecimiento de las sesiones MBGP es el siguiente:

Tabla17. Direccionamiento CORE RENATA

Cali RUAV	2001:13F8::1/64
Barranquilla RUMBA	2001:13F8::2/64
Bucaramanga UNIRED	2001:13F8::3/64
Medellín RUANA	2001:13F8::4/64
Pereira RADAR	2001:13F8::5/64
Bogotá D.C. RUMBO	2001:13F8::6/64
Bogotá D.C. COLCIENCIAS	2001:13F8::7/64
Popayán RUP	2001:13F8::8/64

Fuente: http://www.renata.edu.co/index.php/redes-academicas-regionales.html

La asignación IPV6 para RENATA es **2001:13F8::/32**

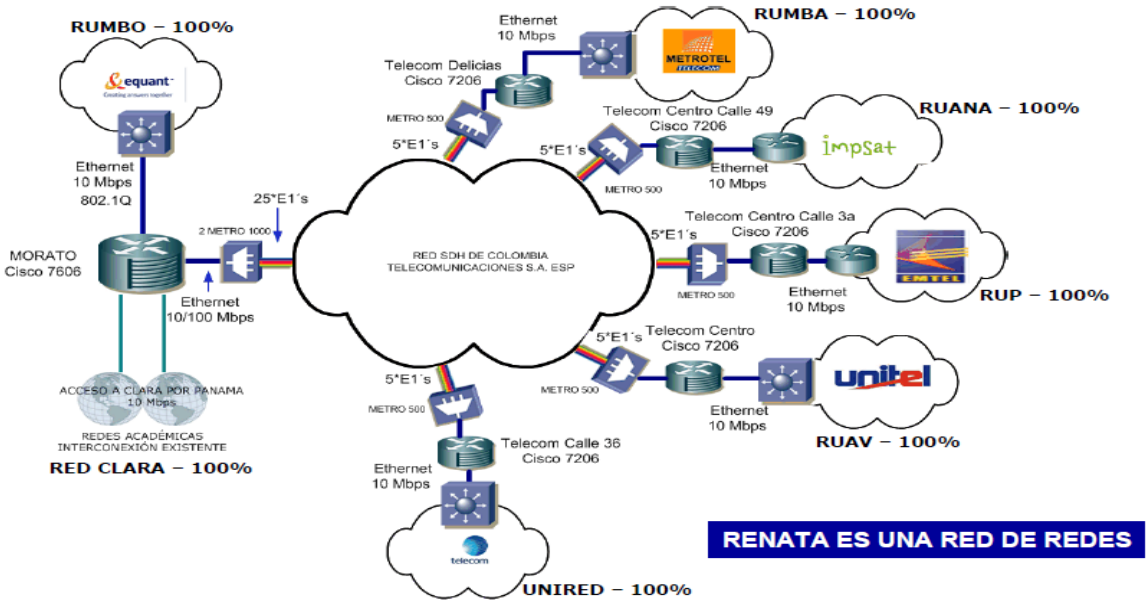
La implementación de asignación de los **bloques ::/36**, comenzará a partir del primer **bloque ::/40** asegurando asignar la totalidad del mismo y de forma

continua, antes de aprovechar/utilizar el siguiente **bloque ::/40** disponible. Por tanto, todos los **bloques ::/40** no asignados se utilizarán como reserva.

6.3.1 Topología RENATA

- Prefijo asignado por LACNIC: 32 bits; espacio para distribuir 96 bits
- Estructura y formato denominado IPV6/ Global Unicast Address, mostrado abajo.
- LACNIC 32 bits entregados. Un relleno de 16 bits para conformar los 48 bits de más alto orden del Prefijo de enrutamiento global.
- Asignación a las RARES de su espacio: Los siguientes 16 bits correspondientes a la subred en el formato IPV6/ Global Unicast Address LA RARE debe distribuir así:
- Id. Universidad: 16 bits
- Id. Dependencia en la universidad: 16 bits
- Dirección del interfaz
- Las 2 anteriores se concatenan si se usa la MAC de la tarjeta como últimos 48 bits de la dirección IP
- La asignación de direcciones IPv6 a las universidades tienen 2 connotaciones necesarias de tener en cuenta: Si la universidad va a usar un enrutador y un enlace independiente de su enlace Internet, a la universidad se le debe asignar en forma individual un espacio de direcciones IPV6. Si la universidad usa el mismo enrutador y un mismo enlace para ambas tareas (Internet y RENATA) es necesaria la tarea de encapsular (por el tunneling) las direcciones IPV4 tradicionales de la universidad en los paquetes IPV6 que maneje la RARE.
- Se dejaron los primeros 16 bits dentro de la RARE para identificar la universidad o institución, los siguientes 16 para identificar dependencias dentro de la universidad. Deben permanecer en “0” durante la migración.

Figura 21. Topología Renata



Fuente: http://www.renata.edu.co/index.php/infraestructura.html

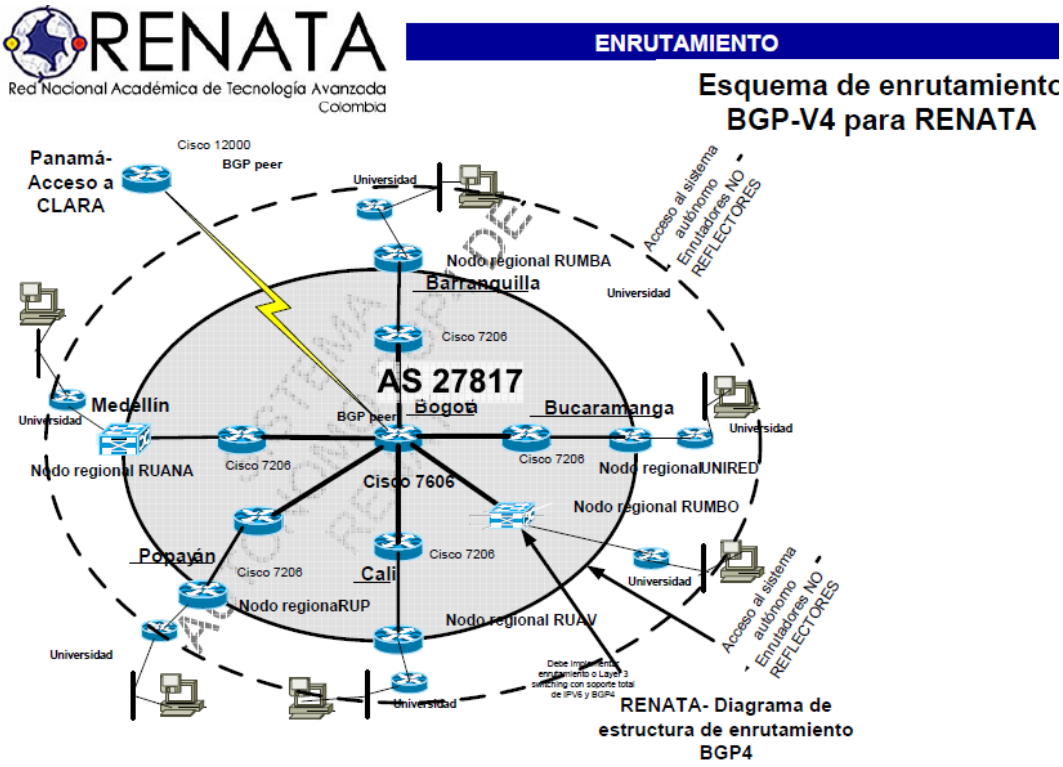
6.3.2. Normatividad y Características de la red claves para su enrutamiento:

BGP-4 como protocolo de enrutamiento, utiliza el AS-PATH para incluir conjuntos de sistemas autónomos así como listas. Este formato extendido permite generar rutas adicionales para acarrear información de más rutas, para este caso las redes bajo ipv6 en Colombia, heredan los beneficios de este protocolo; por tanto el proveedor de servicio de la RARE debe:

- Implantar el protocolo BGP4 en el enrutador de su propiedad que accede al enrutador de borde de COLOMBIA TELECOMUNICACIONES.
- Implantar un procedimiento de actualización y manejo para las peticiones de registro manual de actualizaciones y cambios
- Soportar el enrutamiento interno BGP4 dentro del sistema autónomo de RENATA

- No mezclar ni interferir el tráfico de enrutamiento y el enrutamiento BGP4 que usa para INTERNET con el de RENATA. Se recomienda en lo posible que este proveedor asigne un enrutador dedicado a manejar la salida hacia RENATA
- En lo posible el proveedor de la RARE debe separar en su anillo de switches mediante VLAN u otro mecanismo el tráfico de RENATA del tráfico de Internet.
- RENATA será una red con un solo número de sistema autónomo asignado por CLARA.
- RENATA debe usar BGP-4 como su protocolo de enrutamiento INTERNO (IBGP).
- El punto de entrada para BGP4 de RENATA que ejerce como NODO central de cada RARE es el enrutador del proveedor del servicio.
- Debido a lo anterior cualquier ruta interna al sistema autónomo de RENATA, para la conectividad entre RARES no debe tener mas de 2 enrutadores en su trayectoria, uno por cada RARE.
- En enrutamiento BGP-4 de las RARES para RENATA es completamente independiente y separado del enrutamiento que cada proveedor de las RARE haga para su gestión de enrutamiento a Internet. Así sea este último también BGP4.
- Algunas universidades e instituciones que tengan enrutador dedicado a RENATA podrán estar en el sistema autónomo de RENATA.
- El AS number usado por la RARE y que es el de RENATA no puede ser incluido en la lista de enrutamiento particular de INTERNET.
- Es altamente recomendable que para la conexión de acceso a RENATA, la RARE utilice un enrutador separado física o virtualmente.

Figura 22. Esquema de enrutamiento BGP-V4 RENATA



Fuente: http://oitel.univalle.edu.co/cit/actas/2007/AnexoActa23-Renata.pdf

6.3.3. Casos especiales:

- Universidad Nacional y Universidad de los Andes en Bogotá poseen sistemas autónomos propios.
- Esos miembros se conectarán a RENATA como sistemas autónomos independiente.
- Su interrelación con RENATA es como cualquier otro sistema autónomo es decir RENATA tendrá su propio sistema autónomo mas los de las universidades Nacional y Los Andes.

BGP4 EN RUANA

- No existe un enrutador central de la RARE.
- Cada Universidad enrutará en BGP4 interno, al enrutador periférico de Colombia Telecomunicaciones en Medellín.
- El enrutador de la universidad actuará en modo NO REFLECTOR.
- El enrutador periférico de Colombia Telecomunicaciones en Medellín trabajará en BGP4 interno REFLECTOR.
- Si el proveedor de RUMBO sirve Internet a la universidad en el mismo enrutador de acceso a RENATA, manejará un protocolo interno diferente a BGP4 o al menos garantizara números autónomos diferentes a RENATA si llegare a usar BGP4.

BGP4 EN RUMBO

- No existe un enrutador central de la RARE
- Cada Universidad enrutará en BGP4 interno, al enrutador central de Colombia Telecomunicaciones
- El enrutador de la universidad actuará en modo NO REFLECTOR
- Si el proveedor de RUMBO sirve Internet a la universidad en el mismo enrutador de acceso a RENATA, manejará un protocolo interno diferente a BGP4 o al menos garantizara números autónomos diferentes a RENATA.

BGP4 EN RUAV, RUMBA, RUP y UNIRED

- El proveedor de servicios de la RARE provee un enrutador central
- El enrutador central de la RARE actuará en modo NO REFLECTOR.
- Cada Universidad enrutará en un protocolo interno diferente a BGP4 interno, al enrutador central de la RARE
- El enrutador periférico de Colombia Telecomunicaciones en la RARE trabajará en BGP4 interno REFLECTOR

- Si el proveedor de la RARE sirve Internet a la universidad en el mismo enrutador de acceso a RENATA, manejará un protocolo interno diferente a BGP4 o al menos garantizara números autónomos diferentes a RENATA si usa BGP4.

A continuación se presenta la distribución del direccionamiento IP por Regiones. Nombre de la red con sus respectivas direcciones.

Tabla 18. Direccionamiento RENATA

Red	**Direcciones equipos centrales de transmisión**
RENATA 2001:13F8:0000::/36	2001:13F8:0000::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0100::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0200::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0300::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0400::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0500::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0600::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0700::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0800::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0900::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0A00::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0B00::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0C00::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0D00::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0E00::/40
RENATA 2001:13F8:0000::/36	2001:13F8:0F00::/40

Fuente: http://www.renata.edu.co/index.php/redes-academicas-regionales.html

RUMBO, Red Universitaria Metropolitana de Bogotá. Nombre de la red con sus respectivas direcciones

Tabla 19. Direccionamiento RENATA para la Red Universitaria Metropolitana de Bogotá.

Red	**Direcciones equipos centrales de transmisión**
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1000::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1100::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1200::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1300::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1400::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1500::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1600::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1700::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1800::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1900::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1A00::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1B00::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1C00::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1D00::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1E00::/40
BOGOTÁ 2001:13F8:1000::/36	2001:13F8:1F00::/40

Fuente: http://www.renata.edu.co/index.php/redes-academicas-regionales.html

RADAR, Red Académica de Alta Velocidad Regional. Nombre de la red con sus respectivas direcciones

Tabla 20. Direccionamiento RENATA para RADAR

Red	**Direcciones equipos centrales de transmisión**
PEREIRA 2001:13F8:1000::/36	2001:13F8:2000::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2100::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2200::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2300::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2400::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2500::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2600::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2700::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2800::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2900::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2A00::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2B00::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2C00::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2D00::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2E00::/40
PEREIRA 2001:13F8:1000::/36	2001:13F8:2F00::/40

Fuente: http://www.renata.edu.co/index.php/redes-academicas-regionales.html

RUAV, Asociación Red Universitaria de Alta Velocidad del Valle del Cauca

Nombre de la red con sus respectivas direcciones

Tabla 21. Direccionamiento RENATA para RUAV

Red	**Direcciones equipos centrales de transmisión**
CALI 2001:13F8:3000::/36	2001:13F8:3000::/40
CALI 2001:13F8:3000::/36	2001:13F8:3100::/40
CALI 2001:13F8:3000::/36	2001:13F8:3200::/40
CALI 2001:13F8:3000::/36	2001:13F8:3300::/40
CALI 2001:13F8:3000::/36	2001:13F8:3400::/40
CALI 2001:13F8:3000::/36	2001:13F8:3500::/40
CALI 2001:13F8:3000::/36	2001:13F8:3600::/40
CALI 2001:13F8:3000::/36	2001:13F8:3700::/40
CALI 2001:13F8:3000::/36	2001:13F8:3800::/40
CALI 2001:13F8:3000::/36	2001:13F8:3900::/40
CALI 2001:13F8:3000::/36	2001:13F8:3A00::/40
CALI 2001:13F8:3000::/36	2001:13F8:3B00::/40
CALI 2001:13F8:3000::/36	2001:13F8:3C00::/40
CALI 2001:13F8:3000::/36	2001:13F8:3D00::/40
CALI 2001:13F8:3000::/36	2001:13F8:3E00::/40
CALI 2001:13F8:3000::/36	2001:13F8:3F00::/40

Fuente: http://www.renata.edu.co/index.php/redes-academicas-regionales.html

RUP, Asociación Red Universitaria de Popayán. Nombre de la red con sus respectivas direcciones.

Tabla 22. Direccionamiento RENATA para RUP

Red	**Direcciones equipos centrales de transmisión**
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4000::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4100::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4200::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4300::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4400::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4500::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4600::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4700::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4800::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4900::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4A00::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4B00::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4C00::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4D00::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4E00::/40
POPAYÁN 2001:13F8:4000::/36	2001:13F8:4F00::/40

Fuente: http://www.renata.edu.co/index.php/redes-academicas-regionales.html

UNIRED, Corporación Red de Instituciones de Educación, Investigación y Desarrollo del Oriente Colombiano. Nombre de la red con sus respectivas direcciones

Tabla 23. Direccionamiento RENATA para UNIRED

Red	**Direcciones equipos centrales de transmisión**
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5000::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5100::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5200::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5300::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5400::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5300::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5400::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5500::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5600::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5700::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5800::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5900::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5A00::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5B00::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5C00::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5D00::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5E00::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5F00::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5000::/40
BUCARAMANGA 2001:13F8:5000::/36	2001:13F8:5100::/40

RUTA, Red Universitaria de Tecnología Avanzada del Caribe. Nombre de la red con sus respectivas direcciones

Tabla 24. Direccionamiento RENATA para RUTA

Red	**Direcciones equipos centrales de transmisión**
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6000::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6100::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6200::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6300::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6400::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6500::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6600::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6700::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6800::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6900::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6A00::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6B00::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6C00::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6D00::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6E00::/40
BARRANQUILLLA 2001:13F8:6000::/36	2001:13F8:6F00::/40

Fuente: http://www.renata.edu.co/index.php/redes-academicas-regionales.html

RUANA, Red Universitaria Antioqueña. Nombre de la red con sus respectivas direcciones

Tabla 25. Direccionamiento RENATA para RUANA

Red	**Direcciones equipos centrales de transmisión**
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7000::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7100::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7200::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7300::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7400::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7500::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7600::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7700::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7600::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7700::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7800::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7900::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7A00::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7B00::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7C00::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7D00::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7E00::/40
MEDELLÍN 2001:13F8:7000::/36	2001:13F8:7F00::/40

Fuente: http://www.renata.edu.co/index.php/redes-academicas-regionales.html

Direcciones de Reserva. Nombre de la direcciones de reserva en diferentes ciudades del país

Tabla 26. Direccionamiento RENATA para direcciones de Reservas

Ciudad	**Red de la ciudad**	**Direcciones IP de la ciudad**
Manizales	2001:13F8:8000::/39	2001:13F8:8000::/40
Manizales (Reserva)	2001:13F8:8200::/39	2001:13F8:8200::/40 2001:13F8:8300::/40
Pereira	2001:13F8:8400::/39	2001:13F8:8400::/40 2001:13F8:8500::/40
Pereira (Reserva)	2001:13F8:8600::/39	2001:13F8:8600::/40 2001:13F8:8700::/40
Armenia	2001:13F8:8800::/39	2001:13F8:8800::/40 2001:13F8:8900::/40
Armenia (Reserva)	2001:13F8:8A00::/39	2001:13F8:8A00::/40 2001:13F8:8B00::/40
Ibagué	2001:13F8:8C00::/39	2001:13F8:8C00::/40 2001:13F8:8D00::/40
Ibagué (Reserva)	2001:13F8:8E00::/39	2001:13F8:8E00::/40 2001:13F8:8F00::/40
Cartagena	2001:13F8:9000::/39/td>	2001:13F8:9000::/40 2001:13F8:9100::/40
Cartagena (Reserva)	2001:13F8:9200::/39	2001:13F8:9200::/40 2001:13F8:9300::/40
Santa Marta	2001:13F8:9400::/39	2001:13F8:9400::/40 2001:13F8:9500::/40
Manizales	2001:13F8:8000::/39	2001:13F8:8000::/40

		2001:13F8:8100::/40
Santa Marta (Reserva)	2001:13F8:9600::/39	2001:13F8:9600::/40 2001:13F8:9700::/40
Pasto	2001:13F8:9800::/39	2001:13F8:9800::/40 2001:13F8:9900::/40
Pasto (Reserva)	2001:13F8:9A00::/39	2001:13F8:9A00::/40 2001:13F8:9B00::/40
Neiva	2001:13F8:9C00::/39	2001:13F8:9C00::/40 2001:13F8:9D00::/40
Neiva (Reserva)	2001:13F8:9E00::/39	2001:13F8:9E00::/40 2001:13F8:9F00::/40
Cúcuta	2001:13F8:A000::/39	2001:13F8:A000::/40 2001:13F8:A100::/40
Cúcuta (Reserva)	2001:13F8:A200::/39	2001:13F8:A200::/40 2001:13F8:A300::/40
Tunja	2001:13F8:A400::/39	2001:13F8:A400::/40 2001:13F8:A500::/40
Tunja (Reserva)	2001:13F8:A600::/39	2001:13F8:A600::/40 2001:13F8:A700::/40
Montería	2001:13F8:A800::/39	2001:13F8:A800::/40 2001:13F8:A900::/40
Montería (Reserva)	2001:13F8:AA00::/39	2001:13F8:AA00::/40 2001:13F8:AB00::/40
Riohacha	2001:13F8:AC00::/39	2001:13F8:AD00::/40
Riohacha (Reserva)	2001:13F8:AE00::/39	2001:13F8:AE00::/40 2001:13F8:AF00::/40
Valledupar	2001:13F8:B000::/39	2001:13F8:B000::/40 2001:13F8:B100::/40

Valledupar (Reserva)	2001:13F8:B200::/39	2001:13F8:B200::/40 2001:13F8:B300::/40
Sincelejo	2001:13F8:B400::/39	2001:13F8:B500::/40
Sincelejo (Reserva)	2001:13F8:B600::/39	2001:13F8:B600::/40 2001:13F8:B700::/40
Villavicencio	2001:13F8:B800::/39	2001:13F8:B800::/40 2001:13F8:B900::/40
Villavicencio (Reserva)	2001:13F8:BA00::/39	2001:13F8:BA00::/40 2001:13F8:BB00::/40
Quibdó	2001:13F8:BC00::/39	2001:13F8:BC00::/40 2001:13F8:BD00::/40
Quibdó (Reserva)	2001:13F8:BE00::/39	2001:13F8:BE00::/40 2001:13F8:BF00::/40
San Andrés	2001:13F8:C000::/39	2001:13F8:C000::/40 2001:13F8:C100::/40
San Andrés (Reserva)	2001:13F8:C200::/39	2001:13F8:C200::/40 2001:13F8:C300::/40
Mocoa	2001:13F8:C400::/39	2001:13F8:C400::/40 2001:13F8:C500::/40
San José del Guaviare	2001:13F8:C800::/39	2001:13F8:C800::/40 2001:13F8:C900::/40
San José del Guaviare (Reserva)	2001:13F8:CA00::/39	2001:13F8:CA00::/40 2001:13F8:CB00::/40
Arauca	2001:13F8:CC00::/39	2001:13F8:CC00::/40 2001:13F8:CD00::/40
Arauca (Reserva)	2001:13F8:CE00::/39	2001:13F8:CE00::/40 2001:13F8:CF00::/40
Florencia	2001:13F8:D000::/39	2001:13F8:D000::/40

		2001:13F8:D100::/40
Florencia (Reserva)	2001:13F8:D200::/39	2001:13F8:D200::/40 2001:13F8:D300::/40
Leticia	2001:13F8:D400::/39	2001:13F8:D400::/40 2001:13F8:D500::/40
Leticia (Reserva)	2001:13F8:D600::/39	2001:13F8:D600::/40 2001:13F8:D700::/40
Yopal	2001:13F8:D800::/39	2001:13F8:D800::/40 2001:13F8:D900::/40
Yopal (Reserva)	2001:13F8:DA00::/39	2001:13F8:DA00::/40 2001:13F8:DB00::/40
Puerto Inírida	2001:13F8:DC00::/39	2001:13F8:DC00::/40 2001:13F8:DD00::/40
Puerto Inírida (Reserva)	2001:13F8:DE00::/3	2001:13F8:DE00::/40 2001:13F8:DF00::/40
Mitú	2001:13F8:E000::/39	2001:13F8:E000::/40 2001:13F8:E100::/40
Mitú (Reserva)	2001:13F8:E200::/39	2001:13F8:E200::/40 2001:13F8:E300::/40
Puerto Carreño	2001:13F8:E400::/39	2001:13F8:E400::/40 2001:13F8:E500::/40
Puerto Carreño (Reserva	2001:13F8:E600::/39	2001:13F8:E600::/40 2001:13F8:E700::/40

Fuente: http://www.renata.edu.co/index.php/redes-academicas-regionales.html

Reserva Adicionales

2001:13F8:E800::/39
2001:13F8:EA00::/39
2001:13F8:EC00::/39
2001:13F8:EE00::/39
2001:13F8:F000::/39
2001:13F8:F200::/39
2001:13F8:F400::/39
2001:13F8:F600::/39
2001:13F8:F800::/39
2001:13F8:FA00::/39
2001:13F8:FC00::/39
2001:13F8:FE00::/39

CONCLUSIONES

- Muchos Proveedores de Servicios (ISPs) ya cuentan con sus troncales preparadas para la demanda de clientes que quieran desplegar el nuevo protocolo. Hablamos de ISPs a nivel nacional y regional que poseen esta particularidad, incluso ofreciendo tecnologías más avanzadas, como MPLS, con soporte para IPv6 redes experimentales y proyectos de investigación: 6BONE, LONG, ARMSTRONG, etc.

- Es necesario que los distintos organismos de gobierno y entidades públicas o redes de universidades, a la hora de lanzar licitaciones para la compra de equipamientos o servicios, exijan en ellos el soporte del nuevo protocolo, preparándose de esa manera para una transición que se considera inevitable.

- La compatibilidad de IPV4 e IPv6 es posible gracias a las diferentes herramientas de transición: nodos duales, túneles y traductores de protocolo.

- IPV4, presenta demasiadas limitantes, como son escases de direcciones, servicios, dispositivos, aplicaciones e innovaciones en internet.

- IPv6 seguirá las buenas prácticas de IPv4 y eliminará las características no utilizadas u obsoletas de IPv4, con lo que se conseguirá una optimización del protocolo de Internet. La idea es quedarse con lo bueno y eliminar lo malo del protocolo actual.

- En todo momento, las entidades asociadas para el estudio de IPV6 siguen descubriendo mecanismos como el túnel para mejorar las transmisiones y facilitar la migración del protocolo IPV4 a IPV6.

- La acogida de esta tecnología ha favorecido grandemente a Latinoamérica, ya que gracias a IPV6, Colombia hace parte de una gran red de avanzada la cual trae grandes beneficios Académicos e intelectuales. Actualmente también se está aplicando esta tecnología en la telefonía IP y la Celular.

BIBLIOGRAFIA

Blanchet, Marc. Migrating to IPv6: A practical Guide to Implemeting IPv6 in Mobile and Fixed Networks. Enero 3, 2006.

Feyrer, Hubert. Introduction to IPv6. Mayo 2001. O'Reilly.

Grosse, Erick. Lakshman. Network Processors Applied to IPv4/IPv6 Transition. Laboratorios Bell. Nueva Jersey, Estados Unidos. Agosto 2003.

Huston, Geoff. Waiting for IP version 6. The ISP Column., Enero 2003 .

Kotal, Vladimír. PhD Thesis. Principles, implementation and transistion to IPv6 protocol. Universidad de Karlova, Praga.Abril 19 de 2005.

Ramírez, Sergio, María Cervantes. Introducción al IPv6. Universidad de la República. Uruguay. Noviembre de 2005.

Verdejo Álvarez, Gabriel. El protocolo IPv6 y sus extensiones de seguridad IPsec. Bellaterra, España. Febrero de 2000.

Waddingtin, Daniel G, Fangzhe Chang. Realizing the Transition to IPv6. IEEE Communications Magazine. Vol. 6, issue 3., pp.38-48., Junio 2002.

Wu, Eric, Johny Lai, et al. An accurate Simulation Model for Mobile Ipv6 Protocol. 2006.

Referencias Electrónicas

http://www.ipv6forum.com

http://www.co.ipv6tf.org/

http://www.renata.edu.co/index.php/ipv6.html?start=3

http://www.ipv6.unam.mx/documentos/IPv6_Redes-Academicas-Eriko-Azael.pdf

http://www.redclara.net/

http://www.nsrc.org/STHAM/CO/RENATA_CLARA_TEC_2006-COLOMBIA.pdf

http://www.gobiernoenlinea.net/1804.html

www.6bone.net

www.cudi.edu.mx

www.ipv6.unam.mx/Internet2/

www.ipv6.retina.ar / www.ipv6.cl

www.rnp.br/en/ipv6 / www.rau.edu.uy/ipv6

www.redclara.net/03/06_05.htm

www.lacnic.net

www.sixxs.net

http://portalipv6.lacnic.net/node/420

ANEXOS

COLOMBIA

COMPUTERWORLD Colombia
La publicación de informática y tecnología

Fecha de Publicación: 9/3/2009

Título Noticia: Realizada reunión sobre el protocolo IPv6

Detalle de la Noticia:

Actualidad

Realizada reunión sobre el protocolo IPv6

Se invita a la comunidad y a las empresas desarrolladoras de contenidos y aplicaciones de software a usar el protocolo IPv6, con el objetivo de obtener un máximo provecho en aplicaciones para la movilidad, el mejoramiento en los niveles de seguridad y facilitar las aplicaciones móviles.

Esta es una de las conclusiones del seminario "Instauración del protocolo IPv6 en Colombia", realizado por el Ministerio de Tecnologías de la Información y las Comunicaciones (TIC) y el SENA, que contó con la participación de cerca de 300 asistentes y más de 140 personas que recibieron la información a través de video conferencias coordinadas por el SENA en distintas ciudades del país.

"La generación de demanda por servicios IPv6 muy seguramente tendrá la respuesta correspondiente en los operadores, ISP, quienes tendrán que incluir en sus agendas estratégicas la adopción del protocolo IPv6; por lo tanto, es un llamado a los desarrolladores de aplicaciones y a la industria del software nacional para aprovechar este protocolo con el propósito de generar productos innovadores", señaló la ministra Maria del Rosario Guerra.

El protocolo IPv6 es una nueva versión de IP (Internet Protocol), diseñada para reemplazar a la versión 4 (IPv4), actualmente en uso.

Diseñado por Steve Deering de Xerox PARC y Craig Mudge, IPv6 está destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India y otros países asiáticos densamente poblados. Pero el nuevo estándar mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles con sus direcciones propias y

permanentes. Se calcula que las dos terceras partes de las direcciones que ofrece IPv4 ya están asignadas.

Propuesto por el Internet Engineering Task Force en 1994 (cuando era llamado "IP Next Generation" o IPng), la adopción de IPv6 por parte de Internet es menor, la red todavía está dominada por IPv4.

La necesidad de adoptar el nuevo protocolo debido a la falta de direcciones ha sido parcialmente aliviada por el uso de la técnica NAT. Pero NAT rompe con la idea originaria de Internet donde todos pueden conectarse con todos y hace difícil o imposible el uso de algunas aplicaciones P2P, de voz sobre IP y de juegos multiusuario. Un posible factor que influya a favor de la adopción del nuevo protocolo podría ser la capacidad de ofrecer nuevos servicios, tales como la movilidad, Calidad de Servicio (QoS), privacidad, etc.

Otra vía para la popularización del protocolo es la adopción de este por parte de instituciones. El gobierno de los Estados Unidos ordenó el despliegue de IPv6 por todas sus agencias federales para el año 2008.

IPv6 es la segunda versión del Protocolo de Internet que se ha adoptado para uso general. También hubo un IPv5, pero no fue un sucesor de IPv4; mejor dicho, fue un protocolo experimental orientado al flujo de streaming que intentaba soportar voz, video y audio.

En Colombia uno de los primeros seminarios sobre el tema lo lideró la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) en conjunto con el Ministerio y se han hecho avances en conocer experiencias de otros países, pero aún falta el impulso de todo el ecosistema.