Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación
Laboratorio de Comunicación y Redes

Propuesta para la Implementación de un Servicio de Hilos Musicales utilizando IPv6 Multicast

Trabajo Especial de Grado
presentado ante la ilustre
Universidad Central de Venezuela
por el Bachiller
Antonio Gustavo Sánchez Nuñez
para optar al título de
Licenciado en Computación

Prof. Eric Gamess

Caracas, Julio / 2010

Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación

ACTA DEL VEREDICTO

Quienes suscriben, Miembros del Jurado designados por el Consejo de Escuela de Computación, para examinar el Trabajo Especial de Grado, presentado por el Bachiller Antonio Gustavo Sanchez Nuñez, C.I. 14.727.937, con el título "**Propuesta para la Implementación de un Servicio de Hilos Musicales utilizando IPv6 Multicast**", a los fines de cumplir con el requisito legal para optar al título de Licenciado en Computación, dejan constancia de lo siguiente:

Leído como fue dicho trabajo por cada uno de los Miembros del Jurado, éstos fijaron el día 8 de Julio de 2010, para que su autor lo defendiera en forma pública, lo cual éste realizó, mediante una exposición oral de su contenido, y luego respondió satisfactoriamente a las preguntas que le fueron formuladas por el Jurado, todo ello conforme a lo dispuesto en la Ley de Universidades y demás normativas vigentes de la Universidad Central de Venezuela.

Finalizada la defensa pública del Trabajo Especial de Grado, el jurado decidió APROBARLO.

Firmas del Tutor y Jurados Examinadores:

Prof. Eric Gamess
(Tutor)

Prof. Maria Elena Villapol
(Jurado Principal)

Prof. Robinson Rivas
(Jurado Principal)

Dedicatoria

A mis padres, como una pequeña recompensa por los años invertidos en mi formación, porque se los debía, porque se lo merecen, eso y mucho más, gracias a ustedes estoy aquí.

A mi familia, porque son grandiosos; una mención especial al Tío Hebert, sé que también estarás muy feliz y orgulloso donde quiera que te encuentres.

Agradecimientos

En primer lugar a Dios, por darme vida y salud para poder culminar este trabajo.

A mis padres, Antonio y Ana Núñez de Sánchez, por su apoyo, paciencia, amor y comprensión.

A mi familia, por nunca perder las esperanzas en mí, por estar siempre unidos en las buenas y en las malas.

A mi novia, Liliana Dumont, por su perseverancia durante todo este tiempo, por ayudarme a culminar este ciclo, sin ti no hubiera podido.

A mi tutor Prof. Eric Games, por acompañarme durante la finalización de este ciclo de estudiante, por sus conocimientos y apoyo.

Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación

TRABAJO ESPACIAL DE GRADO

Título: Propuesta para la Implementación de un Servicio de Hilos Musicales utilizando IPv6 Multicast.

Autor: Antonio G. Sánchez N.

Unidad de Investigación: LACORE.

Palabras Claves: IPv6, Multicast, Hilos Musicales, Servidor de Streaming.

Tutor: Prof. Eric Gamess.

Fecha de Presentación: Julio 2010.

Resumen

El objetivo del presente Trabajo Especial de Grado consiste en investigar los requerimientos necesarios para habilitar un Servicio de Hilos Musicales sobre IPv6 Multicast para la Universidad Central de Venezuela. Esta investigación se basa en el estudio de la tecnología Multicast, la infraestructura y configuración necesaria para este tipo de servicios en un entorno IPv6.

El trabajo empieza con un proceso de investigación de la tecnología Multicast, que contempla su origen, evolución e interacción con los nuevos estándares de comunicación IP. Posteriormente, en base a dicha investigación, se propone una infraestructura de red que abarca protocolos, estándares, tecnologías y equipos necesarios para implementar un servicio de Hilos Musicales sobre IPv6 Multicast.

El protocolo de enrutamiento multicast ha utilizar es PIM-SM, debido a que es uno de los protocolos más utilizados en este tipo de ambientes, definido formalmente en un RFC y adoptado por las principales compañías fabricantes de dispositivos de red.

Por otra parte, para el servicio de difusión de los hilos musicales, y tras una investigación de las aplicaciones disponibles, se utilizó Microsoft Windows Media Service 9 como servidor de streaming debido a un conjunto de características importantes, tales como soporte de formatos de audio ampliamente desplegados en Internet, fácil instalación y administración, soporte IPv6 y Multicast, entre otros.

Finalmente, este trabajo provee, además de una propuesta para un Servicio de Hilos Musicales para la UCV, una implementación del servicio para la Facultad de Ciencias.

Tabla de Contenido

Índice de Figuras

Índice de Tablas

1. Introducción

Las aplicaciones multimedia se han desplegado rápidamente en ambientes de redes LANs y WANs en los últimos años. Para ambientes LANs, las aplicaciones de red multimedia, tal como la videoconferencia, se perciben como la próxima generación de herramientas de productividad. De igual forma, el uso de audio y video digital a través de la infraestructura de red corporativa tiene un gran potencial para aplicaciones internas y externas.

Más del 85% de las computadoras personales son vendidas con capacidades multimedia. Esta revolución en el hardware ha iniciado una revolución en el software que trajo un amplio rango de aplicaciones basadas en audio y video para el usuario final. Con estos tipos de aplicaciones, los flujos de audio y video son transferidos sobre la red entre pares iguales o entre clientes y servidores.

Muchas de estas aplicaciones se fundamentan en la tecnología de enrutamiento multicast, que permite llevar los datos desde un origen a varios destinos de tal manera de impactar en el menor grado posible el rendimiento de las redes involucradas. Y aunque multicast no ha sido desplegado en forma amplia en Internet de hoy en día, es muy frecuente en ambientes empresariales.

A su vez, la introducción del nuevo protocolo IPv6 trae consigo un conjunto de nuevas características (incremento del número de direcciones, seguridad, calidad de servicio, mejoras multicast, entre otras) que impulsaran aún más el desarrollo de aplicaciones de red multimedia.

En este sentido, el proyecto Reacciun2 del Centro Nacional de Innovación Tecnológica (CENIT), al cual pertenece la Universidad Central de Venezuela, permite interactuar con este nuevo protocolo y con los desarrollos de aplicaciones, servicios e investigaciones sobre esta nueva tecnología que se trabajan en las universidades del país y centros de investigaciones el mundo entero.

Por todo lo antes expuesto, este trabajo tiene por objetivo una investigación sobre la tecnología multicast y sus protocolos asociados, así como del Protocolo de Internet versión 6 (IPv6) para así definir y proponer una infraestructura que soporte un servicio de hilos musicales sobre una plataforma IPv6 multicast.

Este documento está estructurado de la manera siguiente:

- Capítulo 2 (Planteamiento del Problema): se describe el estado actual de la Red Interna de Sonido de la UCV, así como el objetivo general y específicos del trabajo basados en la propuesta de un servicio multicast.
- Capítulo 3 (Marco Teórico): se exponen los conceptos asociados al despliegue de un servicio multicast sobre IPv6.
- Capítulo 4 (Marco Metodológico): se describe la metodología a utilizar en el desarrollo del trabajo, incluyendo las fases de estudio de la red actual de la UCV, analisis, diseño e implementación del servicio multicast sobre IPv6.

- Capítulo 5 (Conclusiones y Recomendaciones): contiene las conclusiones y recomendaciones finales del trabajo de investigación.

2. Planteamiento del Problema

La Red Interna de Sonido, adscrita a la Dirección de Información y Comunicación de la Universidad Central de Venezuela, es un sistema de sonido interconectado que recorre parte de la Ciudad Universitaria y contempla una programación radial orientada principalmente al público joven. Hoy en día, dicha infraestructura, conformada por el cableado, dispositivos de audio, consolas de sonido, entre otros, se encuentra muy deteriorada, y su alcance actual se limita a sólo algunos pasillos cubiertos de la Ciudad Universitaria.

Aunque existen varios proyectos de investigación de facultades como la de Ciencias Económicas y Sociales, o la de Humanidades y Educación, que contemplan la utilización de la Red Interna de Audio, no ha sido considerada, a corto plazo, una actualización y/o expansión debido a que los costos de inversión son muy elevados.

Es por esto que hoy en dia la Dirección de Información y Comunicación de la UCV no posee un mecanismo eficiente de difusión de audio que abarque todo el campus universitario.

Por otra parte, en los últimos años ha incrementado rápidamente la diversidad de aplicaciones que combinan texto, gráficos, audio y video en Internet, de la misma manera, los protocolos y estándares para comunicaciones necesarios para dar soporte a dichas aplicaciones. Muchas de estas aplicaciones se fundamentan en la tecnología de enrutamiento multicast, que permite llevar datos desde un origen a varios destinos de tal manera de impactar en el menor grado posible el rendimiento de las redes involucradas.

Si bien la utilización de la tecnología de enrutamiento multicast provee innumerables ventajas, para ciertos flujos de datos, con respecto al enrutamiento unicast, esta no ha sido ampliamente desplegada debido a las limitaciones de IPv4 (escasez de direcciones IP, soporte inadecuado para aplicaciones de próxima generación, no fue diseñado para ser seguro, entre otras). Con el despliegue de IPv6 en los últimos años, y con los beneficios (descritos en el Capítulo 3) que en general trae consigo esta versión del protocolo IP, la utilización de la tecnología multicast se verá fuertemente desarrollada bajo esta nueva infraestructura de red.

En Venezuela, parte de este despliegue se realiza a través del Proyecto Reacciun2[1], conformado por las universidades y centros de investigación más importantes del país; dicho proyecto actualizó la plataforma tecnológica de los miembros involucrados, entre las cuales se encuentra la Universidad Central de Venezuela (UCV), en donde se instaló un laboratorio de Internet2, ubicado en la Escuela de Computación de la Facultad de Ciencias, con el fin de realizar trabajos de investigación y capacitación en Internet2 y nuevas tecnologías.

[1] http:// www.reacciun2.edu.ve

Este trabajo aprovechará la infraestructura instalada en la UCV, específicamente la del Laboratorio de Internet2 de la Escuela de Computación, para proponer una infraestructura de red IPv6 multicast, que permita la implementación de un servicio de hilos musicales (música continua agrupada por generos) y a su vez el desarrollo de las bases para futuros servicios que la utilicen.

2.1. Justificación

Los costos asociados a la implementación de un servicio de hilos musicales basados en IPv6 son mínimos, comparados con la de la actualización o expansión de la Red Interna de Sonido. Además, cualquier estación de trabajo con soporte IPv6 podría eventualmente ser cliente de este sistema de hilos musicales, lo que expandiría el alcance a todo el campus universitario. Por otro lado, el desarrollo de IPv6 en la UCV a través del proyecto Reacciun2 es reciente, y aunque existen numerosas investigaciones para ser desarrolladas, pocos hoy en día utilizan la infraestructura de IPv6.

Por tal motivo el desarrollo de este Trabajo Especial de Grado representa un reto importante, ya que propondrá la implementación de un servicio multicast de hilos musicales, describirá la tecnología multicast sobre IPv6, documentará los procedimientos necesarios para el funcionamiento de esta infraestructura y finalmente aportará conocimiento científico, teórico, metodológico y académico, referente a la utilización de IPv6 en el país.

2.2. Objetivos

2.2.1. Objetivo General

Proponer la implementación de un servicio de hilos musicales utilizando IPv6 multicast para la Universidad Central de Venezuela.

2.2.2. Objetivos Específicos

- Estudiar el Protocolo de Internet versión 6 (IPv6), debido a que es la base para la implementación de servicios multicast.
- Estudiar los protocolos multicast para IPv6, con el fin de definir cuáles son los necesarios para diseñar la infraestructura.
- Investigar aplicaciones similares a la investigación planteada, y de esta manera obtener el conocimiento de experiencias similares y los posibles problemas y soluciones.
- Definir la infraestructura necesaria para la solución multicast, con el fin de colocar en producción servicios multicast.
- Estudiar los diferentes servidores de streaming para escoger el más idóneo para el servicio de hilos musicales.
- Proponer una configuración para los componentes que participan en la solución multicast, para permitir la utilización de servicios multicast.
- Hacer pruebas de funcionalidad para garantizar el correcto funcionamiento del servicio de hilos musicales.

3. Marco Teórico

3.1. Internet Protocol version 6

Las nuevas tecnologías y aplicaciones para usuarios finales demandan hoy en día una gran cantidad de direcciones IP. Millones de personas en todo el mundo esperan tener a su disposición servicios de comunicación de alta calidad, semejantes a los que disponen en su casa o en su oficina, tal es el caso de los dispositivos "always-on" (siempre encendidos) los cuales necesitan direcciones IP permanentes para contactarlos (teléfonos móviles, juegos, voz residencial sobre IP, Fax IP, entre otros).

La evidencia de falta de direcciones fue el motivo básico por el que surge, en el seno del IETF (*Internet Engineering Task Force),* la necesidad de crear un nuevo protocolo, que en un primer momento se denominó IPng (*Internet Protocol Next Generation)*, y que terminó denominándose IPv6 [1] (Internet Protocol version 6).

IPv6 se presenta como la nueva versión del protocolo de red para las comunicaciones TCP/IP. Como es conocido, por muchos años, IPv4 [2] ha sido el protocolo usado para transportar paquetes de datos, voz y video sobre Internet, pero IPv6 promete ser el soporte para la próxima generación de Internet y ofrece unas significativas mejoras en términos de escalabilidad, seguridad, movilidad, convergencia, entre otras.

3.1.1. Justificación de IPv6

El inicio de las comunicaciones entre equipos se diseñó con conectividad punto-a-punto, lo que dio origen a Internet. A medida que este fue popularizándose, y el acceso al mismo fue creciendo, también fue incrementándose la necesidad de direcciones IP (ver Figura 3-1 tomada de [85]). Esto originó un aumento en los esfuerzos de conservación de las direcciones, creando nuevos estándares y protocolos para su preservación, tales como NAT (Network Address Translation) [3], CIDR (Classless Inter-Domain Routing) [4], direccionamiento compartido con PPP (Point-to-Point Protocol) [5] y DHCP (Dynamic Host Configuration Protocol) [6].

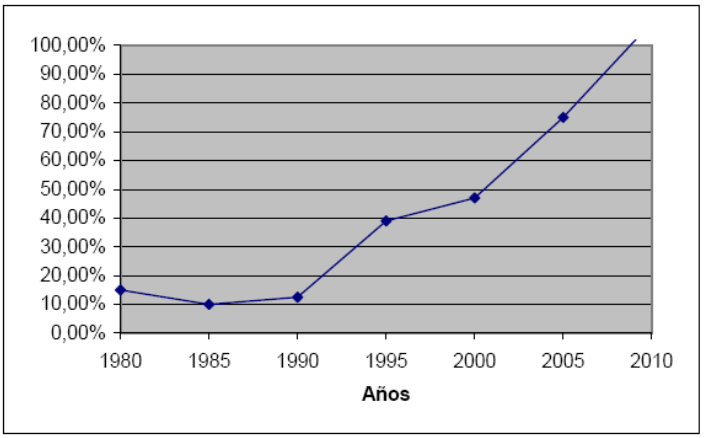

Figura 3-1: Asignación de Direcciones IP.

Teóricamente el espacio de direccionamiento de 32 bits de IPv4 garantiza alrededor de 4 billones de direcciones para los dispositivos. Pero el límite práctico para ese espacio

de direcciones según [7] es de alrededor 250 millones de dispositivos, de los cuales dos tercios del total de direcciones IPv4 en todo el mundo ya han sido asignados dentro de la comunidad global de Internet.

A continuación se mencionan algunos factores importantes por lo cual se hizo necesario el desarrollo de IPv6:

- Direccionamiento de 32 bits de IPv4: teóricamente permitiría 4 billones de dispositivos con direcciones IP, pero aproximadamente el 40 % del espacio de direcciones está aun sin uso. Esto debido, entre otras cosas, a una importante falta de coordinación (durante la década de los 80) en la delegación de direcciones, sin ningún tipo de optimización, dejando incluso grandes espacios de direcciones IP discontinuos.
- Población en Internet: aproximadamente 945 millones de usuarios para el año 2004, lo que representa tan sólo el 10-15% de la población total. Se calcula que para el año 2050 existirán alrededor de 9 billones de usuarios. Países con Internet emergiendo necesitan espacios de direcciones IP, tal es el caso de China el cual usa cerca de 2 Clases A (Noviembre, 2001).
- Internet Móvil: presenta una nueva generación de dispositivos de Internet tales como PDA (~20 millones en 2004), teléfonos móviles (~1.5 billones en 2003), Tablet PC, entre otros. Habilitadas a través de nuevas tecnologías como 3G, 802.11, entre otras.
- Redes de Transporte Móviles: se estima que existirán 1 billón de automóviles con soporte a tecnología inalámbrica que necesitaran direcciones IP en los próximos años. Muchos mercados verticales brindan hoy acceso a Internet en aviones (Lufthansa), trenes (Narita Express), etc.

3.1.2. Características y Beneficios de la Tecnología de IPv6

Las nuevas características de IPv6 llevan consigo un conjunto de beneficios entre los cuales se pueden mencionar:

- Mayor número de direcciones: IPv6 tiene direcciones de 128 bits, lo cual implica un gran incremento en el número de direcciones IP disponibles. Los escenarios donde la escasez de direcciones IP imponían la instalación de NAT desaparecerán, lo que permite una configuración de red más simplificada y fácil de administrar, así como reduce la complejidad en hardware y software.
- Conectividad final-a-final: IPv6 elimina la necesidad de NAT y rescata la comunicación final-a-final. IPv4 necesita NAT en ciertos escenarios donde hay escasez de direcciones IP. Pero NAT no trabaja bien con ciertas aplicaciones final-a-final como VoIP[2].
- Enrutamiento eficiente: IPv6 tiene un encabezado más simple que IPv4. Esto reduce la sobrecarga de procesamiento en los routers, originando menor complejidad en hardware y un procesamiento de paquetas más rápidos. El direccionamiento jerárquico de IPv6 permite ahorrar espacio de almacenamiento con tablas de enrutamiento más pequeñas y aumenta la eficiencia en la red global.

[2] http://es.wikipedia.org/wiki/Voz_sobre_IP

- Autoconfiguración: IPv6 provee autoconfiguración de direcciones IP en dispositivos con IPv6 habilitado. Esto incrementa la escalabilidad y simplifica la administración de redes. Nuevos dispositivos pueden ser conectados directamente a una red sin configuración manual de una dirección IP o necesidad de un servidor DHCP.
- Seguridad: IPSec [8] es obligatorio en IPv6, esto provee un sólido marco de trabajo seguro para las comunicaciones en Internet. IPSec puede ser usado para implementar encriptación y autenticación.
- Movilidad y multicast: provee mejoras para IPv6 móvil las cuales optimizan las redes inalámbricas de hoy en día. La adición del campo "scope" para multicast renovó el marco de trabajo para el tráfico multicast.
- Mecanismo de migración: la suite de protocolos de transición y traslación ayudan en los planes de migración de IPv4 a IPv6, mientras permite la coexistencia de ambos protocolos.

3.1.3. Formato del Encabezado IPv6

El encabezado de IPv6 (ver Figura 3-2 tomada de [1]) ha sido simplificado con respecto al de IPv4. Las opciones fueron reestructuradas para ubicarse después del encabezado y no formar parte de él. Esto hace que el procesamiento del encabezado de IPv6 en los nodos intermedios sea mucho más fácil.

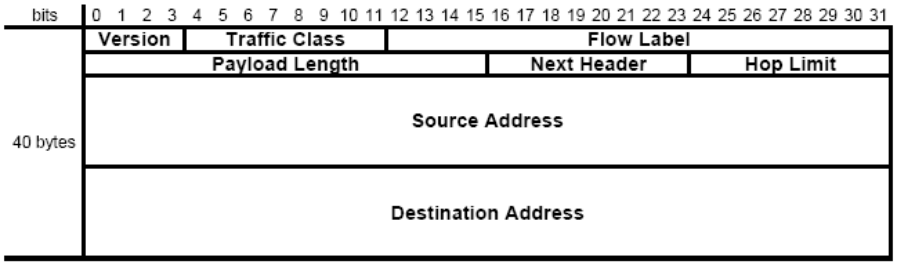

Figura 3-2: Formato del Encabezado IPv6.

Se llevaron a cabo cambios importantes con respectos a los campos del encabezado (ver Figura 3-3 tomada de [85]), los cuales se pueden clasificar en tres aspectos claves:

- Revisiones
  - El campo *Total Length* del encabezado se renombró *Payload Length*.
  - El campo *Time to Live* pasa a llamarse *Hop Limit*.
  - El campo *Protocol* pasa a llamarse *Next Header*.
  - El campo *Type of Service* pasa a llamarse *Traffic Class*.
  - Se incrementa el direccionamiento de 32 bits a 128 bits.

- Mejoras
  - Los campos de fragmentación se movieron fuera de la base del encabezado.
  - El campo *Options* se movió fuera de la base del encabezado.
  - Se eliminó el campo *checksum* del encabezado.
  - El campo *Payload Length* no incluye al tamaño del encabezado IPv6.

- Extensiones: Se agregó el campo *Flow Label* para proveer calidad de servicio mejorada en el futuro.

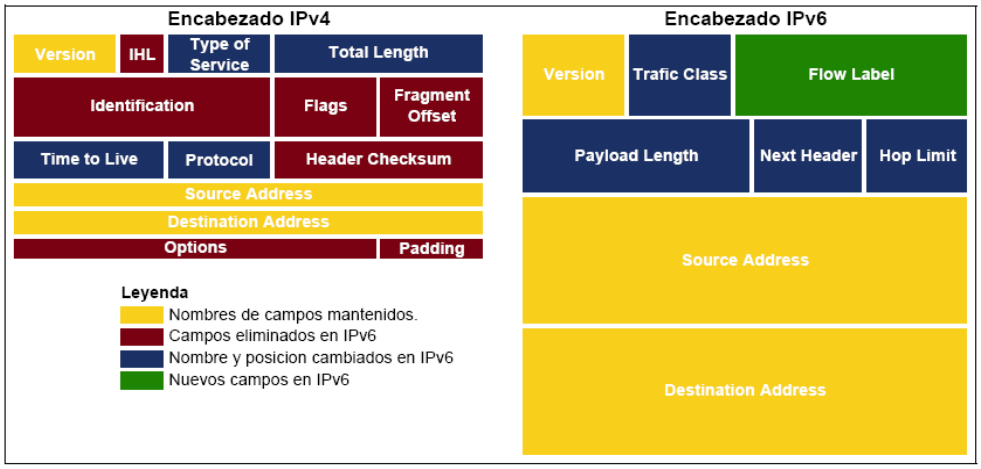

Figura 3-3: Comparación del Encabezado de IPv4 e IPv6.

3.1.4. Direccionamiento de IPv6

Unos de los motivos para crear IPv6 fue corregir las deficiencias de direccionamiento de IPv4. Junto con la necesidad de adquirir más direcciones, los diseñadores de IPv6 buscaban una forma de interpretar, asignar y usar las direcciones de una manera que estuvieran acordes con las redes de Internet actuales.

El direccionamiento de IPv6 está definido principalmente en [1], sin embargo, muchos de los detalles de su implementación están contenidos en [10] y [11]. Su esquema de direccionamiento es similar en concepto al direccionamiento de IPv4, pero ha sido revisado completamente para crear un sistema de direcciones que sea capaz de soportar la continua expansión de Internet y las nuevas aplicaciones previsibles para el futuro.

Entre las características más resaltantes del direccionamiento de IPv6 se mencionan las siguientes:

- Funciones de direccionamiento: Las principales funciones del direccionamiento IPv6 son la identificación de interfaces de red y el enrutamiento.
- Representación del prefijo e interpretación de la dirección: Las direcciones IPv6 tienen una estructura definida por dos partes; una que identifica la red y otra que identifica el dispositivo o interfaz. La longitud del prefijo, especificada como en la notación CIDR [4] de IPv4, es usada para indicar la longitud del identificador de red.
- Direcciones públicas y privadas: el concepto de asignación de direcciones públicas y privadas definida en [9] para direcciones IPv4 se mantiene en IPv6 (direcciones globales únicas y direcciones locales al enlace), aunque son definidas y usadas de manera distinta como se describe en [10].

Representación de Direcciones IPv6

Debido al incremento en el tamaño del espacio de direcciones de 32 bits (IPv4) a 128 bits (IPv6), el sistema de notación punto decimal tradicional usado en IPv4 hace difícil la manipulación de direcciones IPv6, por ello este nuevo esquema de direccionamiento define su propio sistema de notación.

A continuación se exponen dos formas convencionales para representar una dirección IPv6, según [10]:

Notación Dos Puntos Hexadecimal

Bajo esta notación las direcciones están agrupadas en 8 grupos de 16 bits, separadas por dos puntos (:) de la manera siguiente:

805B:2D9D:DC28:0000:0000:FC57:D4C8:1FFF

Se pueden suprimir los ceros contiguos no significativos en un mismo grupo para reducir el tamaño de la representación:

805B:2D9D:DC28:0:0:FC57:D4C8:1FFF

También permite que una simple sucesión de ceros contiguos en una dirección IPv6 pueda ser reemplazada por doble dos puntos (::), por ejemplo:

805B:2D9D:DC28::FC57:D4C8:1FFF

Se puede determinar cuantos ceros fueron reemplazados por el doble dos puntos (::) contando los grupos hexadecimales faltantes para los 8 grupos que posee una dirección completa. El doble dos puntos (::) sólo puede aparecer una vez en una dirección IP.

Notación Mezclada de IPv6

Esta notación es utilizada para expresar direcciones IPv6 que incorporan direcciones IPv4 (ver “Direcciones IPv6 con Direcciones IPv4 Integradas” más adelante). Es útil en entornos de transición donde existen nodos IPv6 e IPv4. Los primeros 96 bits se definen con la notación dos puntos hexadecimal (:) de IPv6, y los 32 bits siguientes con notación punto decimal (.) de IPv4, por ejemplo:

805B:2D9D:DC28::FC57:212.200.31.255

La Figura 3-4 (tomada de [84]) muestra la representación de las dos formas convencionales expuestas anteriormente.

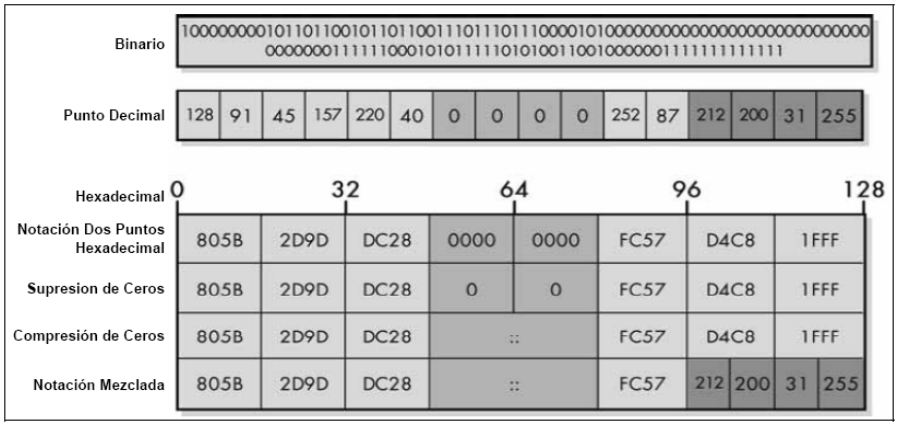

Figura 3-4: Representación Binaria, Decimal y Hexadecimal de direcciones IPv6.

Así como en IPv4, las direcciones IPv6 están compuestas por dos grupos de bits, uno representa al identificador de red y otro al dispositivo. El identificador de red es llamado prefijo, y el número de bits usados en él es la longitud del prefijo. Este prefijo es representado por la adición de un slash (/) después de la dirección y colocando la longitud del prefijo después del slash.

Prefijo (ID de Red) **Longitud del Prefijo**

805B:2D9D:DC28::FC57:D4C8:1FFF/48

Tipos de Direcciones IPv6

Un importante cambio en el modelo de direccionamiento de IPv6 son los tipos de direcciones soportados. En IPv4 existe soporte para tres tipos de direcciones: unicast, multicast y broadcast, en donde la mayor parte del tráfico actual es unicast. Con respecto al soporte a IP multicast, éste no fue ampliamente desarrollado hasta muchos años después de que Internet fue establecido, y el uso de broadcast en IP es severamente restringido por razones de rendimiento.

En IPv6, según [10], también existe soporte para tres tipos de direcciones:

- ***Unicast*:** Un identificador para una sola interfaz. Un paquete enviado a una dirección unicast es entregado a una interfaz identificada con esa dirección.
- ***Anycast:*** Un identificador para un conjunto de interfaces (típicamente pertenecientes a diferentes nodos). Una dirección anycast es usada cuando un mensaje debe ser enviado a cualquier miembro de un grupo (el más cerca, de acuerdo a las métricas de distancia del protocolo de enrutamiento), pero no necesariamente a todos ellos.
- ***Multicast:*** Un identificador para un conjunto de interfaces (típicamente pertenecientes a diferentes nodos). Un mensaje enviado a una dirección multicast va a todos los dispositivos que pertenecen al grupo identificado por esa dirección. IPv6 incluye características multicast mucho mejores y más direcciones multicast que en IPv4.

Como se puede observar, no hay direcciones broadcast en IPv6, debido a que su funcionalidad está implantada usando direcciones multicast para grupos de dispositivos. Los bits de mayor orden en una dirección IPv6, permiten definir diferentes tipos de direcciones, como se muestra en la Tabla 3-1 (tomada de [10]).

Tipo de Dirección	Prefijo en Binario	Notación en IPv6
No Especificada	00…0 (128 bits)	::/128
Loopback	00…1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Unicast Locales al Enlace	1111111010	FE80::/10
Unicast Globales	Cualquier otra cosa	

Tabla 3-1: Distribución del Espacio de Direcciones IPv6.

Las direcciones anycast son tomadas del mismo espacio de direcciones unicast y no tienen alguna sintaxis que las distinga de ellas.

Antes de ahondar con más detalles en cada uno de los tipos de direcciones mencionados anteriormente, es importante definir que cada dirección IPv6, excepto la "No Especificada" (ver Tabla 3-1), tiene un alcance específico; es decir, una extensión topológica dentro de la cual la dirección puede ser utilizada como identificador único para una interfaz o conjunto de interfaces. El alcance está codificado como parte de la dirección, tal como se especifica en [10].

Para las direcciones unicast, según [12], se definen dos alcances:

- Link-Local (Local al Enlace): interfaces identificadas unívocamente sólo dentro de un mismo enlace.
- Global: interfaces identificadas unívocamente en cualquier parte de Internet.

En [10] se menciona la dirección unicast con alcance Site-Local (Local al Sitio), pero ésta pasó a la obsolescencia por presentar muchas deficiencias (ambigüedad de direcciones y definición confusa de un sitio) como se describe en [13]. El candidato para su sustitución se denomina "Unique Local IPv6 Unicast Address" y se define en [14] (ver Figura 3-5 tomada de [85]).

Las direcciones anycast tienen el mismo alcance que las direcciones unicast debido a que son tomadas del mismo espacio de direcciones. Las direcciones multicast tiene catorce (14) posibles alcances.

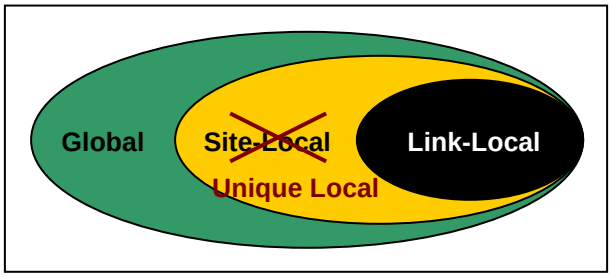

Figura 3-5: Alcance de la Direcciones IPv6 Unicast.

Direcciones Unicast

Las direcciones IPv6 unicast son agregables, con máscaras de bits contiguos similares al caso de IPv4. Existen varios tipos de direcciones unicast en IPv6, en particular la de tipo Global y Link-Local. También existen algunos subtipos de propósitos especiales de la Global, como la de Compatibilidad.

Identificadores de Interfaz

Con el acondicionamiento de las direcciones en IPv6, se presentó una oportunidad para crear una forma de corresponder las direcciones IP unicast con las direcciones físicas de red. La implantación de esta técnica de correspondencia fue uno de los factores que influyó en el tamaño de las direcciones IPv6. De 128 bits de una dirección IPv6, se reservaron 64 bits para uso del identificador de interfaz (ID de interfaz), el cual es análogo al identificador de equipo en IPv4.

Los identificadores de interfaz en IPv6 son usados para identificar interfaces en un enlace o vínculo, son únicos dentro del prefijo de una subred. Todas las direcciones unicast, excepto las que empiezan con el valor binario 000, requieren un Identificador de interfaz (ID) de 64 bits de longitud que puede ser asignado de diferentes formas:

- Autoconfigurado a partir de una dirección MAC de 48 bits, y expandida a un formato EUI-64 Modificado.
- Configurada manualmente.
- Autogeneradas pseudos-aleatoriamente (protección de la privacidad).
- Asignadas vía DHCP.

Los IDs de interfaz basados en el formato EUI-64 Modificado pueden tener un alcance universal, cuando se derivan de un token universal, o un alcance local, cuando no se dispone de un token global o cuando éste no es deseado. El ID de interfaz definido a partir de una interfaz Ethernet está basado en el identificador IEEE EUI-64 y se forma de la siguiente manera (ver Figura 3-6 tomada de [85]):

- El identificador de empresa (OUI) de la dirección Ethernet (los primeros tres bytes) se convierte en los tres primeros bytes del ID EUI-64 Modificado.
- El cuarto y quinto byte del ID EUI-64 Modificado son fijados al valor hexadecimal FFFE.
- Los últimos tres bytes de la dirección Ethernet se convierten en los últimos tres bytes del ID EUI-64 Modificado.
- Por último, para asegurar que la dirección elegida proviene de una dirección Ethernet única, el bit u (bit universal/local en términos de IEEE EUI-64) se coloca a uno (1) para indicar un alcance universal, y a cero (0) para una alcance local.

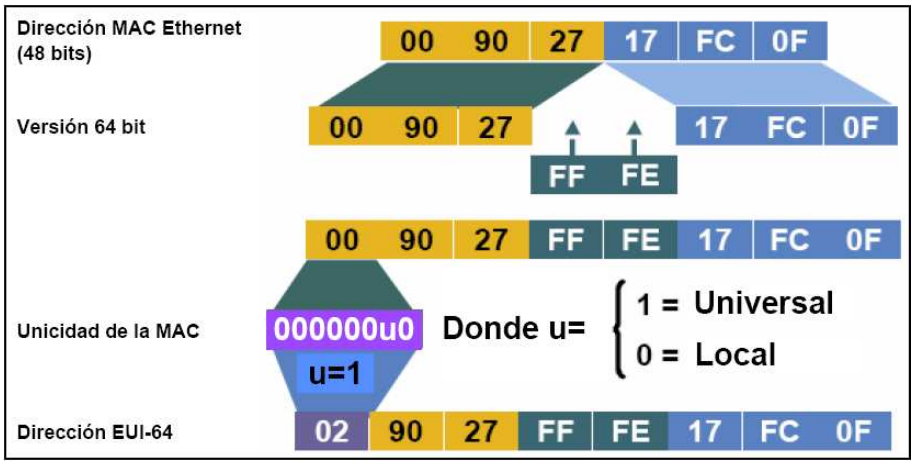

Figura 3-6: Ejemplo de Asignación de ID EUI-64 Modificado.

Direcciones IPv6 Unicast Especiales: Reservada, Privada, No Especificada y Loopback.

Una porción del espacio de direcciones de IPv6 está reservada por IETF. El bloque reservado está en el tope del espacio de direcciones, empezando con 0000 0000 (00 en hexadecimal). Este representa el 1/256 del espacio total de direcciones.

Otro bloque de direcciones se utiliza como direcciones privadas, las cuales pueden ser de tipo link-local o site-local, y nunca son encaminadas fuera de la red de una compañía en particular. Las direcciones privadas se identifican por los primeros 10 bits con el formato siguiente 111111101X, donde X puede tomar un valor hexadecimal entre 8 y F.

La dirección IPv6 0:0:0:0:0:0:0:0 (::) es llamada “no especificada” y no debe ser asignada a ningún nodo, e indica la ausencia de una dirección. Es utilizada en el campo origen de paquetes IPv6 enviados para inicializar un dispositivo antes de aprender su propia dirección.

La dirección Loopback 0:0:0:0:0:0:0:1 (::1) puede ser utilizada por un nodo para enviar paquete a si mismo. No debe ser asignada a ninguna interfaz física. Puede asociarse con una dirección unicast de tipo Link-Local de una interfaz virtual (llamada interfaz de Loopback) con un enlace imaginario que no va a ningún lado.

Direcciones Unicast de Tipo Global

Se puede anticipar que las direcciones unicast serán usadas por la mayoría de tráfico de Internet bajo IPv6, tal como es en el caso para IPv4. Es por eso que el bloque más grande de direcciones (1/8 del espacio de direcciones total) es asignada a ellas, y está identificada por los primeros bits 001 en la dirección.

El formato general de una dirección IPv6 Unicast Global se define en la Figura 3-7 (tomada de [10]).

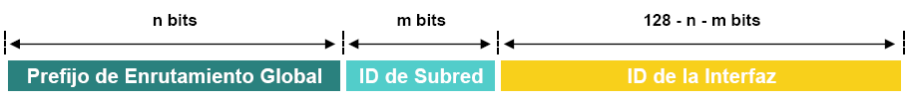

Figura 3-7: Formato General de una Dirección IPv6 Unicast Global.

Donde el prefijo de enrutamiento global (típicamente de estructura jerárquica) es un valor asignado a un sitio (un conjunto de subredes/enlaces), el ID de subred es un identificador de un enlace dentro del sitio, y el ID de interfaz es de la forma EUI-64 Modificado.

En [11] se define el formato de una dirección IPv6 unicast global, ver Figura 3-8, tomada de [10].

Figura 3-8: Formato de una Dirección IPv6 Unicast Global.

Direcciones Unicast de Tipo Link-Local

Las direcciones Link-Local (ver Figura 3-9, tomada de [10]) tienen un alcance que se refiere a un enlace físico particular (una red física). Están diseñadas para propósitos tales como configuración automática de direcciones, descubrimiento de vecinos, o cuando no hay routers presentes. Por otra parte los routers no deberían reenviar paquetes cuya dirección origen o destino sea de tipo Link-Local a otros enlaces.

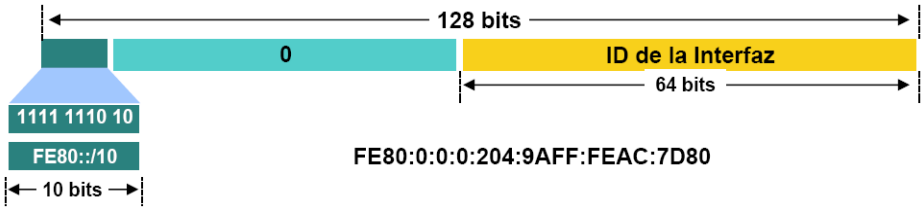

Figura 3-9: Formato de una Dirección IPv6 Unicast Link-Local.

Direcciones Unicast de Tipo Unique-Local

Por defecto, el alcance de las direcciones Unique-Local (ver Figura 3-10, tomada de [14]) es global, debido a que poseen prefijos que son globalmente únicos. Su limitación está en el encaminamiento de los prefijos, los cuales están limitados a un sitio y no a Internet. Principalmente usada para redes privadas virtuales (VPN, por sus siglas en inglés), comunicaciones locales, entre otros.

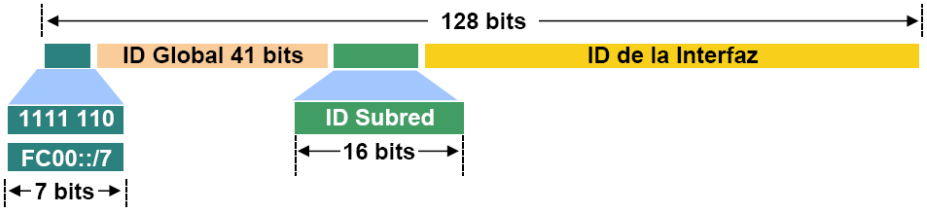

Figura 3-10: Formato de una Dirección IPv6 Unicast Unique-Local.

Direcciones IPv6 con Direcciones IPv4 Integradas

Dos tipos de direcciones IPv6 son definidas para llevar una dirección IPv4 en los últimos 32 bits de la dirección (ver Figura 3-11 y 3-12, tomadas de [10]). Estas son:

- Direcciones IPv6 IPv4-Compatibles: fueron definidas para asistir en la transición hacia IPv6. Por lo general eran usadas en dispositivos que tenían soporte para IPv4 e IPv6. La dirección IPv4 usada debía ser una dirección unicast global única. Hoy en día este tipo de dirección no se utiliza debido a que los mecanismos de transición actuales no la utilizan. Su formato era el siguiente:

Figura 3-11: Formato de una Dirección IPv6 IPv4-Compatible.

- Direcciones IPv6 IPv4-Mapeadas: este tipo de direcciones es usada para representar las direcciones de nodos IPv4 como direcciones IPv6. Por lo general son usadas en dispositivos que sólo tiene soporte para direcciones IPv4. En [16] se detalla a fondo el uso de estas direcciones. Su formato es el siguiente:

Figura 3-12: Formato de una Dirección IPv6 IPv4-Mapeada.

Direcciones Anycast

Una dirección anycast es una dirección que es asignada a más de una interfaz (típicamente perteneciente a diferentes nodos), con la propiedad que un paquete enviado a una dirección anycast es encaminada a la interfaz más cerca que tiene esa dirección, de acuerdo a las métricas de distancia de los protocolos de enrutamiento.

Las direcciones anycast son tomadas del mismo espacio de direcciones de las direcciones unicast, por tal motivo no tienen una sintaxis que las distingan. Cuando una dirección unicast es asignada a más de una interfaz, entonces se convierte en una dirección anycast.

Existe una dirección anycast, requerida para cada subred, que se denomina “Dirección Anycast del Router de la Subred” (ver Figura 3-13, tomada de [10]). Todos los routers deben soportar esta dirección para las subredes a las que están conectados. Los paquetes enviados a esta dirección anycast, serán enviados a un router de la subred.

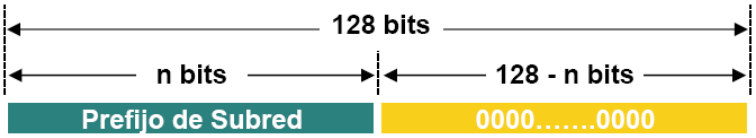

Figura 3-13: Formato de una Dirección IPv6 Anycast del Router de la Subred.

Direcciones Multicast

Una dirección multicast en IPv6 es un identificador para un grupo de interfaces (típicamente en diferentes nodos). Permite que un dispositivo pueda enviar datagramas a un grupo de otros dispositivos. Las direcciones multicast conforman 1/256 del espacio total de direcciones IPv6.

El formato de una dirección multicast se muestra en la Figura 3-14 (tomada de [10]).

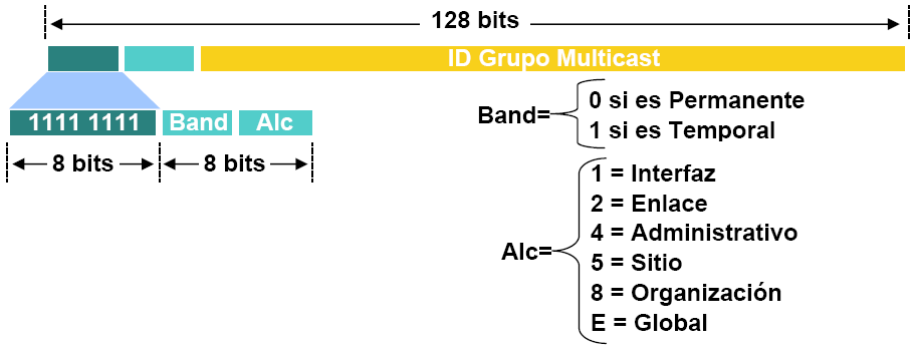

Figura 3-14: Formato de una Dirección IPv6 Multicast.

Los primeros 8 bits en uno (1) identifican a una dirección multicast, 1111 1111 (FF en hexadecimal).

“Band” es un conjunto de 4 banderas. El primer bit debe ser inicializado siempre en 0, el segundo bits llamado “R” (Integra direcciones de Puntos Rendezvous en direcciones IPv6 multicast) se define en [17], el tercer bit llamado “P” (direcciones multicast basadas en prefijo unicast) se define en [18] y el cuarto bit “T” indica la permanencia de una dirección multicast (0 = Permanente, 1 = No Permanente).

“Alc” es un conjunto de 4 bits que definen 16 valores para limitar el alcance de un grupo multicast (ver Figura 3-15 tomada de [84]). Los valores son los siguientes:

- Interface-Local (1): limita el alcance a una sola interfaz en un nodo y es usado sólo para transmisiones multicast de loopback.
- Link-Local (2): limita el alcance a la misma región topológica que el correspondiente alcance unicast.
- Admin-Local (4): el alcance más pequeño que debe ser administrativamente configurado.
- Site-Local (5): limita el alcance a un sitio.
- Organization-Local (8): el alcance está definido para cubrir varios sitios de una misma organización.
- Global (E): el alcance está definido a todo Internet.
- Sin Asignar (6, 7, 9, A, B, C, D): disponibles para que los administradores definan regiones multicast adicionales.
- Reservados (0, 3, F).

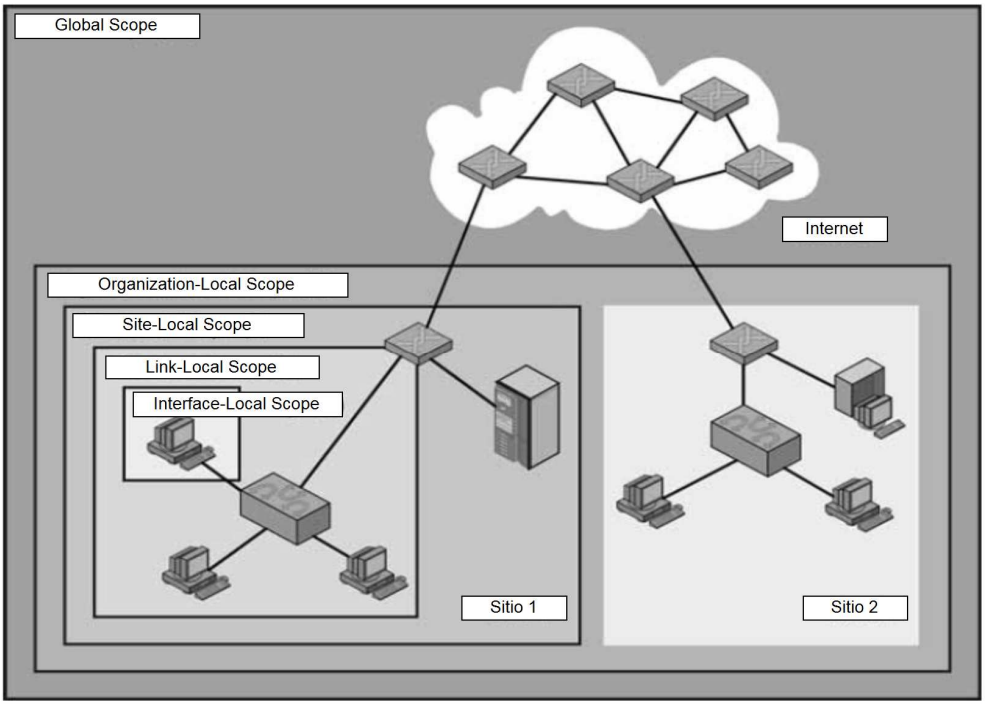

Figura 3-15: Alcances Multicast en IPv6.

El campo de permanencia (T) permite determinar explícitamente cuales direcciones multicast están disponibles para uso normal y cuales están ya asignadas (bien conocidas). Las direcciones multicast bien conocidas están definidas en [19]. Entre las más importantes se encuentran:

- Direcciones de Todos los Nodos: FF01:0:0:0:0:0:0:1 (local a la interfaz) y FF02:0:0:0:0:0:0:1 (local al enlace).
- Direcciones de Todos los Routers: FF01:0:0:0:0:0:0:2 (local a la interfaz), FF02:0:0:0:0:0:0:2 (local al enlace) y FF05:0:0:0:0:0:0:2 (local al sitio).
- Direcciones de Nodo Solicitado: FF02:0:0:0:0:1:FFXX:XXXX, básicamente utilizada con dos propósitos, remplazar ARP (Address Resolution Protocol - [20]) y detectar direcciones duplicadas [22].

Las direcciones multicast de nodo solicitado facilitan las consultas de los nodos de red durante las resolución de direcciones. Existe una por cada dirección unicast y anycast. Son formadas tomando los últimos 24 bits de una dirección unicast o anycast y agregándoselo al prefijo FF02:0:0:0:0:1:FF00::/104 resultando una dirección multicast en el rango FF02:0:0:0:0:1:FF00:0000 al FF02:0:0:0:0:1:FFFF:FFFF (ver Figura 3-16, tomada de [10]).

Figura 3-16: Dirección IPv6 Multicast de Nodo Solicitado.

Las direcciones multicast asignadas permanentemente son independientes del valor definido en el alcance. Por ejemplo, si al grupo de servidores NTP (Network Time

Protocol [21]) es asignado una dirección multicast permanente con un ID de grupo 101 (en hexadecimal), entonces:

- FF01:0:0:0:0:0:0:101 representa todos servidores NTP en la misma interfaz (Nodo).
- FF02:0:0:0:0:0:0:101 representa todos servidores NTP en el mismo enlace.
- FF08:0:0:0:0:0:0:101 representa todos servidores NTP en la misma organización.
- FF0E:0:0:0:0:0:0:101 representa todos servidores NTP en Internet.

Las direcciones multicast no asignadas permanentemente son válidas sólo dentro del alcance definido. Por ejemplo, un grupo identificado con la dirección multicast no permanente FF15:0:0:0:0:0:0:101 de alcance site-local no tiene relación con otro grupo que utiliza la misma dirección en un sitio diferente, ni con un grupo no permanente usando el mismo ID de grupo con diferente alcance, ni con un grupo permanente con el mismo ID de grupo.

Por último, el ID del grupo multicast (ver Figura 3-14) identifica al grupo multicast, ya sea permanente o temporal, dentro de un alcance definido.

Como regla, las direcciones multicast no deben ser usadas como dirección origen en un paquete IPv6. Igualmente los routers no deben enviar paquetes multicast más allá del alcance indicado por el campo alcance en la dirección multicast destino.

Direcciones Requeridas por un Nodo

Es requerido que un dispositivo reconozca las siguientes direcciones como identificadores propios:

- Una dirección de tipo Link-Local para cada interfaz.
- Cualquier dirección unicast o anycast que ha sido configurada manualmente en las interfaces de un nodo.
- La dirección loopback.
- La dirección multicast de “todos los nodos” definida anteriormente.
- Las direcciones multicast de “nodo solicitado” por cada una de las direcciones unicast y/o anycast.
- Direcciones multicast de todos los grupos al cual el nodo pertenece.

Adicionalmente los routers deben reconocer:

- Las direcciones anycast subred-router para todas las interfaces para la cual está configurado actuar como router.
- Todas las otras direcciones anycast con la cual el router ha sido configurado.
- La dirección multicast de “todos los routers” definida anteriormente.

3.1.5. Autoconfiguración y Renumeración en IPv6

Autoconfiguración

Una de las características más potentes e interesantes implantadas en IPv6 permite a los dispositivos en una red IPv6 configurarse independientemente de servicios externos tales como DHCP.

IPv6 soporta mecanismos de autoconfiguración con estado y sin estado, tal como se define en [22]. La autoconfiguración sin estados requiere mínima configuración en los routers, ninguna configuración manual de dispositivos ni servidores adicionales. Los mecanismos sin estados permiten a un dispositivo generar su propia dirección, utilizando una combinación de información local e información anunciada por los routers.

En el modelo de autoconfiguración con estado, los dispositivos obtienen la dirección para su interfaz y/o parámetros e información de configuración de un servidor. Estos servidores mantienen una base de datos de las direcciones que han sido asignadas y a quien pertenece.

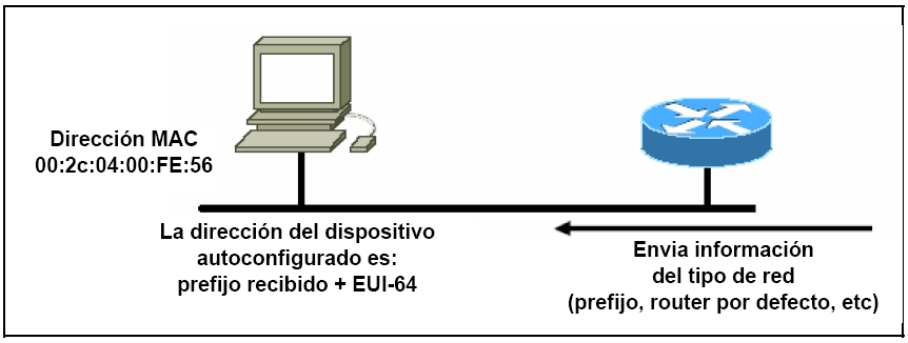

Figura 3-17: Autoconfiguración sin Estado.

Para la autoconfiguración sin estados (ver Figura 3-17 tomada de [85]) se deben cumplir los siguientes pasos:

1. **Generación de la dirección de tipo Link-Local**: El dispositivo genera una dirección de tipo Link-Local. Estas direcciones comienzan con el prefijo FE80::/10. La dirección generada usa esos 10 bits, seguida de 54 ceros y el ID de interfaz de 64 bits [15], generalmente derivado de la dirección (MAC) de la capa de enlace de datos.
2. **Prueba de unicidad de la dirección de tipo Link-Local**: El nodo prueba que la dirección generada no se encuentre utilizada por otro dispositivo en la red local, para esto envía un mensaje de “Neighbor Solicitation” del protocolo NDP (Neighbor Discovery Protocol) [23], si recibe una respuesta de tipo “Neighbor Advertisement” indica que la dirección ya está en uso, por lo tanto se desactiva la interfaz y se genera un mensaje de error. En este caso la configuración se debe hacer manualmente.
3. **Asignación de la dirección de tipo Link-Local**: Asumiendo que se pasó la prueba de unicidad, el dispositivo asigna la dirección de tipo Link-Local a la

interfaz. Esta dirección IP puede utilizarse para comunicaciones dentro de la red local, pero no hacia Internet.

4. **Contacta al router:** El nodo intenta contactar a un router local en busca de más información para continuar la configuración. Esto lo hace escuchando mensajes de “Router Advertisement” enviados periódicamente por el router, o enviando mensajes de “Router Solicitation” para así contactar a los routers dentro del enlace.
5. **Directivas del router:** El router provee directivas al nodo sobre como proceder con la autoconfiguración. Puede decirle al nodo que en la red la autoconfiguración con estado se está usando. Alternativamente, puede decirle al nodo como determinar su dirección de tipo Global.
6. **Configuración de la dirección Global:** Asumiendo que la autoconfiguración sin estados está en uso en la red, el dispositivo puede configurar por si mismo su dirección de tipo Global para Internet. Esta dirección es generalmente formada con el prefijo provisto por el router y el identificador de dispositivo generado en el primer paso. Igualmente esta dirección debe pasar la prueba de unicidad descrita en el punto 2.

Claramente se puede observar que este método tiene numerosas ventajas sobre la configuración manual y la basada en un servidor DHCP. Es particularmente útil en el soporte a la movilidad de dispositivos IP, debido que ellos pueden moverse a nuevas redes y obtener direcciones válidas sin ningún conocimiento de servidores locales o prefijos de red.

Renumeración

La renumeración de dispositivos (ver Figura 3-18, tomada de [85]) es un método relacionando con la autoconfiguración. Una manera bajo IPv6 en que las redes pueden ser renumeradas es teniendo routers que especifiquen un intervalo de expiración de los prefijos de red cuando la autoconfiguración es hecha. Luego, ellos pueden enviar nuevos prefijos que dicen a los dispositivos que regeneren sus direcciones IP. Otras formas de renumerar se especifican en [24] y [25].

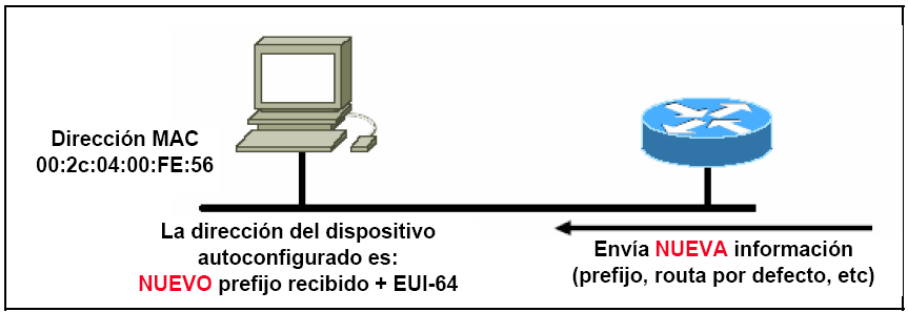

Figura 3-18: Renumeración con Autoconfiguración.

3.1.6. Familia de Protocolos de IPv6

IPv6 no es un protocolo aislado, trae consigo una familia de protocolos los cuales aumentan o reemplazan los ya existentes en IPv4. Entre los más importantes se encuentran:

- **ICMPv6 (Internet Control Messages Protocol version 6):** ICMPv6 está definido en [26], es usado por nodos IPv6 para reportar errores encontrados durante el procesamiento del paquete, y realizar otras funciones tales como diagnósticos (ICMPv6 “ping”). Básicamente es una modificación de ICMP para IPv4, los tipos de mensajes son similares con diferencias en los tipos y códigos.
- **Neighbor Discovery:** definido en [23], provee mecanismos para que los nodos determinen las direcciones de capa de enlace de vecinos que se encuentra ubicados en enlaces directamente conectados; los equipos o estaciones finales lo utilizan para encontrar los routers vecinos dispuestos a enviar paquetes en su nombre; y finalmente los routers utilizan este protocolo para activamente determinar cuales vecinos se encuentra o no alcanzables, y detectar cambios en las direcciones de capa de enlace. Este protocolo es un reemplazo para Address Resolution Protocol [20] (ARP) y de algunas funciones de ICMP. Provee un mecanismo de detección de direcciones duplicadas.
- **Path MTU Discovery:** cuando un nodo IPv6 tiene una gran cantidad de datos para enviar a otro nodo, los datos son transmitidos en una serie de paquetes IPv6. Es usualmente preferible que el tamaño de esos paquetes sea el máximo que pueda ser transmitido por un camino desde el origen al destino. El tamaño de ese paquete es referido como “Path MTU” (PMTU), y es igual al MTU del enlace de mínimo MTU entre el emisor y el destinatario. En [27] se define un mecanismo para que un nodo pueda descubrir el PMTU de un camino arbitrario.
- **MLD (Multicast Listener Discovery):** se encuentra definido en [28]. Especifica un protocolo usado por routers IPv6 para descubrir la presencia de nodos que desean recibir paquetes multicast sobre sus enlaces directamente conectados, y para descubrir específicamente cuales direcciones multicast son de interés a esos nodos vecinos. En su versión 2 [29] adiciona soporte para filtros de origen, habilidad de un nodo para reportar interés en escuchar paquetes sólo de direcciones de orígenes particulares, o de todos los orígenes excepto de direcciones de orígenes particulares.
- **DHCPv6 (Dynamic Host Configuration Protocol for IPv6):** DHCPv6 [30] es la nueva versión de DHCP [6]. DHCPv6 ha sido completamente rediseñado y sólo es conceptualmente similar a DHCP. Permite pasar parámetros de configuración tales como direcciones de red a nodos IPv6.
- **RIPng (RIP next generation):** El protocolo RIPng [31] es muy similar a RIPv2 [32] y ha sido adaptado para soportar los nuevos prefijos de IPv6. Por tal motivo RIPng es un protocolo de enrutamiento muy simple, ideal para redes IPv6 pequeñas o medianas.
- **OSPFv3 (OSPF para IPv6):** El protocolo OSPFv3 [33] es un protocolo de estado de enlace basado en OSPFv2 [34] con un conjunto de modificaciones realizadas para permitir intercambiar información de enrutamiento IPv6

3.1.7. Mecanismos de Transición a IPv6

La clave para una transición exitosa a IPv6 es la compatibilidad con la gran base de nodos IPv4 instalados. El mantenimiento de la compatibilidad con IPv4 mientras se despliega IPv6 ayudará en la tarea de transición a Internet sobre IPv6.

Existen tres mecanismos de transición disponibles para desplegar IPv6 sobre redes IPv4 (los dos primeros descritos en [35]), los cuales pueden ser utilizados en combinación.

Dual-Stack

Esta técnica permite a IPv4 e IPv6 coexistir en los mismos dispositivos y redes. Los nodos IPv6 que proveen completa implementación de IPv4 e IPv6 son llamados “nodos IPv6/IPv4”, y tienen la habilidad comunicarse directamente con nodos IPv4 usando paquetes IPv4, y con nodos IPv6 con paquetes IPv6.

Dependiendo con que nodo una aplicación esté comunicándose, utilizará IPv4 o IPv6 apropiadamente. El protocolo a utilizar puede ser determinado por la respuesta de un Servidor de Nombres de Dominio [36] [37] (DNS, por sus siglas en inglés) a una petición de resolución de un nombre y a un nuevo tipo de registro llamado “AAAA” definido para direcciones IPv6 [38].

Tunneling

Los mecanismos de túnel encapsulan paquetes IPv6 en paquetes IPv4 y pueden ser usados entre dos nodos IPv6 para comunicarse entre ellos a través de una red IPv4 en una variedad de formas:

- **Router a Router:** los routers IPv6/IPv4 interconectados por una infraestructura IPv4 pueden hacer un túnel de paquetes IPv6 entre ellos mismos.
- **Equipo a Router:** los equipos IPv6/IPv4 pueden hacer túnel de paquetes IPv6 hasta un router IPv6/IPv4 intermedio que es alcanzable por medio de una infraestructura IPv4.
- **Equipo a Equipo:** los equipos IPv6/IPv4 interconectados por una infraestructura IPv4 pueden hacer un túnel para los paquetes IPv6 entre ellos mismos.
- **Router a Equipo:** los routers IPv6/IPv4 pueden hacer túnel de paquetes IPv6 hasta su destino final, equipos IPv6/IPv4.

Existen dos vías para hacer túneles:

- **Configurado:** en este caso las direcciones IPv4 son especificadas en forma manual por el administrador. Permite establecer túneles punto-a-punto para encapsular paquetes IPv6 dentro de paquetes IPv4 y llevarlos sobre una infraestructura de enrutamiento IPv4 [35].
- **Automático:** en esta técnica la dirección en el punto de salida del túnel es determinada por la dirección destino “IPv6 IPv4-compatible” (definida en [76]) que esta pasando por el túnel. Esta técnica ya no se utiliza según [35], en su lugar se debe utilizar la técnica 6to4 definida en [39].

Translation

Los traductores utilizan mecanismos de traslación de direcciones y protocolos para ayudar a equipos IPv6 comunicarse con equipos IPv4, convirtiendo paquetes IPv6 en paquetes IPv4 y viceversa. No requieren que los nodos finales tengan soporte para IPv6 e IPv4 simultáneamente. NAT-PT [41] es un ejemplo de traductores.

3.2. Internet2 y el Proyecto Reacciun2

3.2.1. Internet2

Internet2 es un proyecto que agrupa un gran número de universidades y centros de investigación a nivel mundial, el objetivo principal es promover las tecnologías de redes de alta velocidad (tales como IPv6), que contribuyan al desarrollo de las aplicaciones con alta demanda de recursos tecnológicos, requeridas por el sector académico, científico y tecnológico en el ámbito de la cooperación nacional e internacional.

El eje de Internet2 es un consorcio formado por aproximadamente 200 universidades de EEUU con apoyo del gobierno y algunas de las empresas líderes del sector informático y de telecomunicaciones (IBM, Intel Corporation, Cisco Systems, AT&T, Microsoft, Juniper Networks, Lucent Technologies, Qwest Communications, Sun Microsystems, por ejemplo). A este eje se le han ido incorporado otras universidades, organizaciones no gubernamentales relacionadas con el trabajo de redes y corporaciones interesadas en participar en el proyecto. Los usuarios finales son grupos de investigadores en diversas partes del mundo que desarrollan servicios y aplicaciones que requieren acceso a redes de alta velocidad.

Internet2 es administrada por la University Corporation for Advanced Network Development (UCAID) y, entre otras características, opera sobre una de las redes de mayor velocidad en el mundo denominada Abilene, recientemente llevada a 10 Gbps.

Internet2 no pretende reemplazar al Internet actual, ni tampoco se ha propuesto como principal objetivo construir una infraestructura paralela. Los participantes tienen enlaces al Internet tradicional para servicios como la web, news, correo electrónico y similar. La meta del proyecto es unir a las instituciones académicas, científicas y tecnológicas nacionales y regionales con los recursos necesarios para desarrollar nuevas tecnologías y aplicaciones, que serán las utilizadas en el futuro Internet.

Objetivos Principales

Se pueden englobar los objetivos generales de Internet2 de la siguiente manera:

- Promover el desarrollo de redes de altas prestaciones (de altas velocidades, baja latencia, con enlaces de gran capacidad, calidad de servicio, seguridad, etc.) y ponerlas al servicio de la comunidad científica y de investigación.
- Facilitar el desarrollo de aplicaciones avanzadas con alta demanda de recursos.
- Asegurar la transferencia rápida de los nuevos servicios, tecnologías y aplicaciones a la comunidad Internet.

Principales Aplicaciones

Entre las aplicaciones más importantes que se pueden desarrollar en Internet2 se encuentran:

- Videoconferencia de alta velocidad.
- Telemedicina. La distribución de datos con garantía de calidad de servicio (QoS) y la transmisión de imágenes en alta resolución, pilares de la llamada medicina remota o telemedicina. Además, los resultados de búsquedas en grandes bases

de datos en línea permitirán a los médicos comparar imágenes, historiales y otras opiniones para hacer un diagnóstico altamente fiable.

- Computación en gran escala con procesos de bases de datos en múltiples sitios. Integración de diversos recursos de computación independientes, generalmente heterogéneos y distribuidos geográficamente (grids) a través de un middleware (software que traduce la información de una compañía a un formato entendible por otra empresa diferente), para brindar capacidad de cómputo y almacenamiento a gran escala, de forma transparente para el usuario.
- Ambientes de colaboración interactiva en los que se pueda intercambiar información con otros sin las barreras de las distancias (por ejemplo: investigación e instrucción interactiva basada en redes).
- Multicasting Routing: aplicaciones multimedia de gran ancho de banda. Multicasting es una tecnología IP que permite a los usuarios compartir video, audio y data a través de Internet de manera eficiente. Utiliza una suite de protocolos que hacen que los paquetes viajen a través de la red hasta múltiples receptores. Transferencia de archivos en el orden de los terabytes (1024 GB = 1 TB).
- Tele-inmersión, la cual permite a participantes geográficamente distantes compartir un entorno virtual que recrea su ambiente real, e interactuar en tiempo real. La tele-inmersión tiene gran aplicación en entornos académicos y científicos pues permite el trabajo en grupos.
- Aplicaciones que requieran comunicación a muy alta velocidad entre computadores, con garantía de calidad de servicio (Quality of Service - QoS).
- Aplicaciones que requieran interacción hombre-computadora en tiempo real.
- Modelos en tiempo real basados en sensores.
- Acceso a recursos remotos, como telescopios o microscopios.
- Transmisión de imágenes de alta resolución.
- Laboratorios virtuales.
- Bibliotecas digitales.

Consorcio de Redes

Los consorcios de redes son asociaciones de dos o más compañías, organizaciones o gobiernos (o cualquier combinación de esas entidades) cuyo objetivo es administrar y dar los lineamientos para el uso de la redes de alto desempeño. Entre las más importantes se encuentran:

- **APAN[3] (Asia-Pacific Advanced Network):** Es un consorcio internacional, sin fines de lucro, establecido el 3 de Junio de 1997. APAN conforma una red de alto rendimiento para la investigación y el desarrollo en aplicaciones y servicios avanzados, que enlaza a varios de los países de la región asiática. Los miembros primarios son: Australia, Japón, Corea, Singapur y USA (Universidad de Indiana), los miembros asociados: Malasia y China.
- **CANARIE[4] (Canada Advanced Internet Developments):** Es la organización canadiense para el desarrollo de Internet avanzada. Fue establecida en 1993 y ha trabajado con el gobierno, la industria y las comunidades de investigación y

[3] http://www.apan.net
[4] http://www.canarie.ca

educación para realzar la infraestructura canadiense de Internet, el desarrollo de aplicaciones y su uso. Es una organización privada, sin fines de lucro, apoyada por la industria de Canadá.

- **CLARA[5] (Cooperación LatinoAmericana de Redes Avanzadas):** Es una asociación sin fines de lucro registrada en Montevideo, Uruguay. Fue creada por 14 Redes Nacionales de Investigación y Educación Latinoamericanas.
- **DANTE[6] (Delivery of Advanced Network Technology to Europa):** DANTE, es una organización inglesa establecida en Cambridge con el fin de gestionar los servicios de redes avanzadas para la comunidad investigadora y académica europea, es el coordinador del consorcio GÉANT y responsable de su creación.
- **NSF[7] (National Science Foundation):** La National Science Foundation (NSF) es una agencia independiente del gobierno de los Estados Unidos para promover el progreso de la Ciencia, para el avance de la salud, la prosperidad y el bienestar de la Nación y para asegurar la defensa nacional.
- **UCAID[8] (University Corporation for Advanced Internet Development):** Tiene como misión facilitar y coordinar el desarrollo, despliegue, operación y transferencia de tecnología de redes basadas en aplicaciones y servicios avanzados, para fomentar el liderazgo de los Estados Unidos en la investigación y educación superior, así como para acelerar la disponibilidad de nuevos servicios y aplicaciones en Internet. Actualmente está constituida por más de 200 universidades miembros. UCAID es la organización que coordina el proyecto Internet2.

Principales Redes Actuales

Las redes de alto desempeño proveen la infraestructura para desarrollar los proyectos definidos por los consorcios de redes, existen distintas redes por todo el mundo tales como:

- **Abilene[9] (Abilene Backbone Network):** Abilene es un backbone con tecnología avanzada que es el soporte para el desarrollo y expansión de las nuevas aplicaciones que se desarrollan dentro de la comunidad de Internet2. La red de Abilene se ha desarrollado en sociedad con Internet2, Qwest Comunications, Cisco Systems, Nortel Network y la Universidad de Indiana. La red experimentó una mejora de 2.5 Gbps a 10 Gbps a finales del año 2003.
- **AmericasPATH[10] (AMPATH):** La red de AmericasPATH (AMPATH) es un proyecto de FIU (Florida International University*)* en colaboración con Global Crossing (GC). Utilizando la red terrestre y de fibra óptica submarina de GC, AMPATH interconecta las redes de educación e investigación de América de Sur y Central, el Caribe y México a las redes de investigación y educación de los EEUU y fuera de los EEUU vía la red Abilene de Internet2.
- **Multi-Gigabit Pan-European Research Network[11] (GÉANT):** GÉANT es un proyecto de colaboración entre 26 redes nacionales de educación e

[5] http://www.redclara.net
[6] http://www.dante.net
[7] http://www.nfs.gov
[8] http://www.ucaid.edu
[9] http://abilene.internet2.edu
[10] http://www.ampath.net
[11] http://www.geant.net

investigación, que representan a 30 países en Europa. Su principal propósito ha sido el desarrollo de una red multi-gigabit de comunicación de datos paneuropea reservada específicamente para uso de la investigación y la educación. GÉANT proporciona la capacidad más alta y ofrece la cobertura geográfica más grande de cualquier red de su clase en el mundo.

- **Very High Performance Backbone Network Service[12] (vBNS):** vBNS es una red de la NSF (National Science Foundation, USA) que soporta aplicaciones de alto rendimiento y gran ancho de banda. La red comenzó a operar con enlaces de 622 Mbps con la meta de llegar a 2.4 Gbps para el año 2004. Se espera que la red vBNS sea capaz de soportar más información y de forma más rápida que las redes de telecomunicaciones comerciales actualmente disponibles.

3.2.2. Proyecto Reacciun2

El proyecto de Internet2 iniciada por Centro Nacional de Tecnologías de Información (CNTI) y ahora en manos del Centro Nacional de Innovación Tecnológica (CENIT), denominado Reacciun2 (Red Académica de Centros de Investigación y Universidades Nacionales de Alta Velocidad), interconecta a 10 universidades nacionales y a un centro de investigación, con las redes internacionales experimentales de Internet de alta velocidad (Internet2). También incluye la instalación, de 2 laboratorios para la capacitación e investigación en la tecnología de Internet2, con el objeto de incentivar la formación del talento humano (investigadores, docentes y estudiantes) en el desarrollo e investigación de las telecomunicaciones.

El proyecto Reacciun2 fue suscrito al proyecto AMPATH de la Universidad Internacional de Florida (FIU) en abril de 2003 y se instaló un enlace de 45 Mbps (DS3) con la empresa Global Crossing, de los cuales se utilizan 15 Mbps para el Internet comercial y 30 Mbps están en reserva para ser utilizados en el proyecto de Internet2. En la actualidad ya existe conectividad de la red Reacciun2 con la red principal de Internet2 en América (Abilene) a través de la Universidad Internacional de Florida.

Con relación a la organización del Proyecto Reacciun2, se realizaron varias reuniones del Comité Educativo del CNTI que trataron el tema de Internet2; se iniciaron mesas de trabajo con proveedores de esta tecnología para la adquisición de equipos del proyecto y se capacitó personal en la tecnología de IPv6 y Multicasting. También se adelantó gestiones para que Reacciun2 sea incorporada a la red del proyecto CLARA, que tiene como finalidad interconectar las redes académicas, científicas y de investigación de los países de Latinoamérica y el Caribe con el backbone europeo de alta velocidad GÉANT.

Beneficios del Proyecto Reacciun2

La consolidación de Reacciun2 y de la infraestructura de las redes de alta velocidad provee innumerables beneficios dentro de los cuales se encuentran:

- Permitir el trabajo en colaboración a través de la integración de esfuerzos en los ámbitos académicos, científicos y tecnológicos a nivel mundial.
- Formar un equipo humano que recibirá transferencia tecnológica y capacitación.

[12] http://www.vbns.net

- Permitir a la comunidad académica, científica y tecnológica el desarrollo de nuevas aplicaciones que no son posibles con el Internet actual.
- Disponer de equipamiento tecnológico de última generación para acceso a Internet2.
- Permitir a las instituciones participantes tener acceso a los recursos más avanzados en el campo de las telecomunicaciones.
- Disponer de la infraestructura tecnológica y de contenidos necesaria para la capacitación de Internet2, en los laboratorios de docencia de las instituciones académicas que participen en el proyecto.
- Ampliar los servicios para cubrir el área de Internet2 con personal capacitado que permita dar soporte técnico y asegurar un eficiente servicio a la plataforma instalada.
- Capacitar docentes e investigadores en el área de Internet2.
- Propagar la enseñanza de esta nueva tecnología a través de ofertas de cursos de capacitación.

Fases del Proyecto

La ejecución del proyecto se estimó para dieciocho (18) meses a partir del año 2003, lapso durante el cual se realizaron 6 fases descritas a continuación:

Fase I: Investigación Base

- Promoción del proyecto en instituciones educativas, científicas y tecnológicas a nivel nacional. Preselección de las instituciones más adecuadas para participar en el proyecto.
- Obtención de información de las aplicaciones que están en desarrollo o a ser desarrolladas por las instituciones preseleccionadas, que sean de alto impacto académico-científico, que requieran de intercambio de información tanto a nivel nacional como internacional y que demanden altos recursos tecnológicos.
- Levantamiento de información de los laboratorios para capacitación existentes en las instituciones miembros de la red Reacciun.
- Levantamiento de información de inventario de hardware y software existentes en las instituciones preseleccionadas para participar en el proyecto.
- Identificación y análisis de los requerimientos de las instituciones para el desarrollo de las aplicaciones, con el objeto de realizar el estudio de la solución a ser aplicada en cada uno de los laboratorios.
- Selección de las instituciones a participar en el Proyecto, en las cuales se instalaron los equipos y se activaron la conexión a Internet2, y de las instituciones académicas en las cuales se instalaron los equipos para las actividades de docencia en la tecnología asociada a Internet2.

Fase II: Diseño Tecnológico

- Se solicitó asesoría a los principales proveedores de tecnología, tanto de hardware como de software, nacionales e internacionales, en cuanto a la mejor solución técnica del equipamiento, conectividad y aplicaciones requeridas para el diseño de los centros de investigación a ser desarrollados en las instituciones

participantes. Se definió las especificaciones técnicas de los componentes a instalar para las actividades de docencia en los laboratorios destinados a tal fin.
- Se realizó el diseño topológico de interconexión de las redes internas de los centros de investigación ubicados en cada una de las instituciones participantes así como la conexión con el proyecto mundial de Internet2.

Fase III: Implantación

- Se procedió con la suscripción de la red Reacciun al proyecto AmericanPath (AMPATH) a fin de obtener el acceso al proyecto de la Universidad Internacional de la Florida (FIU) y la integración con la red Internet2.
- Se adquirió y adecuó los equipos y componentes de los centros de investigación en las instituciones participantes.
- Se adquirió y adecuó los equipos y componentes de la plataforma de la Red Académica Nacional (Reacciun).
- Se contrató e instaló los enlaces requeridos para la interconexión entre los centros de investigación y la Red Académica contra Internet2.
- Se instaló los equipos para capacitación en Internet2, en los laboratorios seleccionados.

Fase IV: Capacitación y Control

- Se realizó la capacitación del recurso humano en cada institución participante y la transferencia tecnológica requerida para asegurar la adecuada operación de los servicios.
- Se definió, diseñó e implementó los mecanismos de monitoreo y control de la plataforma a instalada.
- Se procedió a capacitar al personal docente que encargado de dictar los cursos en dicha tecnología.

Fase V: Promoción y Divulgación

- Se definió los mecanismos de difusión y propagación de la información correspondiente al proyecto, abarcando la promoción del mismo en sus inicios y la divulgación de los resultados obtenidos con la finalización del proyecto.

Fase VI: Evaluación Ex-post

- Se realizó la auditoria externa financiera y técnica del proyecto con el objeto de evaluar los resultados obtenidos versus los resultados esperados, así como el impacto del proyecto.

Diseño de la Red Reacciun2

Se seleccionó ocho (8) universidades para formar parte de la primera etapa de la red de Reacciun2: ULA, UCV, IVIC, UC, UCLA, USB, UDO y UPEL. Posteriormente, la UBV, UNEFA y LUZ se incorporaron al proyecto. Se analizó la mejor manera de interconectar a las universidades con el CNTI y se decidió implementar una topología en estrella, con

el CNTI como centro. Esto implicó la adquisición de nueve routers, uno para cada institución y uno para el CNTI. Los routers se seleccionaron de la marca Cisco, por varias razones. Primero, es una marca cuya representación en Venezuela garantiza un mantenimiento oportuno y eficaz. Segundo, ya existe una infraestructura en el CNTI para el entrenamiento en equipos Cisco, con lo cual se facilita la preparación de personal para este tipo de equipos, y finalmente, porque la gran mayoría de la infraestructura existente en las instituciones es de esta marca, lo que facilita la interconexión y mantiene homogeneidad dentro de la red.

De acuerdo al diseño que se ha planteado (ver Figura 3-19, tomada de Reacciun2[13]), cada universidad se interconecta hoy en día con el CENIT a través de una transportista. El enlace desde cada institución hasta la nube ATM de la transportista tiene una velocidad de 34 Mbps, excepto el de la UNEFA y UBV, que tienen 8 Mbps cada una. Desde la nube hasta el CENIT existen dos (2) enlaces de 155 Mbps.

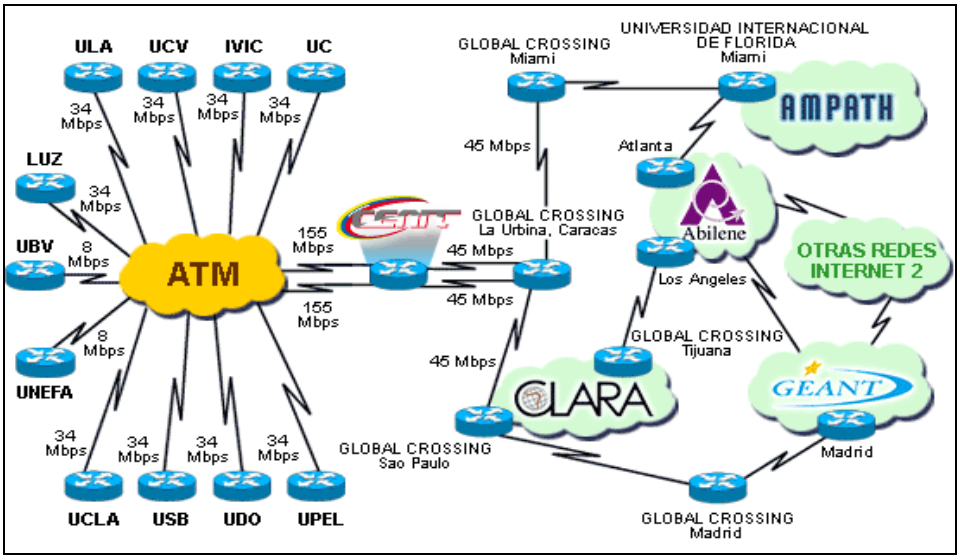

Figura 3-19: Topología de la Red.

Plan de Direccionamiento

El 13 de noviembre de 2004, LACNIC adjudica un bloque /32 de direcciones IPv6 (2001:1338::/32) a CNTI/Reacciun, siendo el primero en asignarse a Venezuela y el primero en otorgarse a un ccTLD (Country-Code Top-Level Domain) en Latinoamérica y el Caribe.

Entre los objetivos planteados por CNTI para implantar el plan de direccionamiento se encontraban:

- Cumplir con los requerimientos de LACNIC.
- Proveer un esquema de direccionamiento amigable, flexible, seguro y perdurable.
- Alentar el uso de IPv6.

[13] http://www.reacciun2.edu.ve/view/fase2.php

Todo esto soportado técnicamente por RFCs, políticas globales de asignación, etc.

Una de las primeras decisiones con respecto a las asignaciones fue que se regularían de la siguiente manera:

- /48 a nodos de la red académica.
- /48 ó /64 a otras entidades relevantes.
- El bloque 0x0000 y 0x0001 es asignado a CNTI.
- El bloque 0xFFFF y 0xFFFE es reservado para conexiones punto-a-punto.

3.3. Multicast sobre IPv4

Un extremo del espectro de comunicaciones IPv4 es la comunicación unicast, en donde una IP origen de un equipo envía paquetes a una IP destino de otro equipo. En este caso, la dirección destino en el paquete IP es una dirección única de un equipo en la red. Estos paquetes IP son enviados a través de la red desde el equipo origen hasta el equipo destino por medio de los routers. Los routers en cada punto a lo largo del camino entre el origen y el destino usan su Base de Información de Enrutamiento (RIB, por sus siglas en inglés) para tomar decisiones de envío unicast basados en la dirección IP destino del paquete.

En el otro extremo del espectro de comunicaciones IPv4 está el broadcast, en donde un equipo origen envía paquetes a todos los equipos en un segmento de red. La dirección destino de un paquete IP broadcast tiene la porción que identifica al equipo destino establecida todas a uno y la porción que identifica a la red a la dirección de la subred destino (ver Figura 3-20 tomada de [79]).

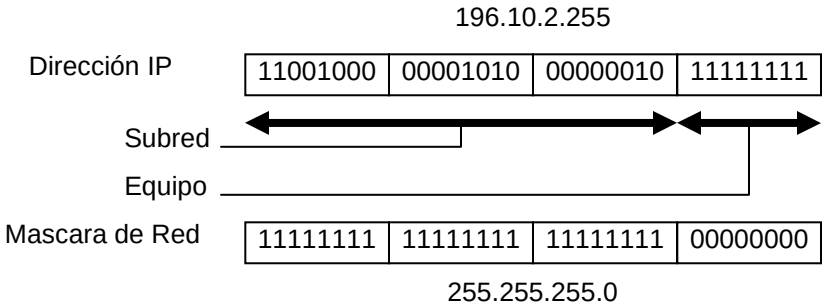

Figura 3-20: Dirección IP Broadcast.

Los equipos (incluyendo los routers) entienden que los paquetes, los cuales contienen una dirección broadcast en la dirección destino, son dirigidos a todos los equipos IP de la subred. Los router, a menos que se indique lo contrario, no envían paquetes IP broadcast, por lo tanto, la comunicación IP broadcast es normalmente limitada a la subred local.

La Figura 3-21, tomada de [79], describe lo anteriormente expuesto, donde el equipo A envía un broadcast a la subred 198.1.1.0/24. Debido a que el equipo B y equipo C están en la misma subred, ellos reciben el broadcast. El equipo D, sin embargo, está en una subred distinta (198.1.2.0/24) y no recibe el broadcast debido a que el router no lo envía.

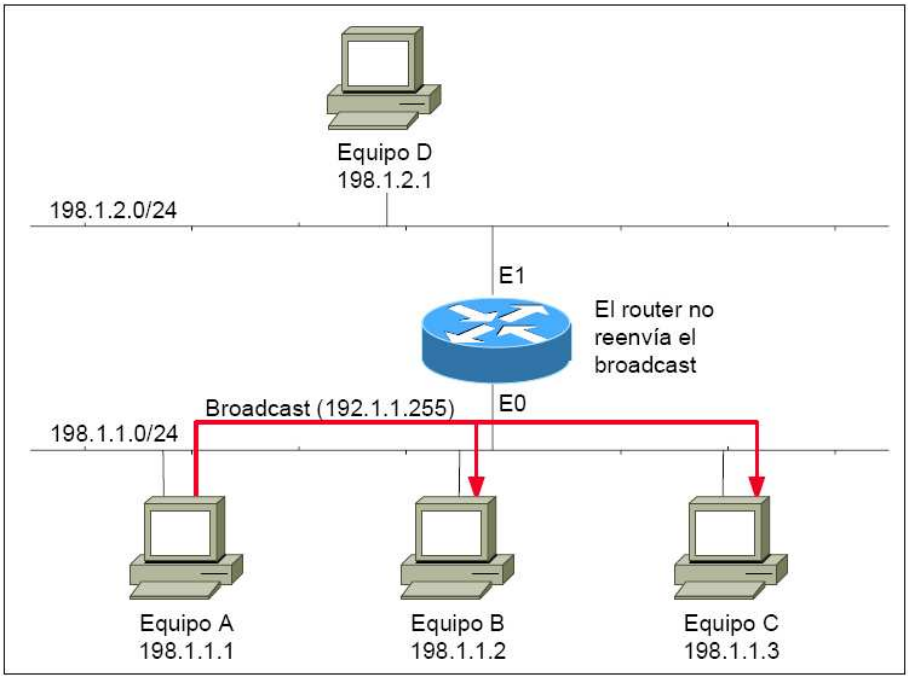

Figura 3-21: Broadcasts Filtrados por los Routers.

Por último, entre las comunicaciones unicast y broadcast se encuentra la comunicación multicast, que permiten a un equipo enviar paquetes IP a un grupo de equipos en cualquier parte dentro de una red IP. Para hacer esto, la dirección destino en un paquete IP multicast es una forma especial de dirección IP llamada “dirección IP de grupo multicast”. Los routers deben enviar los paquetes IP multicast entrantes hacia todas las interfaces que alcancen a miembros de un grupo multicast (Figura 3-22 tomada de [79]).

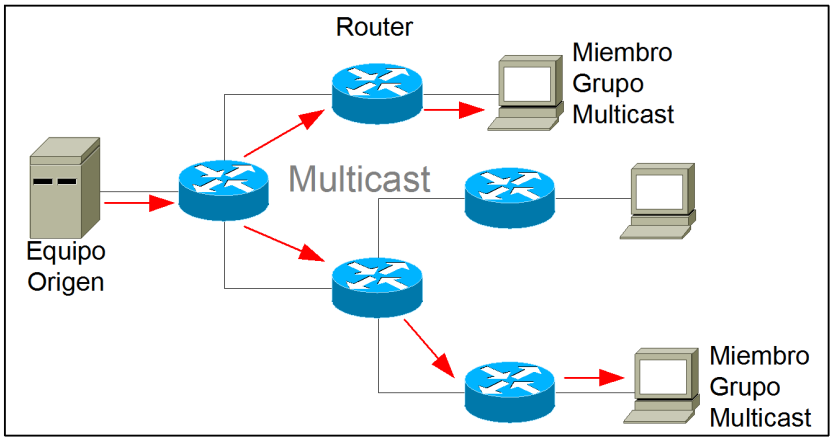

Figura 3-22: Envío de Paquetes Multicast.

Multicast, originalmente definida en [43], provee un mecanismo eficiente para la entrega de tráfico que puede ser caracterizado como de “uno a muchos” o “muchos a muchos”. La radio y la televisión son ejemplos de tráficos que encajan en el modelo “uno a muchos”.

Con unicast, una estación de radio debería establecer una sesión separada con cada usuario interesado en la transmisión. La carga de procesamiento y la cantidad de ancho de banda consumido por la transmisión, incrementa linealmente con la cantidad de usuarios sintonizando la estación. Este esquema podría trabajar bien con unos cuantos usuarios, sin embargo, con cientos o miles de usuarios este método podría ser extremadamente ineficiente.

Utilizando broadcast, la estación de radio podría transmitir sólo un flujo de paquetes, así esté destinando para un usuario o para miles de usuarios. La red podría replicar este flujo y entregarlo a cada usuario. Desafortunadamente, los usuarios no interesados en escuchar la radio también podrían recibir este flujo de paquetes. Este método es ineficiente cuando existen muchos usuarios que no desean escuchar la estación de radio, ya que ese flujo no deseado impacta en los recursos de la red a los cuales está conectado.

Multicast permite a la estación de radio transmitir un solo flujo que encuentre un camino para cada usuario interesado. Como en el caso del broadcast, la carga de procesamiento y el ancho de banda consumido permanecen constantes sin importar el tamaño de la audiencia. La red es la responsable de la replicación de los datos y la entrega sólo a los usuarios que deseen escuchar la estación de radio. Los enlaces de los usuarios que no desean escuchar la estación no se sobrecargan con este tráfico, ya que este fluye únicamente hacia los enlaces conectados a los equipos de los usuarios que desean recibir los datos.

Características de Multicast

Como se mencionó anteriormente, una de los beneficios más obvios de esta tecnología es la preservación del ancho de banda, ya que envía un sólo flujo de datos a un grupo de clientes en vez de enviarlos a todos o tener múltiples flujos de datos a la vez. Las características más relevantes de multicast son:

- Facilita la transmisión de un datagrama IP a un grupo multicast conformado de cero o más equipos identificados por una sola dirección IP destino.
- Envía un datagrama multicast a todos los miembros de un grupo multicast con la misma confiabilidad de “mejor esfuerzo” que los datagrama IP unicast regulares.
- Soporta la asociación dinámica de un grupo multicast.
- Soporta todos los grupos multicast sin importar la ubicación o número de miembros.
- Soporta la asociación de un sólo equipo en uno o varios grupos multicast.
- Mantiene múltiples flujos de datos a nivel de aplicación para una sola dirección de grupo.
- Soporta una sola dirección de grupo para múltiples aplicaciones en un equipo.
- Multicast es anónimo, dado que un servidor transmite a una dirección de grupo multicast (que representa a un grupo de receptores), éste nunca sabe la dirección unicast de ninguno de los receptores.
- El tráfico multicast es manejado en la capa de transporte usando el Protocolo de Datagrama de Usuario (User Datagram Protocol, UDP, definido en [44]). Debido a la simplicidad de UDP, los encabezados de los paquetes de datos contiene

pocos bytes y consumen menos recursos de red que el Protocolo de Control de Transmisión (Transmission Control Protocol, TCP, definido en [45]).

Ventajas

Tanto Internet como las intranets corporativas han crecido en términos de números de usuarios conectados, y frecuentemente una gran cantidad de ellos desean acceder a la misma información en un mismo tiempo. Al utilizase las técnicas de multicast para distribuir la información se puede reducir substancialmente el ancho de banda demandado sobre una red (Figura 3-23 tomada [79]).

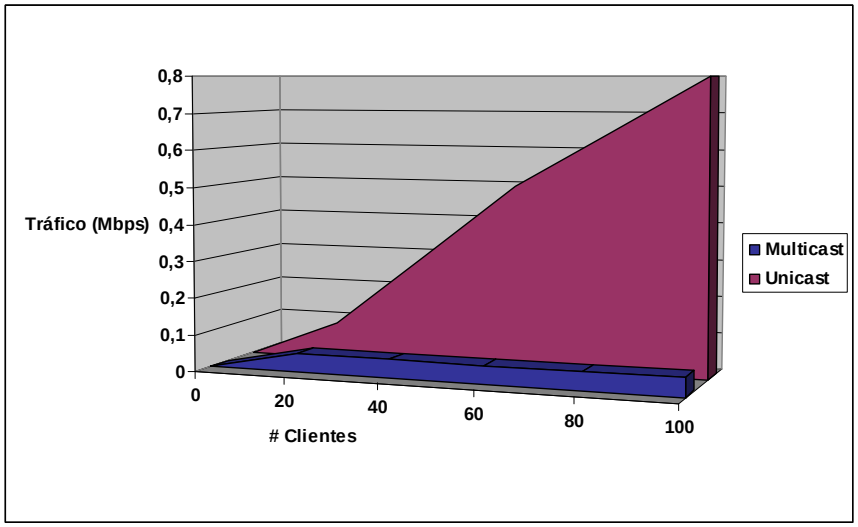

Figura 3-23: Unicast vs. Multicast para audio.

A continuación presentamos algunas ventajas de esta tecnología:

- **Eficiencia aumentada:** el ancho de banda disponible es utilizada más eficientemente debido a que múltiples flujos de datos son reemplazados con una sola transmisión, esto aumenta el control en el tráfico de la red y reduce la necesidad de servidores y carga de procesamiento.
- **Rendimiento optimizado:** se elimina el tráfico redundante, por lo que menos copias de datos se requieren enviar y procesar (Figura 3-24 tomada de [79]).
- **Aplicaciones distribuidas:** hace posible las aplicaciones multipuntos.

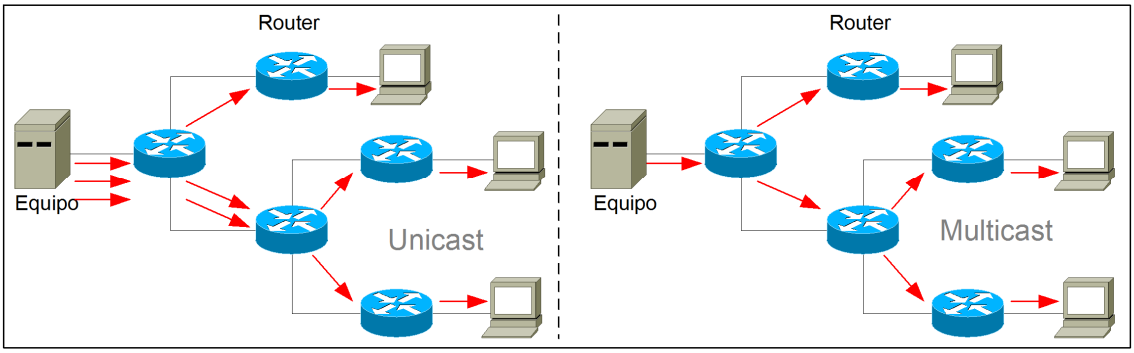

Figura 3-24: Tráfico Unicast vs. Multicast.

Desventajas

Aunque existen un buen número de razones para desear usar IP multicast en una red, se necesita considerar que hay limitaciones y desventajas para esta tecnología, asociado principalmente a que multicast está basado en UDP. Algunas de ellas se mencionan a continuación:

- **Entrega con el mejor esfuerzo:** esto resulta en pérdidas ocasionales de paquetes. Muchas aplicaciones multicast que operan en tiempo real pueden ser impactadas por estas perdidas. Es por ello, que una aplicación que usa IP multicast debe esperar ocasionalmente perdida de paquetes y estar preparado para aceptarlas, o manejarla de alguna manera en la capa de aplicación o vía un protocolo multicast confiable por encima de UDP.
- **Congestión de red:** en el caso de paquetes unicast TCP, el mecanismo estándar de manejo de ventanas automáticamente ajusta la velocidad de la transferencia de datos, de esta forma se provee un grado de control de congestión en la red. Debido a que IP multicast no usa TCP, no hay un mecanismo de control de congestión para prevenir a un enlace cuyo ancho de banda es bajo u otro recurso crítico de enrutamiento de la red de un flujo multicast.
- **Duplicidad:** La duplicación de paquetes, en el mundo unicast UDP, es un hecho normal. Sin embargo, una diferencia clave entre el enrutamiento unicast y multicast es que, en este último, los routers intencionalmente envían copias de paquetes multicast a las múltiples interfaces. Esto incrementa la probabilidad de que múltiples copias de paquete multicast puedan llegar al receptor. Una vez más, una aplicación multicast bien diseñada debería estar preparada para detectar y manejar el arribo ocasional de paquetes duplicados.
- **Paquetes fuera de secuencia:** varios eventos en la red pueden ocasionar el arribo de paquetes fuera de secuencia. Las aplicaciones multicast deben diseñarse para manejar estos eventos.

Aplicaciones Multicast

Aunque la primera aplicación a ser usada sobre una red habilitada para tráfico IP multicast es frecuentemente la videoconferencia, ésta es una de las muchas aplicaciones IP multicast que puede agregar valor al modelo de negocios de cualquier organización. A continuación mencionamos algunas otras:

- **Conferencias multimedia:** muchas personas empiezan con conferencias de audio/video debido a que el video es la forma de comunicación más excitante sobre la red. Pero las conferencias de audio acompañadas de una aplicación basada en IP multicast, tal como una aplicación de datos compartidos (pizarra digital) que permita a los miembros de la conferencia compartir información gráfica, serán mucho más utilizadas de manera rutinaria.
- **Distribución de datos:** La replicación de datos es una área de aplicaciones IP multicast que rápidamente se está haciendo muy popular. Usando multicast, se puede adoptar un nuevo modelo de actualización de archivos y base de datos.
- **Datos multicast en tiempo real:** La entrega de datos en tiempo real a un gran grupo de estaciones es otra área donde IP multicast es muy popular. La entrega

de datos financieros, pizarrones compartidos y herramientas de colaboración son aplicaciones típicas en tiempo real.

- **Juegos y simulación:** IP multicast estaría muy bien situado para usarse en redes de juegos o aplicaciones de simulación. Ya que, aunque numerosos juegos de PC y simulaciones permiten grupos de redes de jugadores para batallas unos contra otros en peleas simuladas en entornos de fantasías, virtualmente todas esas aplicaciones hacen uso de unicast (conexiones punto-a-punto).

3.3.1. Grupos Multicast

Multicast está basado en el concepto de grupo, en donde un conjunto de clientes expresan interés en recibir un flujo de datos en particular. Los clientes pueden estar ubicados en cualquier parte de Internet por lo que no tienen ningún tipo de límites físicos o geográficos. Los clientes que están interesados en recibir un flujo de datos para un cierto grupo deben unirse a dicho grupo.

Direcciones IP Multicast

Las direcciones multicast definen a un grupo arbitrario de equipos IP que pertenecen a un grupo y desean recibir el tráfico enviado a él. Las direcciones IP multicast usan el rango de direcciones de la clase D asignado por la "Internet Assigned Numbers Authority" (IANA) como se puede ver en [46]. Las direcciones en este espacio consisten de un prefijo binario 1110 en los primeros cuatro (4) bits del primer octeto, seguido por una dirección de grupo de 28 bits (Figura 3-25 tomada de [80]). El rango de direcciones para la clase D va desde la dirección 224.0.0.0 hasta la 239.255.255.255.

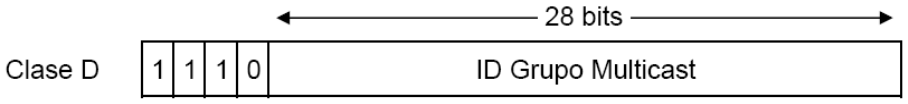

Figura 3-25: Estructura de una Dirección IP Clase D.

Las direcciones multicast pueden ser asignadas dinámica o estáticamente. El direccionamiento multicast dinámico provee aplicaciones con una dirección multicast a demanda, debido a que estas direcciones tienen un tiempo de vida específico, las aplicaciones deben requerir este tipo de direcciones sólo por el tiempo necesario. Las direcciones asignadas estáticamente son reservadas, por la IANA, para protocolos específicos que requieren direcciones bien conocidas.

En forma distinta a la asignación de direcciones unicast, donde los bloques son delegados a registros regionales, las direcciones multicast son asignadas directamente por la IANA. Una guía de asignación de direcciones multicast se encuentra definida en [77]. Entre las más resaltantes se encuentran:

- *Local Network Control Block:* La IANA ha reservado las direcciones en el rango desde la IP 224.0.0.0 hasta la 224.0.0.255 para ser usado por protocolos de red en un segmento de red local. Los paquetes con esas direcciones no deben ser enviados por los router, deben permanecer en el segmento LAN, por esto siempre son transmitidos con un TTL (Time To Live) igual a 1. En la Tabla 3-2 (tomada de [77]) se muestran algunos ejemplos de este tipo de direcciones.

Dirección	Uso
224.0.0.1	Todos los sistemas en una subred
224.0.0.2	Todos los routers en una subred
224.0.0.5	Routers OSPF

Tabla 3-2: Algunas Direcciones Multicast "Local Network Control Block".

- *Internetwork Control Block:* El rango de direcciones desde 224.0.1.0 hasta 224.0.1.255 son llamadas direcciones de alcance global. Estas pueden ser usadas para tráfico multicast entre organizaciones y a través de Internet. La Tabla 2-2 (tomada de [71]) lista algunas de ellas.

Dirección	Uso
224.0.1.1	Network Time Protocol (NTP)
224.0.1.24	Microsoft-ds
224.0.1.75	SIP

Tabla 3-3: Algunas Direcciones Multicast "Internetwork Control Block".

- *Administratively Scoped Block:* El rango de direcciones desde 239.0.0.0 hasta la 239.255.255.255 contiene direcciones de alcance limitado o administrativo. Fueron definidas en [47] para limitarlas a un grupo u organización local. Los routers son típicamente configurados con filtros para prevenir tráfico multicast en este rango de direcciones desde un flujo externo a un sistema autónomo (AS) o cualquier dominio definido por el usuario.

- *Block GLOP:* En [48] se propone que el rango de direcciones 233.0.0.0/8, denominado GLOP (no es un acrónimo), sea reservado para direcciones definidas estáticamente para organizaciones que ya tienen un número de AS reservado. El número de AS del dominio es insertado en los bytes segundo y tercero de las direcciones del rango 233.0.0.0/8.

3.3.2. Direcciones Multicast en Capa 2

Normalmente, las tarjetas de interfaz de red (NICs, por sus siglas en inglés) en un segmento de LAN reciben sólo los paquetes destinados a su dirección MAC (Media Access Control) o a la dirección MAC de broadcast. De esta manera, para manejar el tráfico multicast, se debió idear alguna forma de que múltiples equipos puedan recibir los mismos paquetes y aun ser capaces de diferenciar entre grupos multicast.

La IEEE tomó previsiones para la transmisión de paquetes broadcast y/o multicast en el estándar 802.3; en la dirección MAC el último bit del primer byte es usado para indicar si una trama es broadcast o multicast (Figura 3-26 tomada de [79]).

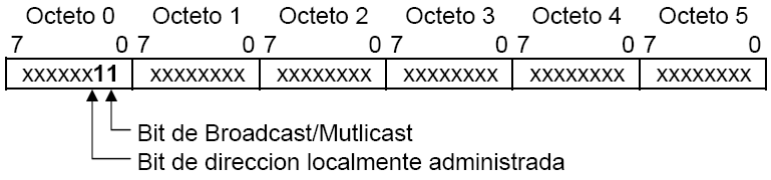

Figura 3-26: Formato de una Dirección MAC IEEE 802.3.

Si este bit es igual a uno (1) indica que la trama va dirigida a un grupo de equipos o a todos los equipos de la red (en el caso de la dirección de broadcast 0xFFFF.FFFF.FFFF). IP multicast hace uso de esta característica para enviar paquetes IP a un grupo de equipos en un segmento LAN.

Asignación de Direcciones IP Multicast a Direcciones Ethernet

LA IANA asignó el rango de direcciones desde 01:00:5e:00:00:00 hasta 01:00:5e:7f:ff:ff para ser usado con IP multicast. El prefijo 01:00:5e identifica a una trama como multicast, el siguiente bit de este prefijo siempre es cero (0), dejando sólo 23 bits para las direcciones IP multicast.

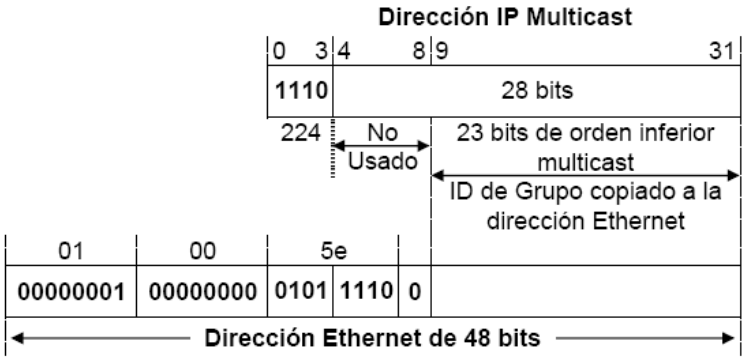

Figura 3-27: Asignación de IP Multicast a Ethernet.

Como todas las direcciones IP multicast tienen los primeros 4 bits en 1110, se toman los últimos 28 bits de la dirección IP para ser asignados a los últimos 23 bits de dirección Ethernet (Figura 3-27 tomada de [80]).

Debido a que los 28 bits de la dirección IP multicast no pueden ser asignados en un espacio de direcciones Ethernet de 23 bits, 5 bits de información se pierden durante este proceso. Esto genera una ambigüedad, en donde cada dirección MAC multicast puede representar a 32 direcciones IP multicast como se observa en la Figura 3-28 (tomada de [80]).

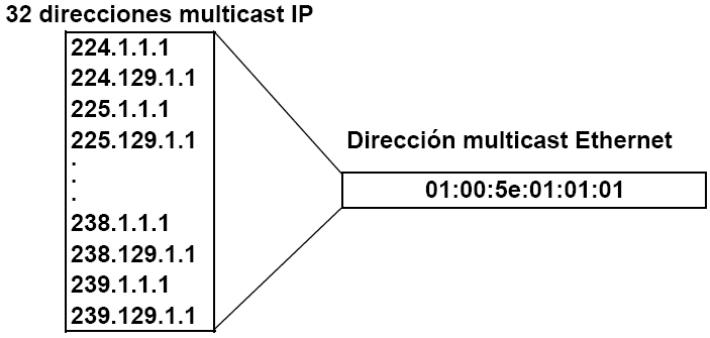

Figura 3-28: Ambigüedad de Direcciones MAC.

Existen mecanismos similares para la asignación de direcciones IP multicast tanto para Token Ring [49] como para FDDI [50] definidos en [51] y [52] respectivamente.

3.3.3. Administración del Tráfico Multicast

El concepto del envío de paquetes multicast dentro de un simple dominio de broadcast es de alguna forma un proceso trivial. Sin embargo, cuando se extiende esto a múltiples segmentos dentro de entorno más amplio, con varios switches y routers, se puede complicar el proceso significativamente.

El proceso de envío especifica una dirección destino como una dirección multicast. El manejador del dispositivo en el servidor origen convierte esta dirección a la correspondiente dirección Ethernet y envía el paquete hacia la red. Los dispositivos receptores, o clientes, deben indicar que ellos desean recibir datagramas destinados a una dirección multicast dada. Las complicaciones se presentan cuando multicast se extiende más allá de una sola interfaz de red y los paquetes deben pasar a través de varios routers.

Antes de que un tráfico multicast pueda atravesar la red, los routers necesitan saber cuales clientes, si existen, en una red específica pertenecen a un grupo multicast. Debido a que los nuevos modelos de redes están comprendidos por routers y switches, estos últimos también necesitan conocer como dirigir tráfico multicast.

Suscripción y Mantenimiento de Grupos Multicast

Internet Group Management Protocol (IGMP) provee una manera de reportar, a los routers multicast vecinos, la asociación de un cliente a un grupo multicast. IGMP administra el tráfico multicast a través de la redes por medio del uso de equipos y dispositivos de red (generalmente routers) multicast especiales. Los equipos manifiestan la asociación a un grupo enviando mensajes IGMP a sus routers multicast locales. Los routers escuchan esos mensajes IGMP y periódicamente envían consultas para descubrir cuales grupos están activos o inactivos en una subred en particular.

En términos generales, IGMP soporta dos estructuras de mensajes específicos:

- Mensajes de Consulta: son usados para descubrir cuales dispositivos de red son miembros de un grupo multicast dado.
- Mensajes de Reporte: son usados por los equipos en respuesta a mensajes de consulta para informar a los routers multicast de un equipo miembro.

La primera versión de IGMP (IGMPv1) se definió en [43], tenia dos tipos de mensajes:

- Host Membership Query.
- Host Membership Report.

De acuerdo a la especificación, un router multicast por LAN debe periódicamente transmitir mensajes “Host Membership Query” para verificar que al menos un equipo en la subred este interesado en recibir tráfico dirigido a un grupo multicast. Este mensaje es dirigido a la dirección IP 224.0.0.1 que es el grupo multicast de “todos los sistemas en una subred” (ver Tabla 3-2) con un TTL igual a uno.

Cuando la estación final recibe un mensaje IGMPv1 “Host Membership Query”, ésta responde al router multicast con un mensaje “Host Membership Report” indicando el

grupo al cual pertenece, uno por cada grupo al que es miembro. Si un router multicast no recibe respuesta después de varios mensajes de “Host Membership Query” para un grupo multicast, éste asume que el grupo no tiene miembros y deja de enviar tráfico para ese grupo.

La segunda versión de IGMP (IGMPv2) está definida en [53], y contiene los siguientes mensajes:

- Membership Query.
- Version 2 Membership Report.
- Leave Group.
- Version 1 Membership Report.

Esta versión elimina algunas limitaciones con respecto a la anterior, principalmente en lo referente a los tiempos de latencia entre el ingreso y egreso de un equipo a un grupo multicast. Incluye la definición “Group-Specific Query”, como un subtipo de “Membership Query”, que permite a los routers transmitir un mensaje a un grupo en particular. También incluye la definición del mensaje “Leave Group”, para los equipos finales, que disminuye la latencia al abandonar un grupo. El mensaje de “Version 1 Membership Report” es usado por compatibilidad con IGMPv1.

La versión 3 de IGMP (IGMPv3) está definida en [54], con los siguientes mensajes:

- Membership Query.
- Version 3 Membership Report.
- Version 2 Membership Report.
- Version 1 Membership Report.
- Version 2 Leave Group.

IGMPv3 permite a los equipos finales especificar una dirección origen de tráfico multicast, o direcciones específicas de origen, enviadas a una dirección de grupo multicast en particular. Esa información puede ser utilizada por los protocolos de enrutamiento multicast para evitar la entrega de paquetes multicast de orígenes específicos a redes donde no hay interés en recibirlos.

3.3.4. Conmutación de Tráfico Multicast

El comportamiento por defecto de un switch capa 2 es enviar todo el tráfico multicast por todos los puerto del dispositivo. Esto es contrario al propósito de un switch, el cual es limitar el tráfico a los puertos que necesitan recibir los datos.

Debido a esto, el control del tráfico multicast en capa 2 puede ser realizado de varias maneras:

- VLANs: se pueden definir VLANs que correspondan con los limites de los grupos multicast. Sin embargo, no soporta cambios dinámicos en los grupos.
- IGMP Snooping: este mecanismo requiere que el switch examine cada paquete multicast en busca de paquetes con mensajes IGMP. Cuando detecta un mensaje de “Membership Report” de un equipo para un grupo multicast en

particular, el switch agrega el número de puerto del equipo a una tabla de entradas multicast. Si detecta un mensaje “Leave Group” de un equipo, elimina el puerto del equipo de la tabla. Sin embargo, este mecanismo consume una gran cantidad de capacidad de procesamiento del switch y de allí degrada el funcionamiento de envió y aumenta la latencia.

- Cisco Group Management Protocol (CGMP): este mecanismo permite a los routers trabajar en conjunto con los switches para configurar el envió de tráfico multicast sólo a los puertos interesados en dicho tráfico. Cuando un equipo desea unirse a un grupo multicast, éste envía un mensaje IGMP “Membership Report” al grupo destino. Este mensaje pasa a través del switch hacia el router. El router recibe el mensaje de reporte IGMP y lo procesa normalmente, pero en adición, crea un mensaje “Join” y lo envía al switch por donde llegó el mensaje IGMP. De igual manera funciona con los mensajes IGMP “Leave Group”, en donde el router en vía al switch un mensaje “Leave”. De esta manera el switch mantiene una tabla de grupos multicast. Debido a que es un protocolo propietario, sólo está disponible en dispositivos Cisco.

3.3.5. Enrutamiento de Tráfico Multicast

Una dirección multicast identifica más a un flujo de transmisión de datos en particular que a un destino físico. Un equipo es capaz de unirse a una transmisión multicast usando IGMP para comunicar este deseo al router de la subred en donde se encuentra ubicado.

Debido a que el número de receptores para un tráfico multicast puede potencialmente ser grande, el origen no necesita saber todas las direcciones IP interesadas. En vez de eso, los routers de la red deben ser capaces de trasladar las direcciones multicast en direcciones de equipos. El enrutamiento multicast está basado en la construcción de “árboles”, que conectan los miembros de varios grupos multicast.

Árboles de Distribución Multicast

Un árbol de distribución especifica un camino único de envió entre la subred del origen y cada subred que contenga miembros de grupos multicast. Debido a que los grupos multicast son dinámicos, con miembros uniéndose o dejando un grupo en cualquier momento, los árboles de distribución deben ser actualizables. Ramas que contienen nuevos miembros deben ser agregadas y las que no tienen miembros deben ser eliminadas.

Los dos tipos básicos de árboles de distribución multicast son:

Árboles de Origen

La forma más simple de un árbol de distribución multicast es el árbol de origen, en donde la raíz es el origen del tráfico multicast y las ramas forman un árbol de difusión hacia la red de receptores. Debido a que este árbol utiliza el camino más corto hacia una red, es también referenciado frecuentemente como “árbol de camino más corto” (SPT, por sus siglas en inglés).

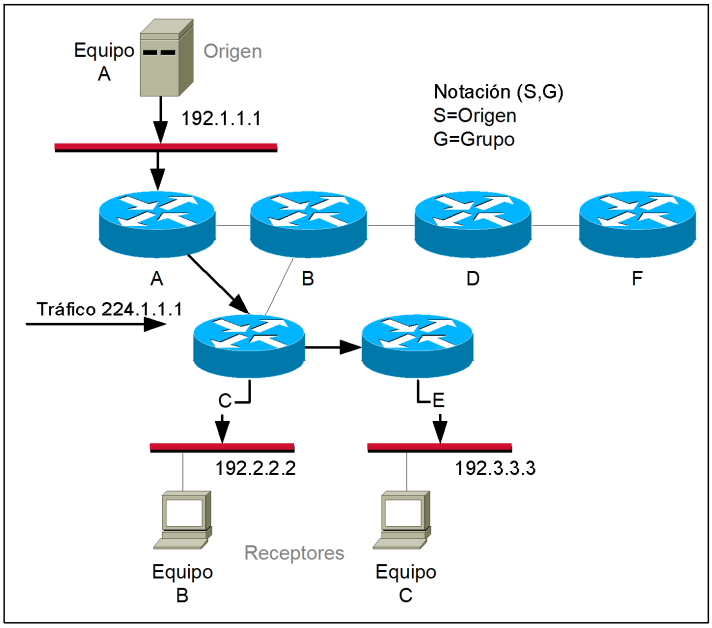

Figura 3-29: Árbol de Camino más Corto.

En la Figura 3-29 (tomada de [79]) se muestra un ejemplo de un SPT para el grupo 224.1.1.1 iniciado en el origen, equipo A, y conectando a dos (2) receptores, equipos B y C.

La notación especial de (S,G) enumera un SPT donde S es la dirección del origen y G es la dirección del grupo multicast. El SPT del ejemplo se escribiría (192.1.1.1,224.1.1.1). Se puede observar que esta notación implica un SPT por cada par origen-grupo diferente, es decir, que si el equipo B está enviando tráfico multicast al grupo 224.1.1.1 y los equipos A y C son receptores, entonces un SPT separado debe existir con notación (192.2.2.2, 224.1.1.1).

Árboles Compartidos

Los árboles compartidos usan una sola raíz en común ubicada en algún punto de la red. Dependiendo del protocolo de enrutamiento multicast, esta raíz es frecuentemente llamada “Punto Rendezvous” (RP, por sus siglas en inglés) o “Core” (núcleo), lo cual origina otros nombres para los árboles compartidos, tales como árboles RP (RPT, por sus siglas en inglés) o árboles basados en núcleo (CBT, por sus siglas en inglés).

En la Figura 3-30 (tomada de [79]) se muestra un árbol para el grupo 224.2.2.2 con la raíz (RP) ubicada en el router D, cuando se usa árboles compartidos, los orígenes deben enviar su tráfico a la raíz, y ésta se encarga de enviarlo a todos los receptores.

Debido a que todos los orígenes en el grupo multicast usan un árbol compartido en común, una notación especial escrita (*,G) representa al árbol. En este caso * significa todos los orígenes, y G representa al grupo multicast.

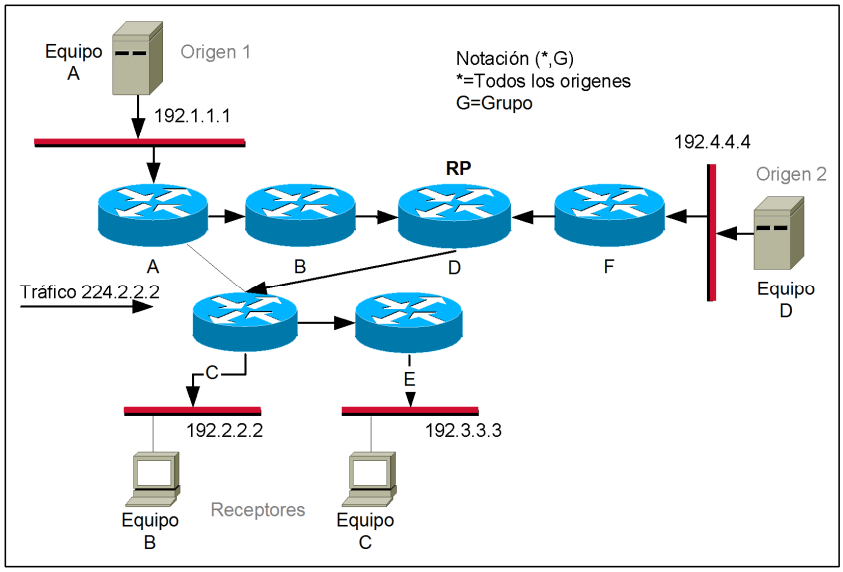

Figura 3-30: Árbol de Distribución Compartida.

Reverse Path Forwarding (RPF)

En las comunicaciones multicast, el origen envía tráfico a un grupo arbitrario de equipos representados por una dirección de grupo multicast en el campo dirección destino de un paquete IP. En contraste con el modelo unicast, los routers multicast no pueden basar su información de envío en la dirección destino de un paquete, estos routers típicamente tienen que enviar los paquetes multicast hacia múltiples interfaces para alcanzar a todos los receptores.

Virtualmente todos los protocolos de enrutamiento IP multicast hacen uso de alguna forma de RPF como mecanismo para determinar si un paquete multicast entrante se envía o elimina. Cuando un paquete multicast llega a un router, éste realiza un chequeo RPF en el paquete, si el cheque es exitoso, el paquete es enviado, de otra manera se elimina.

Para un tráfico fluyendo a través de un “árbol de origen”, el mecanismo de chequeo RPF trabaja de la siguiente manera:

1. El router examina la dirección origen del paquete multicast que ingresa para determinar si éste llega por medio de una interfaz que esta sobre el camino de regreso al origen.
2. Si el paquete ingresa por la interfaz de regreso al origen, el chequeo RPF es exitoso y el paquete es enviado.
3. Si el chequeo RPF falla, el paquete es descartado.

La Figura 3-31 (tomada de [79]) ilustra el proceso de chequeo RPF. Un paquete multicast de origen 151.10.3.21 es recibido por la interfaz S1. Un chequeo de la tabla de enrutamiento multicast muestra que la interfaz de regreso al origen es S1, por lo tanto el chequeo RPF es exitoso. Por otro lado si el paquete multicast hubiese llegado por la interfaz S0, el chequeo RPF fallaría, descartando el paquete multicast.

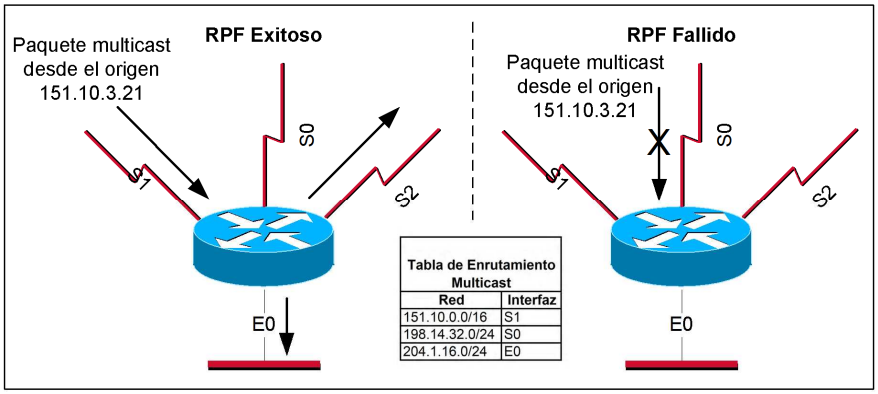

Figura 3-31: Falla y Éxito de Chequeos RPF.

Debido a que el router multicast determina cual interfaz está en el camino de regreso al origen, el RPF depende del protocolo de enrutamiento en uso.

Umbrales TTL

Cada vez que un paquete multicast es enviado por un router, el valor TTL en el encabezado IP es reducido en uno. Si el TTL del paquete es reducido a cero, el router elimina el paquete. Los umbrales TTL pueden ser aplicados a interfaces individuales de un router multicast para prevenir que paquetes multicast con un TTL menor sea enviado por la interfaz. La Tabla 3-4 (tomada de [79]) muestra los valores iniciales TTL y umbrales típicos para varios alcances.

Alcance TTL	Valor inicial TTL	Umbral TTL
LAN	1	N/A
Sitio	15	16
Región	63	64
Todos	127	128

Tabla 3-4: Valores Típicos de Umbrales TTL.

Los umbrales TTL proveen un mecanismo simple para prevenir el envío de tráfico multicast más allá de los límites de un sitio u organización basado en el campo TTL del paquete IP multicast.

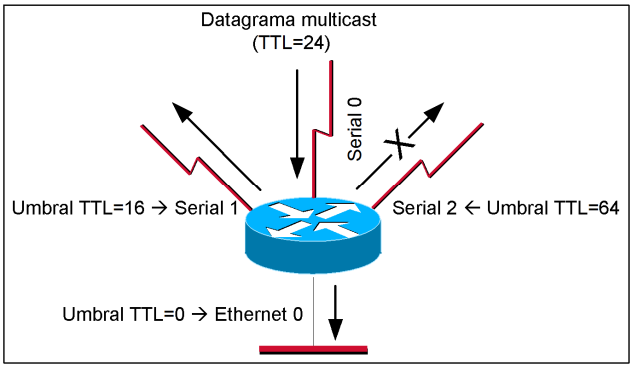

Figura 3-32: Umbrales TTL.

En la Figura 3-32 (tomada de [79]), un paquete multicast llega via Serial 0 con un TTL igual a 24. Asumiendo que el chequeo RPF fue exitoso y que las interfaces Serial 1, Serial 2 y Ethernet 0 están todas en la lista de interfaces de salida, el paquete normalmente podría ser enviado por todas esas interfaces. Pero debido a que un umbral TTL ha sido definido en esas interfaces, el router debe asegurarse que el valor TTL del paquete, que ahora es 23, es mayor o igual al umbral TTL de cada interfaz antes de enviar el paquete por cada una de ellas. Para este ejemplo entonces, el paquete es sólo enviado por las interfaces Serial 1 y Ethernet 0.

3.3.6. Protocolos de Enrutamiento Multicast

Un protocolo de enrutamiento multicast es responsable de la construcción de los árboles de entrega multicast y es necesario para permitir el envío de paquetes multicast. Diferentes protocolos de enrutamiento IP multicast usan distintas técnicas para la construcción de árboles de difusión y para el envío de paquetes.

Los protocolos multicast actuales pueden ser divididos en dos categorías básicas: los protocolos de modo denso y los protocolos de modo disperso.

Protocolos de Modo Denso

Los protocolos de modo denso emplean sólo SPTs para entregar tráfico multicast (S,G) usando un principio de “push”. Este principio asume que cada subred en la red tiene al menos un receptor del tráfico multicast (S,G), y de ahí el tráfico es enviado o inundado a todos los puntos en la red.

Inundar el tráfico multicast a cada punto en la red conlleva un costo asociado (ancho de banda, procesamiento en el router, etc.). Por tal motivo, para evitar el consumo innecesario de los recursos de la red, los routers envían mensajes “prune” de regreso al origen del árbol de distribución para “cortar” el tráfico multicast indeseado. El resultado es que las ramas sin receptores son eliminadas del árbol de distribución, dejando sólo las ramas que contiene receptores.

En la Figura 3-33 (tomada de [79]), cuando un router A recibe un mensaje “prune” para el flujo de tráfico multicast (S,G) en una interfaz de salida (E0), el router coloca la interfaz en estado “pruned” y detiene el envío de tráfico (S,G) por esa interfaz. El estado “pruned” tiene un valor de tiempo de expiración, de modo tal que cuando este tiempo se cumple, el router devuelve la interfaz ha su estado anterior, enviando paquetes multicast.

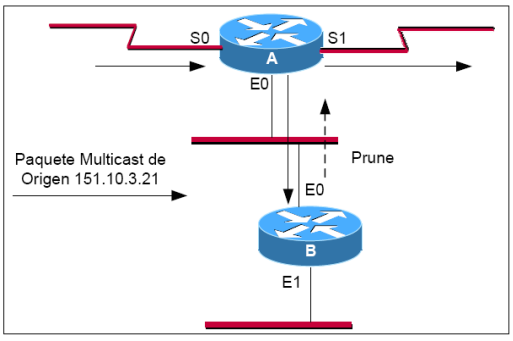

Figura 3-33: Eliminando un Flujo en Modo Denso.

Muchos protocolos de modo denso pueden agregar rápidamente una rama previamente eliminada del árbol de distribución. Cuando un router recibe un mensaje “graft” de otro router, inmediatamente coloca la interfaz por la cual recibió el mensaje en un estado de envío de tráfico multicast hacia el receptor.

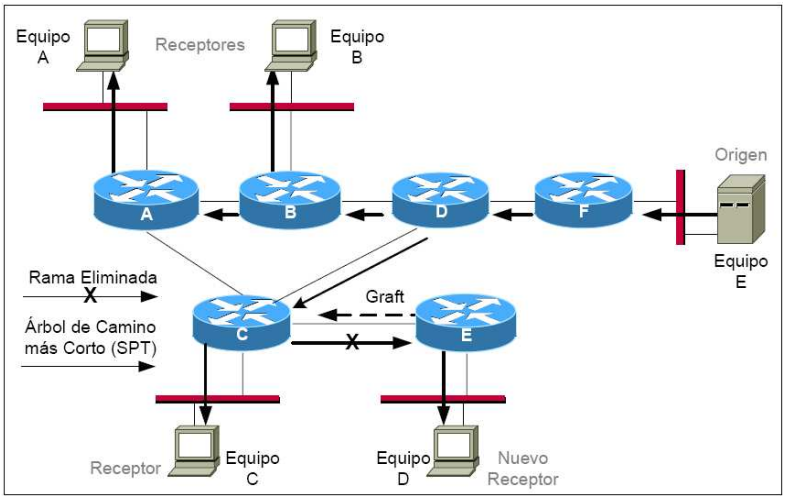

Figura 3-34: Mensaje “Graft” en Modo Denso.

En la Figura 3-34 (tomada de [79]) se muestra este proceso, el origen (Equipo E) está transmitiendo tráfico multicast hacia el SPT (denotado por las flechas sólidas) a los Equipos A, B y C. El router E previamente ha enviado un mensaje “prune” al router C. En este punto, el Equipo D se une al grupo multicast como un nuevo receptor. Esta acción conlleva al router E a enviar un mensaje “graft” al router C para inmediatamente reiniciar el envió del flujo multicast. Con este proceso, el router E puede evitar tener que esperar por la expiración del tiempo del estado “pruned” de la interfaz del router C.

Entre los protocolos de modo denso se incluyen los siguientes:

- *DVMRP (Distance Vector Multicast Routing Protocol*): está definido en [55], y en gran medida fue derivado de RIP. Cuando un router recibe un paquete, este envía el paquete por todas las interfaces excepto por la de regreso al origen. Si un router está unido a un conjunto de LANs que no desean recibir un grupo multicast en particular, el router puede enviar un mensaje “prune” de regreso al árbol de distribución para detener los paquetes subsecuentes que van donde no hay miembros. DVRMP periódicamente inunda con paquetes multicast de tal manera de alcanzar cualquier nuevo equipo que desee recibir tráfico de un grupo multicast en particular. También implementa su propio protocolo de enrutamiento unicast, basado en el número de saltos, de manera de determinar por cual interfaz se devuelve al origen del flujo de datos.
- *MOSPF (Multicast Extensions to OSPF)***:** fue definido en [56] como una extensión del protocolo de enrutamiento unicast OSPF [57], trabaja incluyendo información multicast en los anuncios de estado de enlace de OSPF; de esta manera un router MOSPF aprende cuales grupos multicast están activos en cuales LAN. MOSPF construye un árbol de distribución por cada par (S,G) y computa un árbol para activar el envío desde el origen al grupo. El estado del árbol es almacenado, y debe ser recalculado cuando un estado de un enlace cambia o cuando el

tiempo de almacenamiento del árbol expira. MOSPF debe ser utilizado en entornos que tienen relativamente pocos pares (S,G) en cualquier momento, y sólo en redes que usan OSPF.

- *PIM-DM (Protocol Independent Multicast – Dense Mode)*: definido en [58], asume que cuando un origen empieza a enviar, todos los demás sistemas desean recibir los datagramas multicast. Inicialmente los datagramas son enviados a todas las áreas de la red; en las áreas de la red en donde los grupos no tienen miembros, PIM-DM enviará un mensaje "prune" para iniciar un estado "pruned" y detener el flujo de paquetes hacia esa área. El estado "pruned" tiene una vida finita, cuando éste expira, los datos volverán ha ser enviados hacia la red. Comparado con DVMRP, PIM-DM ha simplificado el diseño y no está atada a un protocolo de descubrimiento de topología específico. Sin embargo, esta simplificación aumenta el trabajo, debido a que causa inundaciones y estados "pruned" en algunos enlaces, que podrían ser evitados si suficiente información de la topología estuviese disponible. Las condiciones bajo las cuales PIM-DM es útil son:
  - Orígenes y receptores están relativamente cerca unos a otros.
  - Hay pocos orígenes y muchos receptores.
  - El volumen del tráfico multicast es alto.
  - El flujo del tráfico multicast es constante.

Protocolos de Modo Disperso

El otro método de enrutamiento multicast está basado en una distribución dispersa de grupos de miembros multicast. Por tal motivo, el empleo de un método más eficiente para lograr el enrutamiento multicast llega a ser necesario.

Los protocolos en modo disperso usan árboles compartidos y ocasionalmente SPT para distribuir el tráfico multicast a los receptores en la red. También hace uso de un modelo "pull" en el cual el tráfico multicast es enviado hacia los receptores en la red. Este modelo "pull" asume que el tráfico multicast no es deseado a menos que se solicite específicamente usando mecanismos de unión explícitos.

Para enviar tráfico multicast hacia los receptores en una red en modo disperso, una rama del árbol compartido debe ser construida desde el nodo raíz a los receptores. Para construir esta rama, un router envía un mensaje "join" a la raíz del árbol compartido (ver Figura 3-35 tomada de [79]). Este mensaje viaja a través de los routers intermedios hacia la raíz, construyendo de esta manera una rama del árbol compartido.

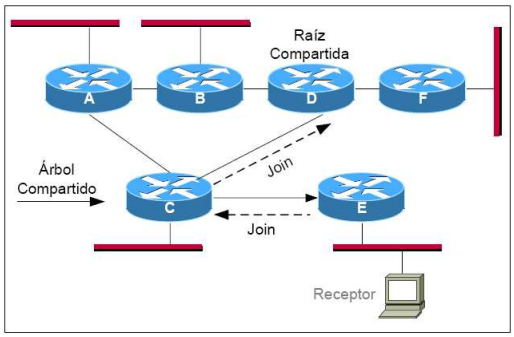

Figura 3-35: Mensaje de Unión en un Árbol Compartido.

En el modo disperso, los mensajes “prune” son enviados al árbol de distribución cuando el tráfico de un grupo multicast ya no es deseado. Esta acción permite a las ramas, del árbol compartido o SPT, que fueron creadas vía mensajes “join” desaparecer cuando no se necesiten más.

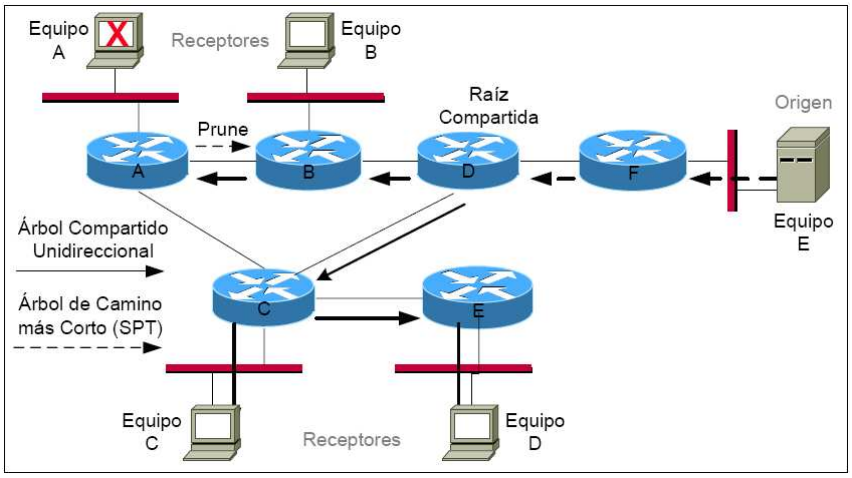

Figura 3-36: Mensaje “Prune” en un Árbol de Distribución.

En la Figura 3-36 (tomada de [79]) se muestra este proceso, el Equipo A ha dejado el grupo multicast, por lo tanto, el router A no necesita enviar más tráfico del árbol compartido (indicado por las flechas sólidas) y envía un mensaje “prune” de regreso del árbol compartido hacia la raíz. Este mensaje elimina la rama del árbol entre el router A y B y detiene el tráfico multicast innecesario hacia el router A.

Entre los protocolos de modo disperso se incluyen los siguientes:

- *CBT (Core Based Trees):* fue originalmente descrito en [59] y actualizado en [60], pero desafortunadamente CBTv1 y CBTv2 no son compatibles. Este protocolo construye un sólo árbol que es compartido por todos los miembros de un grupo. El tráfico multicast para todo el grupo es enviado y recibido sobre el mismo árbol. CBT utiliza un router central que es usado para construir el árbol. Cuando los router están listos para unirse al árbol envían un mensaje de “join” al router central, entonces el router central envía un mensajes de respuesta que viajan por el camino de regreso hacia los routers que solicitan la unión, de esta manera se crea las ramas del árbol. Debido a que los mensajes CBT “join” tienen un TTL de 1, los routers CBT en la red envían los mensajes salto por salto hasta alcanzar al router central o algún otro router CBT que está en el árbol compartido.
- *PIM-SM (Protocol Independent Multicast – Sparse Mode):* es un protocolo, definido en [61], para el enrutamiento eficiente de grupos multicast que pueden ser distribuidos en un área amplia de Internet. Aunque puede usarse enrutamiento unicast para proveer información del camino de regreso para la construcción de árboles multicast, no depende de ningún protocolo de enrutamiento unicast en particular. PIM-SM construye árboles compartidos unidireccionales originados en un Punto Rendezvous (RP) por grupo, y opcionalmente crea árboles de caminos más corto por origen. Un RP es un router que ha sido configurado para ser usado como la raíz de un árbol de

- distribución de origen no específico para un grupo multicast. Los mensajes “join” de los receptores para grupos son enviados hacia el RP, y los datos de los orígenes son enviados al RP para que los receptores puedan descubrir cuales orígenes están y empezar a recibir el tráfico destinado al grupo. En resumen, para hacer que el tráfico multicast fluya bajo PIM-SM, los equipos deben registrase con el RP. Existen dos variantes que nacen de PIM-SM, estos son:
  - Source Specific Multicast (SSM): sólo es soportado por modelos uno a muchos. PIM-SSM construye SPTs originados en la raíz del tráfico multicast. Los routers cercanos a receptores interesados son informados de la dirección IP unicast del origen del tráfico multicast; por este motivo PIM-SSM no necesita RP.
  - Bidireccional (Bidir): su principal diferencia radica en el mecanismo usado para enviar los datos desde el origen al RP. En PIM-SM los datos son enviados usando algún tipo de encapsulado o árbol basado en el origen, en PIM-Bidir los datos fluyen al RP por medio del árbol compartido, el cual es un flujo de datos bidireccional a lo largo de las ramas.

3.4. Multicast sobre IPv6

Multicast sobre IPv4 se ha desarrollado a lo largo de varios años. Múltiples características y protocolos fueron desarrollados, y muchos de ellos también fueron dejados de lado basados en la experiencia ganada con el despliegue y operación del servicio. Las características y protocolos que no fueron útiles en IPv4 multicast fueron completamente ignorados en IPv6, tal como se muestra en la Tabla 3-5 (tomada de [81]), las características explicitas de IPv4 multicast que no fueron consideradas en IPv6 son marcadas NC (No Considerada).

Función del Protocolo	Protocolo Multicast	IPv4	IPv6
Administración de Grupos	Internet Group Management Protocol (IGMP) v1, v2 y v3	X	
	Multicast Listener Discovery (MLD) v1, v2		X
Soporte Multicast en Capa 2	Snooping (IGMP o MLD)	X	X
	Cisco Group Management Protocol (CGMP)	X	NC
Enrutamiento Multicast	Protocol Independent Multicast – Dense Mode (PIM-DM)	X	NC
	Protocol Independent Multicast – Sparse Mode (PIM-SM)	X	X
	Protocol Independent Multicast – Source Specific Multicast (PIM-SSM)	X	X
	Bidirectional – Protocol Independent Multicast (BIDIR-PIM)	X	X
Administración de Puntos Rendezvous	Static-RP	X	X
	Auto-RP	X	
	Bootstrap Router (BSR)	X	X
	Embedded RP		X
	Multicast Source Discovery Protocol (MSDP)	X	NC

Tabla 3-5: Taxonomía de los protocolos multicast y su disponibilidad en IPv6.

Un aspecto importante de los servicios multicast es el direccionamiento. En donde una dirección unicast identifica un nodo, una dirección multicast identifica un grupo de nodos interesados en los mismos datos.

IPv6 multicast se beneficia de la nueva arquitectura de direccionamiento definida en IPv6 por las siguientes razones:

- Un mayor espacio de direcciones implica la disponibilidad de un mayor número de direcciones para grupos multicast.
- El alcance de direcciones ofrece una forma limpia para la contención de tráfico multicast dentro de un dominio previsto.

3.4.1. Grupos Multicast

Un grupo multicast en IPv6, como se mencionó anteriormente, es un grupo arbitrario de receptores que desean recibir un flujo particular de datos.

Direcciones IPv6 Multicast

Una dirección IPv6 multicast es una dirección IPv6 que tiene el prefijo FF00::/8 (1111 1111), también es un identificador para un conjunto de interfaces que típicamente pertenece a diferentes nodos. Un paquete enviado a una dirección multicast es entregada a todas las interfaces identificadas por la dirección multicast.

El segundo byte que sigue al prefijo (ver Figura 3-14) define la permanencia y alcance de una dirección multicast. Si la dirección es permanente, tiene el bit de permanencia igual a 0, si es temporal, igual a 1. Una dirección multicast que tiene un alcance de nodo, enlace, sitio, organización o global tienen un parámetro de alcance de 1, 2, 5, 8 ó E, respectivamente.

Los nodos IPv6 (equipos y routers) siempre deben unirse a los grupos multicast siguientes (definidos en [10]):

- Grupo multicast de todos los nodos FF02::1 (con alcance local al enlace): agrupa a todos los nodos IPv6, tanto equipos como routers.
- Grupo multicast de nodo solicitado FF02:0:0:0:0:1:FF00::/104 por cada una de sus direcciones unicast y anycast asignadas.

Además los routers IPv6 deben también unirse al grupo multicast de todos los routers FF02::2 (con alcance local al enlace), que agrupa sólo los routers IPv6.

La dirección multicast de nodo solicitado es un grupo multicast que corresponde a una dirección IPv6 unicast o anycast. La dirección IPv6 multicast de nodo solicitado tiene el prefijo FF02:0:0:0:0:1:FF00::/104 (ver Figura 3-37 tomada de [81]) concatenado con los 24 bits de orden inferior de una dirección unicast o anycast correspondiente. Por ejemplo, la dirección multicast de nodo solicitado correspondiente a la dirección IPv6 2037::01:800:200E:8C6C es FF02::1:FF0E:8C6C.

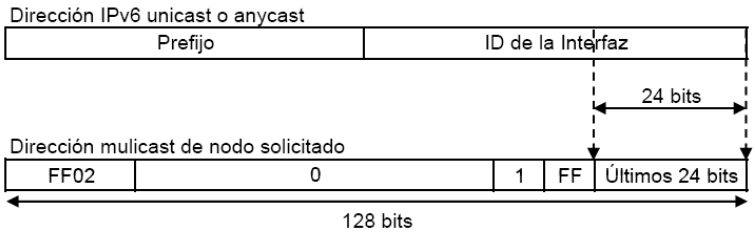

Figura 3-37: Formato de una Dirección IPv6 Multicast de Nodo Solicitado.

Alcance de las Direcciones IPv6

Una zona es una instancia en particular de una región topológica, en donde un alcance es el tamaño de la región. Por ejemplo, el conjunto de enlaces conectados por los routers en un sitio en particular, y las interfaces asociadas a esos enlaces, comprenden una sola zona de alcance local al sitio.

Las zonas de diferentes alcances se instan de la siguiente manera:

- Cada enlace, y las interfaces asociadas al enlace, comprenden una sola zona de alcance local al enlace (tanto para unicast y multicast).
- Existe una sola zona de alcance global (tanto para unicast y multicast), comprende todos los enlaces e interfaces de Internet.
- Los limites de las zonas de alcance distintas a local a la interfaz, local al enlace y global deben ser definidas y configuradas por los administradores de red.

3.4.2. Direcciones IPv6 Multicast en Capa 2

Así como en IPv4, el último bit del primer byte de una dirección MAC IEEE 802.3 es usado para indicar si una trama es broadcast o multicast (Figura 3-38). Si el bit es igual a uno (1), la trama va dirigida a un grupo de equipos o a todos los equipos de la red.

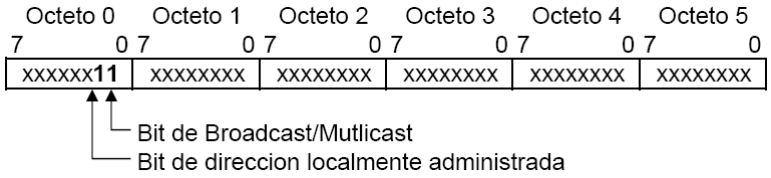

Figura 3-38: Formato de una Dirección MAC IEEE 802.3.

Asignación de Direcciones IPv6 multicast a Direcciones Ethernet

Las direcciones MAC en Ethernet son de 48 bits. De esos 48 bits, 24 bits comprenden el OUI y los otros 24 bits el número de serial de la tarjeta, los cual forman una dirección única.

Para IPv6 multicast existe un formato OUI, que se define en [62], en donde los dos primeros bytes son definidos en 33:33, dejando los siguientes 4 bytes disponibles para los últimos 32 bits de la dirección IPv6 multicast de 128 bits (ver Figura 3-39 tomada de [81]).

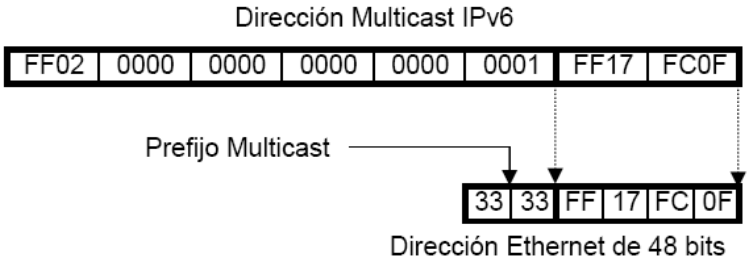

Figura 3-39: Asignación de IPv6 Multicast a Ethernet.

3.4.3. Administración del Tráfico IPv6 Multicast

IGMP es usado en IPv4 para permitir a los equipos sobre un enlace unirse, dejar, o simplemente comunicar a un router la pertenencia a un grupo multicast. Pasó por varios desarrollos, IGMPv1 [43], IGMPv2 [53] e IGMPv3 [54], ésta última versión es compatible con las anteriores, pero cada una de ellas agrega características que mejoran la operación de su predecesor.

En IPv6 “Multicast Listener Discovery” (MLD) realiza las funciones de IGMP. Y de la misma manera se desarrollaron varias versiones del protocolo, MLDv1 [28] y MLDv2 [29], los cuales se corresponden idénticamente con las dos últimas versiones de IGMP (ver Tabla 3-6 tomada de [81]).

MLD	IGMP	Tipo de Mensaje MLD	Tipo ICMPv6
-----	IGMPv1 (RFC 1112)	-----	-----
MLDv1 (RFC 2710)	IGMPv2 (RFC 2236)	Multicast Listener Query	130
		Multicast Listener Report	131
		Multicast Lsitener Done	132
MLDv2 (RFC 3810)	IGMPv3 (RFC 3376)	Multicast Listener Query	130
		Multicast Listener Report	143

Tabla 3-6: Tipos de Mensajes MLD.

Suscripción y Mantenimiento de Grupos Multicast en IPv6

MLD es el protocolo que permite a los escucha multicast registrarse a direcciones multicast que desean usar, para asegurar un enrutamiento eficiente. Por tal motivo, es necesario un mecanismo de enrutamiento para administrar el envío de mensajes multicast.

MLD es un protocolo asimétrico, el comportamiento de los que escuchan, por ejemplo los nodos que desean recibir mensajes destinados a un grupo multicast específico, difiere del comportamiento de los routers. Los routers utilizan MLD para descubrir cuales direcciones multicast tienen receptores en cada uno de sus enlaces. Por cada

enlace directamente conectado, el router almacena una lista de direcciones de receptores.

Un receptor envía reportes de miembro para una dirección multicast. Con estos mensajes, se registran con los routers sobre el enlace para recibir los mensajes dirigidos a los respectivos grupos multicast. Si la dirección multicast no está en la lista del router para este enlace, el router la agrega a su lista de direcciones multicast a ser enviadas por esa interfaz. Con un mensaje “Done”, un receptor manifiesta su deseo de dejar de recibir mensajes para una dirección multicast. Cuando el último miembro de un grupo se retira de una dirección multicast, el router elimina la dirección de su lista para dicho enlace.

El comportamiento de un router que implementa MLD depende de si hay o no muchos routers multicast en la misma subred. Si existen muchos routers, un mecanismo de elección es usado para elegir a un sólo router multicast en estado “Querier” (de consulta). Todos los routers multicast en la subred escuchan los mensajes enviados por los nodos miembros de grupos multicast, y mantienen la misma información de estado multicast, por lo que pueden rápidamente y en forma correcta tomar la funcionalidad del “Querier”, si este presentara una falla. Sin embargo, es sólo el “Querier” quien envía periódicamente mensajes de consulta en la subred. Los nodos responden a estos mensajes de consulta reportando su estado.

El mecanismo de elección del “Querier” indica que cuando un router empieza a operar en una subred, por defecto este se considera el “Querier” de la subred. Por lo que envía muchos mensajes de consulta separados por intervalos pequeños de tiempo. Cuando un router recibe una consulta con una dirección IPv6 más alta que la propia, y si estaba previamente en estado “Querier”, se cambia a un estado “Non-Querier” y deja de enviar mensajes de consulta sobre el enlace.

Todos lo mensajes MLD (ver Figura 3-40 tomado de [28]) son enviados con una dirección IPv6 de tipo link-local y con un límite de saltos igual a uno (1) para asegurarse de que ellos se mantengan en el enlace local. El paquete tiene la opción de encabezado “hop-by-hop” con la bandera de “Router Alert” [63] activa. Por tal motivo, los routers no ignoraran el paquete, aunque no pertenezcan al grupo multicast en cuestión.

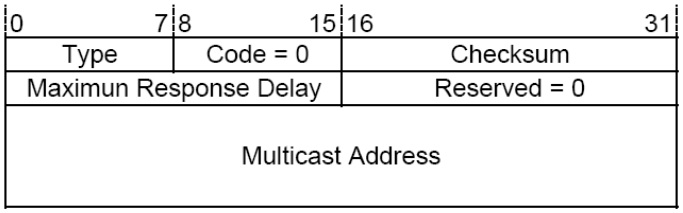

Figura 3-40: Formato de un Mensaje MLD.

MLDv1

La primera versión del protocolo MLD (MLDv1) se definió en [28], en octubre de 1999, y fue derivada de IGMPv2. Una característica importante de MLDv1 es que basa el envío

de sus mensajes en ICMPv6, a diferencia de IGMP que se basa en una implementación propia.

Se definieron tres tipos de mensajes para MLDv1:

- Multicast Listener Query (Tipo de Mensaje ICMPv6 130).
- Multicast Listener Report (Tipo de Mensaje ICMPv6 131).
- Multicast Listener Done (Tipo de Mensaje ICMPv6 132).

Multicast Listener Query (Tipo 130)

Un router IPv6 multicast utiliza este mensaje para consultar en un enlace por miembros de grupos multicast. Existen dos tipos de mensajes de consulta:

- General Query: son enviadas periódicamente (por defecto cada 125 seg.) para consultar a todos los nodos en una subred por la presencia de miembros de grupos multicast de cualquier dirección multicast. La única dirección multicast que no es reportada en la dirección multicast de todos los nodos (FF02::1).
- Multicast-Address-Specific Query: son utilizadas para consultar a todos los nodos en una subred que son miembros de una dirección multicast específica.

Estos dos tipos de mensaje de consulta son distinguidos por el campo “Destination Address” en el encabezado de IPv6 y por el campo “Multicast Address” dentro del mensaje de consulta.

En el encabezado IPv6 de este tipo de mensaje tiene las siguientes características:

- El campo “Hop Limit” es establecido a 1.
- El campo “Source Address” es establecido a la dirección de tipo link-local de la interfaz sobre la cual la consulta es enviada.
- El campo “Destination Address” es la dirección multicast específica a ser consultada. Para las consultas “General Query” es establecida en la dirección multicast de alcance local de “todos los nodos” (FF02::1). Para las consultas “Multicast-Address-Specific Query” es establecida a la dirección multicast específica a ser consultada.

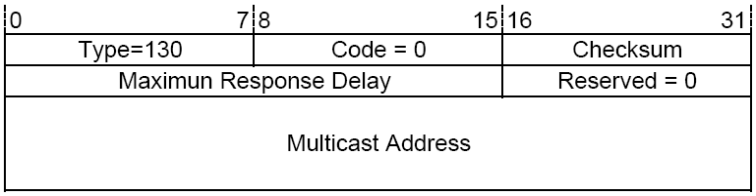

Figura 3-41: Estructura de un Mensaje “Multicast Listener Query”.

Los campos en un mensaje “Multicast Listener Query” (ver Figura 3-41 tomada de [28]) son:

- ***Type:*** el valor de este campo es 130
- ***Code:*** el valor de este campo es cero (0).

- ***Checksum:*** el valor de este campo es la suma de comprobación de ICMPv6.
- ***Maximun Response Delay:*** indica la máxima cantidad de tiempo (por defecto 10.000 milisegundos) dentro del cual un miembro de un grupo multicast debe reportar su membresía usando un mensaje de reporte "Multicast Listener Report". Cuando un equipo que es miembro de un grupo de una dirección multicast dada recibe un mensaje "Multicast Listener Query", el equipo utiliza el valor de éste campo para calcular un nuevo tiempo de respuesta que es menor o igual al valor actual. El equipo dentro de la subred al cual le expire primero este nuevo tiempo de respuesta envía un mensaje "Multicast Listener Report"; cuando los otros equipos miembros del mismo grupo reciben este mensaje, abandonan el intento de enviar su mensaje de reporte del mismo tipo. Este proceso resulta típicamente en que sólo un equipo miembro reporta la membresía para una dirección multicast dada en cada subred.
- ***Reserved***: campo de 16 bits reservado para uso futuro, y establecido en 0.
- ***Multicast Address:*** para las consultas "General Query", este campo es establecido en la dirección sin especificar (::). Para las consultas "Multicast-Address-Specific Query" el campo es establecido a la dirección multicast que está siendo consultada. El tamaño de este campo es de 128 bits.

Multicast Listener Report (Tipo 131)

Este mensaje es usado por un nodo para reportar su interés en recibir tráfico multicast de una dirección multicast determinada o responder a un mensaje "Multicast Listener Query" (ya sea General Query o Multicast-Address-Specific Query).

En el encabezado IPv6 de este tipo de mensaje tiene las siguientes características:

- El campo "Hop Limit" es establecido a 1.
- El campo "Source Address" es establecido a la dirección de tipo link-local de la interfaz sobre la cual la consulta es enviada.
- El campo "Destination Address" es la dirección multicast específica a ser reportada.

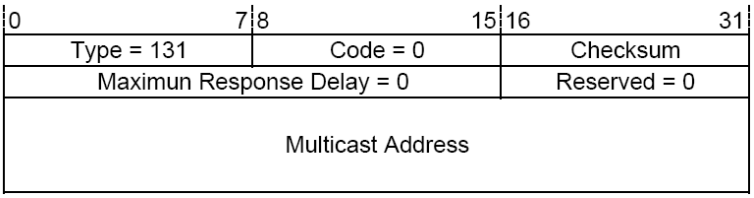

Figura 3-42: Estructura de un Mensaje "Multicast Listener Report".

Los campos en un mensaje "Multicast Listener Report" (ver Figura 3-42 tomada de [28]) son:

- ***Type:*** el valor de este campo es 131
- ***Code:*** el valor de este campo es cero (0).
- ***Checksum:*** el valor de este campo es la suma de comprobación de ICMPv6.
- ***Maximun Response Delay:*** este campo no es utilizado en este tipo de mensajes y es establecido en cero (0).

- ***Reserved***: campo de 16 bits reservado para uso futuro, y establecido en 0.
- ***Multicast Address:*** este campo es establecido a la dirección multicast que está siendo reportada.

Multicast Listener Done (Tipo 132)

Este mensaje es utilizado para informar a los routers locales que pudiera no haber miembros de un grupo de una dirección multicast específica en la subred. El router local verifica que no hay más miembros de un grupo en la subred.

Cuando un equipo no desea seguir recibiendo datos para una dirección multicast específica, este envía un mensaje "Multicast Listener Done" para indicar a los routers su deseo de salir de un grupo. Se puede observar que el miembro del grupo que envía este mensaje podría no ser el último de ese grupo en la subred.
Debido a que los routers IPv6 multicast no almacenan cuantos miembros hay en cada grupo en cada subred, tras la recepción de un mensaje "Multicast Listener Done", el router inmediatamente envía un mensaje "Multicast-Address-Specific Query" para la dirección multicast que está siendo reportada en el mensaje "Multicast Listener Done".

En el encabezado IPv6 de este tipo de mensaje tiene las siguientes características:

- El campo "Hop Limit" es establecido a 1.
- El campo "Source Address" es establecido a la dirección de tipo link-local de la interfaz sobre la cual el reporte está siendo enviado.
- El campo "Destination Address" es establecida la dirección multicast de todos los routers (FF02::2).

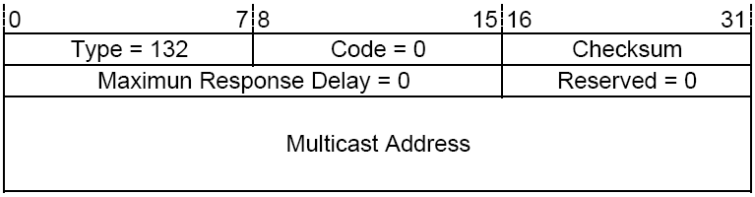

Figura 3-43: Estructura de un Mensaje "Multicast Listener Done".

Los campos en un mensaje "Multicast Listener Done" (ver Figura 3-43 tomada de [28]) son:

- ***Type:*** el valor de este campo es 132
- ***Code:*** el valor de este campo es cero (0).
- ***Checksum:*** el valor de este campo es la suma de comprobación de ICMPv6.
- ***Maximun Response Delay:*** este campo no es utilizado en este tipo de mensajes y es establecido en cero (0).
- ***Reserved:*** campo de 16 bits reservado para uso futuro, y establecido en 0.
- ***Multicast Address:*** este campo es establecido a la dirección multicast específica para la cual no se desea seguir siendo miembro.

MLDv2

La segunda versión de este protocolo MLD (MLDv2) se definió en [29], en junio de 2004, fue derivada de IGMPv3 y mantiene compatibilidad con MLDv1. MLDv2 agrega la habilidad a un nodo de hacer filtros de origen, lo que significa reportar interés en escuchar paquetes con una dirección multicast particular de sólo direcciones orígenes específicas o de todos los orígenes excepto de direcciones de origen específicas. Este mecanismo es denominado Multicast de Origen Específico (Source-Specific Multicast - SSM), definido en [67], en oposición Multicast de Cualquier Origen (Any-Source Multicast - ASM), a la cual pertenece la versión anterior (MLDv1).

Esta nueva versión introduce dos conceptos nuevos para la administración de grupos y recursos:

- Filtro INCLUDE: se reciben paquetes sólo desde orígenes especificados en el mensaje MLDv2.
- Filtro EXCLUDE: se reciben paquetes de todos los orígenes excepto los especificados en el mensaje MLDv2.

Existen dos tipos de mensajes en MLDv2:

- Multicast Listener Query (Tipo de Mensaje ICMPv6 130).
- Multicast Listener Report version 2 (Tipo de Mensaje ICMPv6 143).

Para asegurar la interoperabilidad con nodos que implementan MLDv1, MLDv2 debe soportar los siguientes mensajes:

- Multicast Listener Report version 1 (Tipo de Mensaje ICMPv6 131).
- Multicast Listener Done version 1 (Tipo de Mensaje ICMPv6 132).

Multicast Listener Query (Tipo 130)

Al igual que en MLDv1, estos mensajes son enviados por los routers multicast para consultar el estado multicast de escucha de las interfaces vecinas. Adicionalmente a los dos tipos de mensajes definidos en MLDv1, se incorpora un tercer tipo de mensaje:

- Multicast Address and Source Specific Query: son utilizadas para consultar a todos los nodos en una subred si son miembros o no, de una dirección multicast específica y un origen específico.

Estos tres tipos de mensaje de consulta son distinguidos por el campo “Destination Address” en el encabezado de IPv6, por el campo “Multicast Address” y “Source Address[i]” dentro del mensaje de consulta.

En el encabezado IPv6 de este tipo de mensaje tiene las siguientes características:

- El campo “Hop Limit” es establecido a 1.
- El campo “Source Address” es establecido a la dirección de tipo link-local de la interfaz sobre la cual la consulta es enviada.

- El campo “Destination Address” es la dirección multicast específica a ser consultada. Para las consultas “General Query” es establecida en la dirección multicast de “todos los nodos” (FF02::1). Para las otras consultas es establecida a la dirección multicast específica a ser consultada.

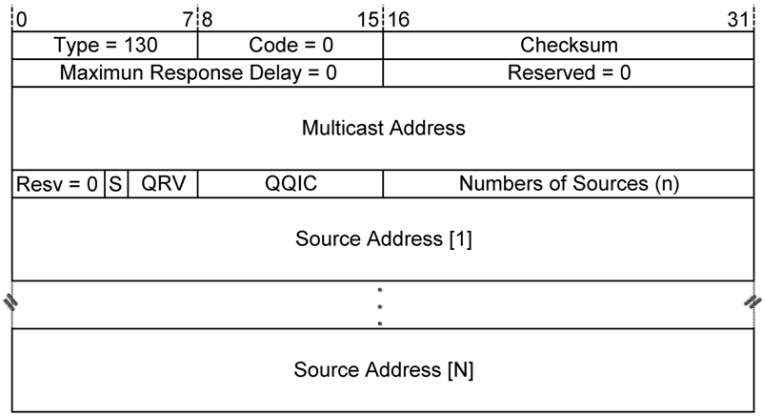

Figura 3-44: Estructura de un Mensaje “Multicast Listener Query version 2”.

Los nuevos campos en un mensaje “Multicast Listener Query” MLDv2 (ver Figura 3-44 tomada de [29]) agregados después del campo “Dirección Multicast” son:

- ***Reserved:*** campo de 16 bits reservado para uso futuro, y establecido en 0.
- ***S (Suppress Router-Side Processing):*** cuando está establecido en uno, indica para cualquier router multicast receptor que debe suprimir la actualización normal de tiempo que realiza tras escuchar una consulta.
- ***QRV (Querier’s Robustness Variable):*** si es distinta a cero, el campo QRV contiene el valor de la variable de robustez usada por el “Querier”. Este valor afecta los tiempos y números de reintentos. Está incluido en las consultas con el fin de sincronizar todos los routers MLDv2 conectados a la misma subred.
- ***QQIC (Querier’s Query Interval Code):*** este campo especifica en intervalo de consulta usado por el “Querier”.
- ***Numbers of Sources(N):*** especifica cuantas direcciones origen son presentados en la consulta. Este número es cero para una consulta “General Query” o para una consulta “Multicast-Address-Specific Query”, y distinta de cero para una consulta “Multicast Address and Source Specific Query”.
- ***Source Address[i]:*** contiene las direcciones orígenes.

Multicast Listener Report version 2 (Tipo 143)

Estos mensajes son enviados por los nodos IP para reportar, a los routers vecinos, el estado actual de escucha multicast, o cambios en los estados de escucha, de sus interfaces.

En el encabezado IPv6 de este tipo de mensaje tiene las siguientes características:

- El campo “Hop Limit” es establecido a 1.
- El campo “Source Address” es establecido a la dirección de tipo link-local de la interfaz sobre la cual la consulta es enviada.

- El campo “Destination Address” es establecida a la dirección de “todos los routers multicast MLDv2” (FF02::16).

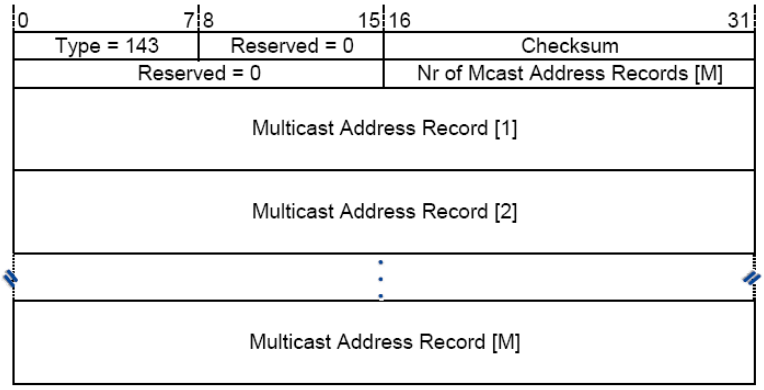

Figura 3-45: Estructura de un Mensaje “Multicast Listener Report version 2”.

Los campos en un mensaje “Multicast Listener Report version 2” (ver Figura 3-45 tomada de [29]) son:

- ***Type:*** el valor de este campo es de 143.
- ***Reserved:*** campo de 8 bits reservado para uso futuro, y establecido en 0.
- ***Checksum:*** el valor de este campo es la suma de comprobación de ICMPv6.
- ***Reserved:*** campo de 16 bits reservado para uso futuro, y establecido en 0.
- ***Nr of Mcast Address Record (M):*** especifica cuantos registros de direcciones multicast están presentes en el reporte.
- ***Multicast Address Record:*** cada registro de dirección multicast es un bloque de campos que contiene información sobre el receptor que escucha a una sola dirección multicast sobre la interfaz por la cual el reporte es enviado.

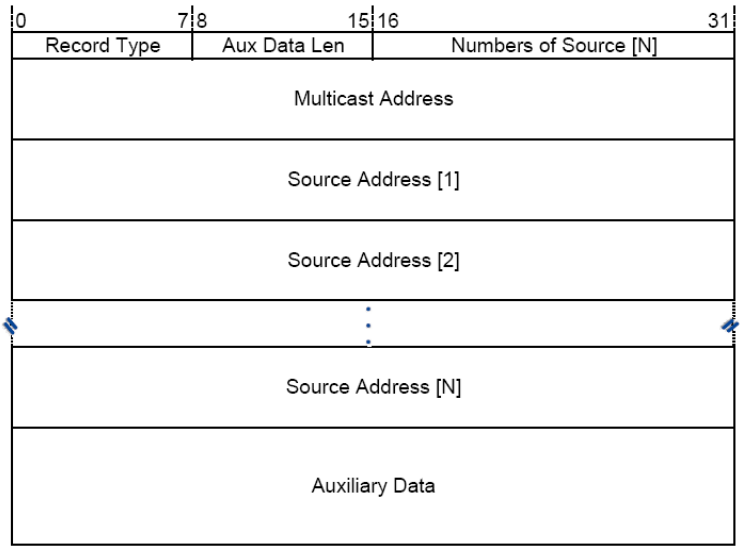

Figura 3-46: Estructura de un Registro de Dirección multicast.

Cada registro de dirección multicast tiene el siguiente formato (ver Figura 3-46 tomada de [29]):

- ***Record Type:*** hay diferentes tipos de registros de direcciones multicast que pueden ser incluidos en un mensaje de reporte:
  - Current State Record: es enviado por un nodo en respuesta a una consulta recibida por una interfaz. Este reporta el estado actual de escucha de la interfaz con respecto a una sola dirección multicast. Puede tener uno de los siguientes valores:
    - MODE_IS_INCLUDE (1): indica que la interfaz tiene un filtro de INCLUDE para las direcciones multicast especificadas.
    - MODE_IS_EXCLUDE (2): indica que la interfaz tiene un filtro de EXCLUDE para las direcciones multicast especificadas.
  - Filter Mode Change Record: es enviado por un nodo si cambia el filtro en la interfaz para una dirección multicast en particular. El registro es incluido en un reporte enviado desde la interfaz sobre la cual el cambio ocurrió. Este registro puede tomar uno de los siguientes valores:
    - CHANGE_TO_INCLUDE_MODE (3): indica que la interfaz a cambiado a un filtro INCLUDE para las direcciones multicast especificadas. Los campos dirección origen en este registro contiene la nueva lista de orígenes de la interfaz para la dirección multicast especificada, si no está vacía.
    - CHANGE_TO_ EXCLUDE_MODE (4): indica que la interfaz a cambiado a un filtro EXCLUDE para las direcciones multicast especificadas. Los campos dirección origen en este registro contiene la nueva lista de orígenes de la interfaz para la dirección multicast especificada, si no está vacía.
  - Source List Change Record: es enviado por un nodo si ocurre un cambio de la lista de origen. Este reporte es enviado desde la interfaz donde ocurrió el cambio. Este registro puede tomar uno de los siguientes valores:
    - ALLOW_NEW_SOURCES (5): indica que los campos dirección origen en este registro contiene una lista de orígenes adicionales que el nodo desea escuchar, para paquetes enviados a la dirección multicast especificada.
    - BLOCK_OLD_SOURCES (6): indica que los campos dirección origen en este registro contiene una lista de orígenes adicionales que el nodo no desea escuchar, para paquetes enviados a la dirección multicast especificada.

La Figura 3-47 (tomada de [81]) resume algunos aspectos principales de la interacción receptor-router sobre un enlace gobernado por MLDv2.

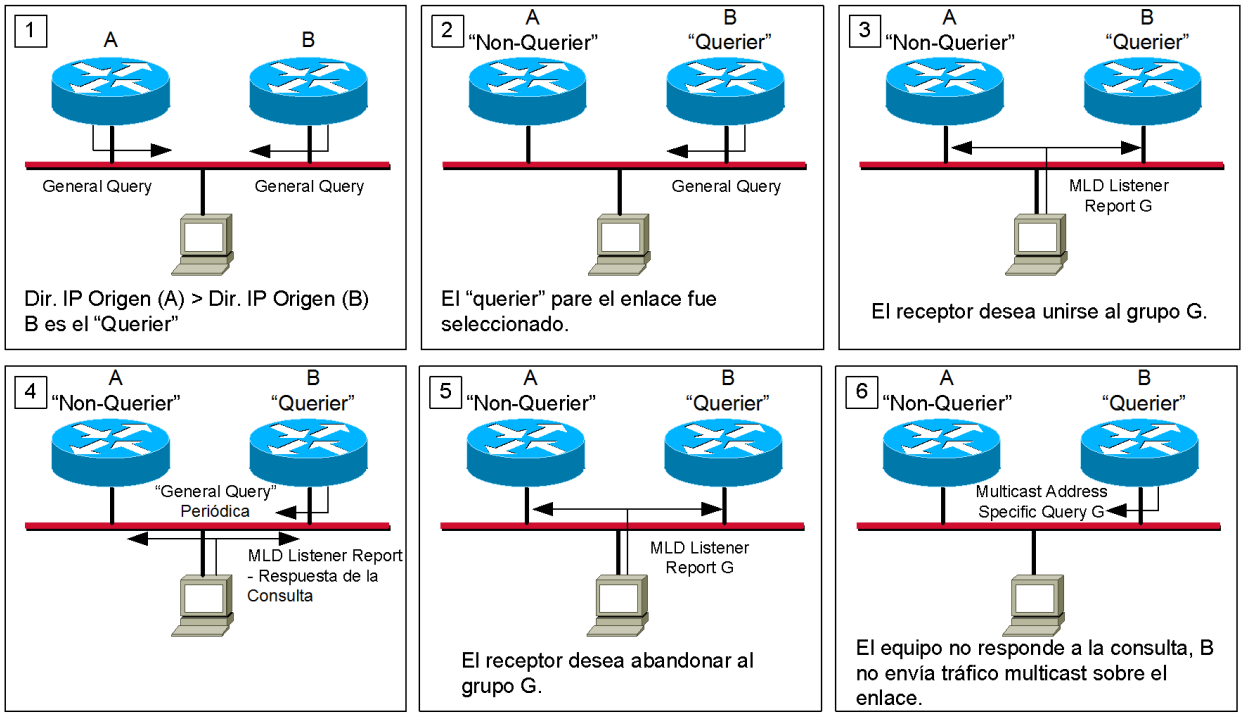

Figura 3-47: Representación de la Interacción Receptor-Router.

3.4.4. Conmutación de Tráfico Multicast en IPv6

En IPv4, los switches capa 2 pueden utilizar IGMP snooping para limitar el flujo de tráfico multicast por medio de la configuración dinámica de las interfaces capa 2, de esta manera el tráfico multicast es enviado sólo a aquellas interfaces asociadas con un dispositivo IP multicast. En IPv6, MLD snooping realiza una función similar, los datos multicast son selectivamente enviados a una lista de puertos que desean recibir los datos, en vez de ser enviados a todos los puertos en una VLAN.

MLD snooping monitorea los mensajes de Reporte MLD de un nodo a un router que pasan por un switch. En el caso de la Figura 3-48 (tomada de IPv6style[14]), el router envía Consultas MLD y el Equipo 1 (conectado en el puerto 1 del switch) responde con un Reporte MLD a G1. El switch con soporte MLD snooping envía entonces el Reporte MLD al puerto conectado al router, mientras memoriza que la dirección multicast G1 sólo debe ser enviada al puerto 1. Cuando el Equipo 1 termina su participación al grupo G1, el switch con soporte MLD snooping detiene el envío de paquetes para el grupo G1 al puerto 1.

En [64] se detallan consideraciones importantes para switches IGMP y MLD Snooping.

[14] http://www.ipv6style.jp/en/tech/20041014/index.shtml

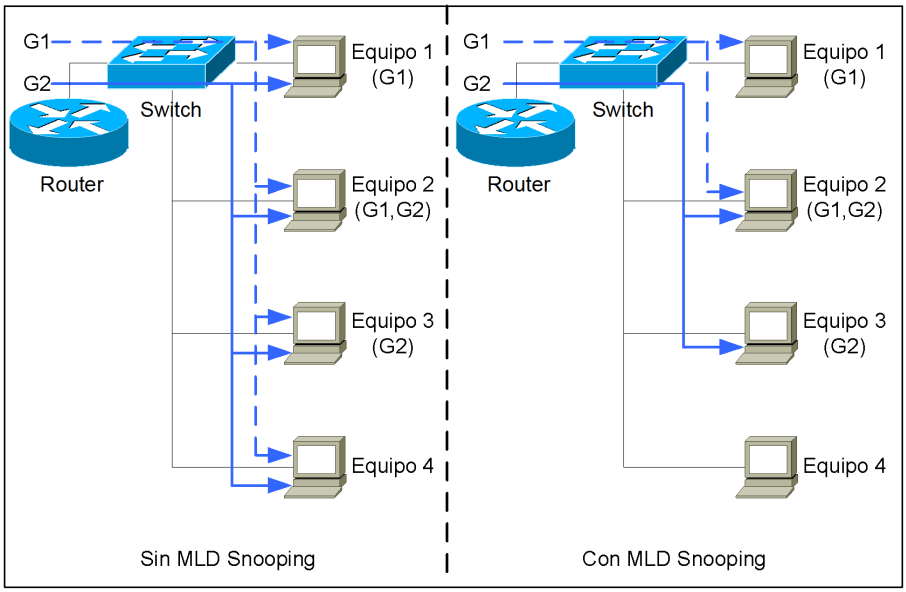

Figura 3-48: MLD Snooping.

3.4.5. Enrutamiento de Tráfico Multicast en IPv6

MLD permite a los routers aprender y administrar los receptores directamente conectados a ellos. El próximo paso en la construcción de una red multicast es permitir a los routers informarse entre ellos de los receptores interesados en un grupo multicast. Estos routers pueden construir colectivamente el camino óptimo para el tráfico multicast desde los orígenes a los receptores.

Árboles de Distribución Multicast

Un concepto fundamental del envió y enrutamiento multicast es el de los árboles de distribución multicast (Multicast Distribution Tree - MDT). Sus ramas conducen a los routers que mantienen redes que hospedan a los receptores. Así como los receptores se unen o abandonan grupos multicast, las ramas son agregadas o eliminadas del árbol multicast.

Generalmente, el camino óptimo para el tráfico multicast es el de un árbol que tiene su raíz en el origen del tráfico multicast, éste árbol es llamado de camino más corto (Shortest Path Tree - SPT), y es identificado por la tupla (S,G), donde S es la dirección del origen y G la dirección del grupo multicast (ver Figura 3-49 tomada de [81]). Todos los routers que son parte de un árbol (S,G) tienen que mantener un estado por cada par origen-grupo en la red.

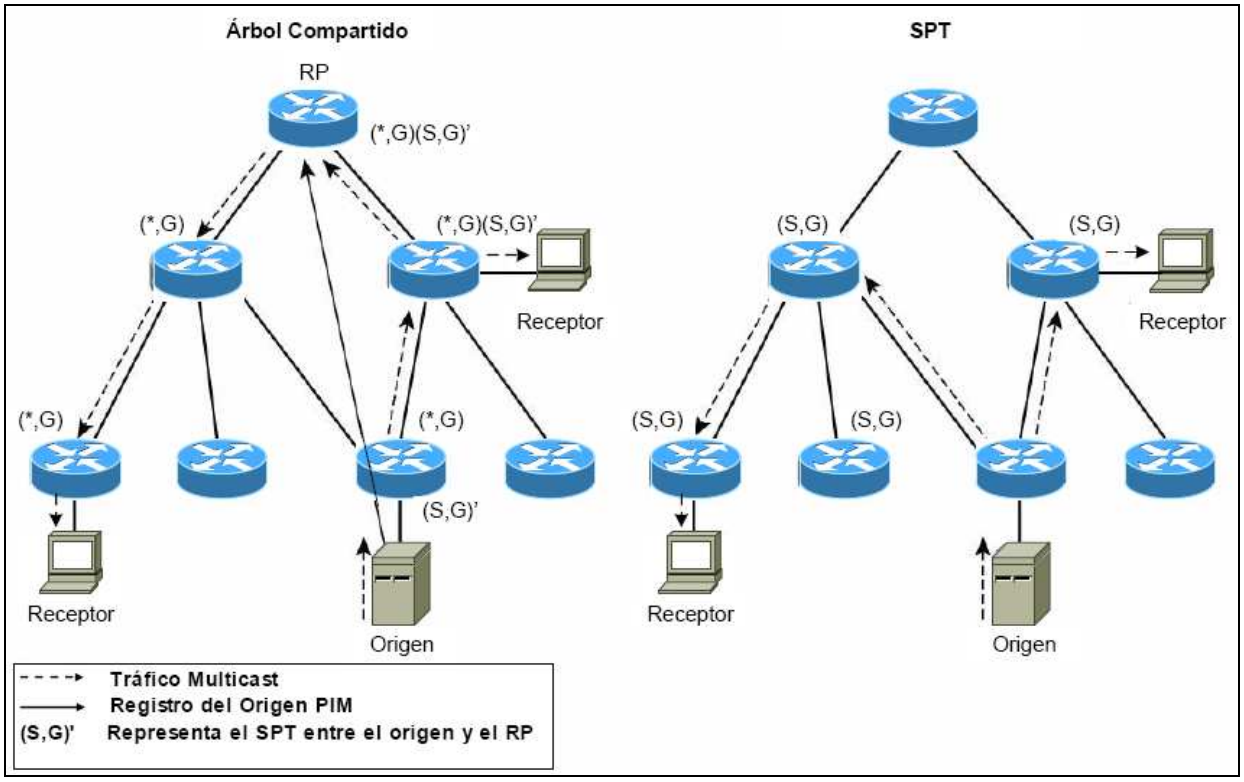

Figura 3-49: Tipos de Árboles de Distribución.

Cuando múltiples orígenes sirven al mismo G, traería ventaja compartir un árbol de distribución en común. Un árbol compartido es identificado como (*,G). El árbol compartido se origina en un router específico llamado “Punto Rendezvous” (RP, por sus siglas en inglés). Un RP está activo por cada grupo, pero el mismo RP puede manejar varios grupos. El origen se registra con el RP y su tráfico es enviado sobre un (S,G) para el RP y de allí hacia el árbol compartido.

El árbol compartido es un recurso de información común para el dominio multicast, pero no puede ser el camino más óptimo para todos los orígenes multicast. Si un router tiene receptores para un grupo dado, una vez que éste router aprende sobre el origen puede elegir cambiarse a un SPT que ofrece un envió óptimo del tráfico multicast.

Reverse-Path Forwarding (RPF)

Cualquiera sea el tipo de árbol, los mensajes de control usados para construirlo y administrarlo son siempre enviados hacia la raíz, ya sea ésta el origen del tráfico multicast o el RP, los routers necesitan encontrar el próximo salto en el camino de regreso (con respecto al flujo de tráfico multicast) hacia la raíz. El proceso de identificación de este nodo es llamado cálculo del RPF.

Para decidir la interfaz de salida para estos mensajes, un router tiene que conocer la topología de la red. Debido a que el enrutamiento multicast construye y mantiene estados sólo para árboles de distribución multicast, un router confía en los protocolos de enrutamiento unicast de las capas inferiores para la información de la topología de la red. Basado en esta información, el router ejecuta un cálculo de RPF y define la mejor interfaz hacia el RP u origen.

La siguiente información es examinada en el proceso de cálculo del RPF:

- Rutas multicast estáticas.
- Rutas BGP Multiprotocolo (MBGP) multicast.
- Información de enrutamiento unicast IPv6 almacenada en la base de información de enrutamiento (RIB, por sus siglas en inglés) y proporcionada por rutas estáticas, RIPng, EIGRP, OSPFv3 e IS-IS pero excluyendo las rutas BGP unicast.

3.4.6. Protocolos de Enrutamiento Multicast en IPv6

El enrutamiento multicast representa el proceso de construcción de los árboles de distribución multicast. La información de la topología de árbol es coleccionada y mantenida en la "Tree Information Base" (TIB). Muchos protocolo fueron desarrollados para IPv4 para soportar este proceso (DVMRP, MOSPF, CBT, PIM), todos asociados a ciertos modelos de entrega de servicios, y ciertas necesidades de aplicaciones.

Tomando la experiencia de su predecesor, IPv6 adoptó sólo tres tipos de protocolos de enrutamiento multicast:

- PIM-SM definido en [61], para aplicaciones muchos-a-muchos, donde múltiples orígenes transmiten al mismo grupo.
- PIM-SSM es un subconjunto de PIM-SM, y es usado para aplicaciones uno-a-muchos, donde un sólo origen transmite a múltiples receptores, está basado en la definición de direcciones Multicast de Origen Específico [65].
- BIDIR-PIM definido en [66], es usado para aplicaciones muchos-a-muchos, donde todos lo miembros de un grupo pueden ser tanto receptores como orígenes de tráfico multicast.

La implementación de PIM sobre IPv6 es similar a la de IPv4, los estándares de protocolos PIM son transparentes con respecto a la versión de IP. A continuación se describe con mayor detalle PIM-SM, base de las demás implementaciones.

Protocol Independent Multicast – Sparse Mode (PIM-SM)

PIM-SM es un protocolo diseñado para el enrutamiento eficiente de grupos multicast que puede abarcar a redes de área amplia (WAN). PIM-SM se dice independiente debido a que no depende de ningún protocolo de enrutamiento en particular, aunque puede usar el enrutamiento unicast de las capas inferiores para proveer la información del camino de regreso para construir el árbol multicast. PIM-SM versión 2 fue definido originalmente en forma experimental en [68] y revisado en [69], para finalmente ser propuesto como estándar en [61] en agosto del 2006.

PIM descansa en un protocolo subyacente, que recoge la topología de la red, para poblar con rutas una tabla de enrutamiento llamada "Multicast Routing Information Base" (MRIB). Las rutas en esta tabla pueden ser tomadas directamente de la tabla de enrutamiento unicast, o provista por un protocolo de enrutamiento diferente, como MBGP [70]. Indistintamente de cómo sea creada, el rol principal de la MRIB en el protocolo PIM es proveer el próximo salto a lo largo de un camino multicast para cada

subred destino. La MRIB da la información del camino de regreso e indica el camino que un paquete de dato multicast debería tomar desde su subred de origen al router que tiene la MRIB.

PIM-SM debe ser capaz de encaminar paquetes de datos desde los orígenes a los receptores sin la necesidad que los orígenes o receptores se conozcan a priori. Esto proceso es esencialmente hecho en tres fases:

- Fase 1: Árbol RP.
- Fase 2: Finalización de Registro.
- Fase 3: Árbol de la Ruta más Corta.

Estas tres fases pueden ocurrir simultáneamente, debido a que tanto los emisores como los receptores, pueden existir en cualquier momento. Antes de profundizar en cada una de estas fases, se definirán algunos términos necesarios:

Punto Rendezvous (RP): un RP es un router que ha sido configurado para ser usado como la raíz de un árbol de distribución de origen no específico para un grupo multicast. Recibe todo el tráfico desde los orígenes y lo reenvía a los receptores. Cada router PIM dentro de un dominio PIM (conjunto de routers los cuales implementan PIM y son configurados para operar dentro de un límite común) debe ser capaz de asociar una dirección de grupo multicast a un mismo RP (group-to-RP mapping). Actualmente existen 3 mecanismos para hacer esto:

- Configuración Estática: configuración manual de la dirección del RP en todos los routers PIM dentro de un mismo dominio.
- Embedded-RP: define una política de asignación de direcciones en la cual la dirección de un RP es enviada en una dirección IPv6 de grupo multicast [17].
- BootStrap Router (BSR): está basado en la elección automática de un BSR entre varios routers candidatos a RP, fue definido por primera vez en [69] y actualmente es un draft definido en [78].

Árboles Compartidos PIM: un árbol de distribución compartido especifica un camino único de envío entre una raíz en común (RP) ubicada en algún punto de la red y cada subred que contenga miembros de grupos multicast.

Router Designado (DR): en una LAN de medio compartido, como Ethernet, pueden existir múltiples routers PIM-SM. Uno de ellos debe ser elegido como el DR, que actuará como intermediario entre los equipos directamente conectados y el protocolo PIM-SM (ver Figura 3-50 tomada de [81]).

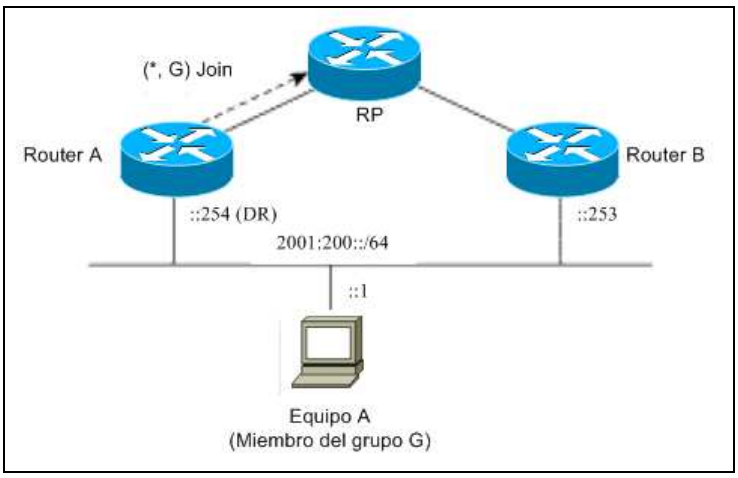

Figura 3-50: Elección del DR.

El mecanismo de elección de un DR es llevado a cabo por el envío de mensajes "Hello" entre los router PIM. Estos son enviados periódicamente y permite a los routers aprender sobre los vecinos PIM en cada una de las interfaces. Los mensajes "Hello" (ver Figura 3-51 tomada de [61]) son enviados a la dirección multicast de "Todos los Routers PIM" (FF02::D) por cada una de las interfaces con PIM habilitado en un router. En términos generales el mecanismo de elección de un DR se basa en la dirección IP y una Prioridad asignada a un router.

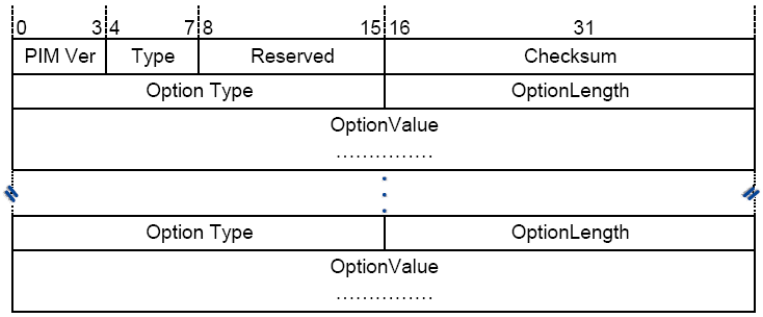

Figura 3-51: Formato de un Mensaje "Hello".

Tree Information Base (TIB): es una colección de estados de un router PIM que ha sido creado para recibir información de mensajes PIM, IGMP y MLD de equipos locales

Estados del protocolo PIM: basado en la TIB se puede determinar cuatro tipos de estados.

- Estado (*,*, RP): estado que mantiene los árboles por RP, para todos los grupos servidos por un RP dado.
- Estado (*,G): estado que mantiene el árbol RP para el grupo G.
- Estado (S, G): estado que mantiene un árbol de origen específico para un origen S y un grupo G.
- Estado (S, G, rpt): estado que mantiene información de origen específico sobre un origen S en el árbol RP para el grupo G.

Mensajes PIM de Registro: el DR local en una LAN o un enlace punto-a-punto encapsula los paquetes multicast, desde el origen al RP, para los grupos pertinentes, hasta recibir un mensaje "Register-Stop" para (S,G) o (*,G) desde el RP. Cuando el DR recibe este tipo de mensaje, mantiene un estado de "Register-Stop" (S,G) por un intervalo de tiempo limitado llamado "Register-Stop Timer". Justo antes de vencer este tiempo, el DR envía un mensaje "Null-Register" al RP para permitirle refrescar la información de "Register-Stop" al DR. Si el "Register-Stop Timer" actual expira, el DR retomará la encapsulación de paquetes del origen al RP. Los mensajes involucrados son:

- "Register": un mensaje de registro (ver Figura 3-52 tomada de [61]) es enviado por el DR al RP cuando un paquete multicast necesita ser transmitido sobre el árbol RP. La IP origen es establecida a la dirección de DR, y la dirección destino a la dirección del RP.

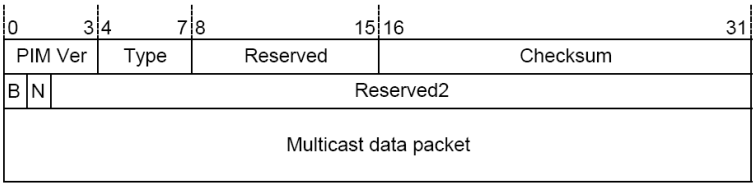

Figura 3-52: Formato de un Mensaje de Registro PIM.

- "Register-Stop": un mensaje de finalización de registro (ver Figura 3-53 tomada de [61]) es enviado por el DR al RP, para detener el envío de mensajes de registro (S, G), bien sea porque el RP comienza a recibir tráfico multicast del origen S vía SPT (S, G), o que el RP no necesite el tráfico porque no existen árboles compartidos para ese grupo.

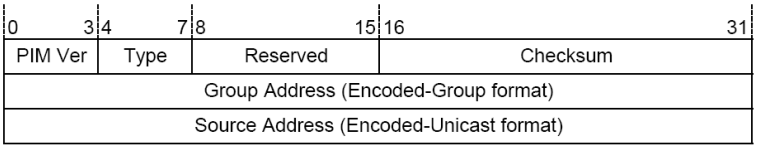

Figura 3-53: Formato de un Mensaje de Finalización de Registro PIM.

Mensajes PIM "Join/Prune": estos mensajes son enviados por lo routers hacia sus orígenes anteriores y RPs. Los mensajes "Join" o de unión son enviados para construir árboles compartidos (RPT) o árboles de origen (SPT). Los mensajes "Prune" o de eliminación son enviados para eliminar árboles de origen cuando los miembros dejan los grupos, así como para orígenes que no usan el árbol compartido. Estos mensajes consisten en una lista de grupos y una lista de orígenes unidos o eliminados para cada grupo. En general, un mensaje PIM "Join/Prune" (ver Figura 3-54 tomada de [61]) debería sólo ser aceptado si viene de un vecino PIM conocido. Si un router recibe un mensaje desde una dirección origen en particular y no ha recibido mensajes "Hello" con anterioridad desde esta dirección origen entonces el mensaje debería ser descartado sin ningún tipo de procesamiento.

- Join/Prune (*,*,RP): al recibir un mensaje "Join (*,*,RP)" el router enviará paquetes destinados a cualquier grupo manejado por el RP por la interfaz que

recibió el mensaje. Al recibir un mensaje “Prune (*,*,RP)” por una interfaz se expresa el interés en detener el envío de paquetes.

- Join/Prune (*,G): son mensajes enviados hacia el RP de un grupo específico, expresa el interés (o desinterés) de recibir el tráfico enviado al grupo G a través del árbol compartido RP.
- Join/Prune (S,G): son mensajes enviados hacia un origen especifico, expresa el interés (o desinterés) de recibir tráfico, por medio del árbol de ruta más corta, enviado por el origen al grupo especificado.
- Join/Prune (S,G,rpt): son mensajes enviados hacia el RP de un grupo específico, expresa el interés (o desinterés) de recibir tráfico, por medio del árbol compartido, enviado por el origen especificado al grupo G.

Figura 3-54: Formato de los Mensajes “Join/Prune”.

Mensajes PIM “Assert”: En redes de acceso múltiple, puede haber rutas paralelas al origen o al punto de reunión (RP). A causa de este hecho, es posible que los miembros de los grupos reciban paquetes duplicados de varios enrutadores. Para evitar el problema, PIM-SM utiliza los mensajes “Assert” (ver Figura 3-55 tomada de [61]) para determinar un retransmisor designado.

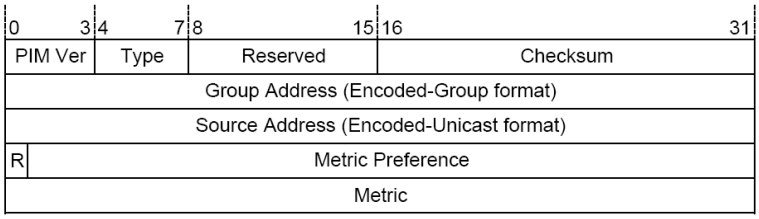

Figura 3-55: Formato de los Mensajes “Assert”.

Si todos los enrutadores ejecutan el mismo protocolo de enrutamiento unicast, el router con la mejor métrica ganará. Por ejemplo, si todos los routers utilizan RIP, se elegirá al router con la cuenta de saltos más pequeña. Si las métricas son iguales, se elegirá el router con la dirección IP más alta. Si los routers ejecutan protocolos unicast diferentes, las métricas no se pueden comparar. En este caso, el valor de prioridad de la métrica determina el router que reenviará el tráfico

Fases del Protocolo PIM-SM

Fase 1: Árbol RP

En la fase uno, un receptor multicast expresa su interés en recibir el tráfico destinado para un grupo multicast. Típicamente esto es hecho usando IGMP o MLD, pero otros mecanismos pueden también servir para este propósito. Uno de los router locales al receptor es elegido como el DR para esa subred. El DR al recibir la expresión de interés de los receptores, envía un mensaje “PIM Join (*,G)” hacia el RP para ese grupo multicast.

Este mensaje viaja salto por salto hacia el RP para ese grupo, y en cada router por el cual pasa, se insta un estado de árbol multicast para el grupo G. Eventualmente, el mensaje Join (*,G) llega a alcanzar el RP o un router que ya tiene un estado Join (*,G) para ese grupo. Cuando varios receptores se unen a un grupo multicast, estos mensaje de “PIM Join” convergen sobre el RP y forman un árbol de distribución para el grupo G que es originado en RP. Los mensajes “PIM Join” son reenviados periódicamente mientras existan receptores para ese grupo. Cuando todos lo receptores sobre una subred dejan el grupo, el DR envía un mensaje “PIM Prune (*,G)” hacia el RP para ese grupo multicast. Sin embargo, si el mensaje “Prune” no es enviado por alguna razón, el estado eventualmente expirará.

Cuando un emisor u origen de datos multicast empieza a enviar sus datos para un grupo multicast, el DR local al emisor toma esos paquetes de datos, los encapsula en paquetes unicast, y los envía directamente al RP. El RP recibe esos paquetes y los desencapsula para enviarlos sobre el árbol compartido. Los paquetes siguen el árbol multicast de estado (*,G) en los routers del árbol RP, y empiezan a ser replicados por todas las ramas del árbol RP, y eventualmente alcanza a todos los receptores para el grupo multicast. El proceso de encapsular paquetes de datos para el RP es llamado “Registro”, y los paquetes encapsulados son conocidos como paquetes de “Registro PIM”.

Al finalizar esta fase, el tráfico multicast está fluyendo en forma encapsulada al RP, y en forma nativa sobre el árbol RP a los receptores multicast.

Fase 2: Finalización del Registro.

Aunque la encapsulación en el registro puede continuar indefinidamente, el RP normalmente elegirá cambiar el envío a la forma nativa, ya que ésta encapsulación de paquetes de datos es ineficiente, debido a:

- La encapsulación y desencapsulación puede ser relativamente costosa operacionalmente para el rendimiento de router, dependiendo si tiene o no el hardware apropiado para esas tareas.
- Viajar todo el camino hacia el RP, y luego por el árbol compartido, puede resultar en paquetes viajando relativamente largas distancias para alcanzar a receptores cercanos al origen. Para algunas aplicaciones éste incremento de latencia o consumo de ancho de banda no es deseable.

Para cambiar el envió a forma nativa, cuando el RP recibe un paquete de datos encapsulada desde el origen S para el grupo G, éste normalmente iniciará un “Join” de origen específico hacia S. Este mensaje viaja salto por salto hacia S, instando un árbol multicast de estado (S,G) en los routers a lo largo del camino. El árbol multicast de estado (S,G) es usado sólo par enviar paquetes para el grupo G si estos paquetes vienen del origen S. Eventualmente el mensaje de “Join” alcanza alguna subred de S o un router que ya tiene un árbol multicast de estado (S,G), y entonces el paquete desde S empieza a fluir siguiendo el árbol de estado (S,G) hacia el RP. Estos paquetes de datos pueden también alcanzar routers con estado (*,G) a lo largo del camino hacia el RP, si esto es así, ellos pueden cortar camino sobre el árbol RP en este punto.

Mientras el RP está en el proceso de unión al árbol de origen especifico para S, los paquetes de datos continuarán siendo encapsulados al RP. Cuando los paquetes desde S empiezan a llegar en forma nativa al RP, el RP recibirá dos copias de cada unos de los paquetes. En este punto, el RP empieza a descartar las copias encapsuladas, y envía un mensaje “Register-Stop” (finalización de registro) hacia el DR de S para prevenir la encapsulación de tráfico innecesariamente.

Al finalizar la fase 2, el tráfico fluirá nativamente desde S a lo largo del árbol de origen específico al RP, y desde allí a lo largo del árbol compartido hacia los receptores. Un emisor u origen pueden empezar a enviar datos antes de que los receptores se unan al grupo, por lo que la fase dos puede suceder antes de que el árbol compartido hacia los receptores esté construido.

Fase 3: Árbol de la Ruta más Corta

Aunque la eliminación de la encapsulación entre el origen y el RP disminuye la sobrecarga de procesamiento, esto no optimiza completamente las rutas de envío. Para muchos receptores, la ruta vía el RP puede envolver una significativa desviación cuando se compara con la ruta más corta desde el origen a los receptores.

Para obtener latencias bajas o utilización del ancho de banda más eficiente, un router en la LAN del receptor, típicamente el DR, puede opcionalmente iniciar una transferencia desde el árbol compartido a un árbol de ruta más corta (SPT) de origen

específico. Para hacer esto, el router emite un “Join (S,G)” hacia S que insta un estado en los routers a lo largo del camino hacia S. Eventualmente, este mensaje “Join (S,G)” alcanza una subred de S o un router con un estado (S,G). Cuando esto sucede, los paquetes de datos desde S empiezan a fluir siguiendo el estado (S,G) hasta alcanzar al receptor.

En este punto, el receptor (o router anterior al receptor) recibirá dos copias de los datos, uno desde el SPT y otro desde el RPT. Cuando el primer tráfico empieza a llegar desde el SPT, el DR o router anterior al receptor empieza a rechazar los paquetes para G desde S que llegan vía el árbol RP. En adición, el DR envía un mensaje “Prune (S,G)” hacia el RP, conocido como mensaje “Prune (S,G,rpt)”. Este mensaje viaja salto por salto, instando el estado a lo largo de la ruta hacia el RP indicando que el tráfico de S para G no debería ser enviado en esa dirección. Este mensaje es propagado hasta alcanzar al RP o un router que aun necesite tráfico desde S para otros receptores.

En este momento, el receptor sólo recibirá tráfico desde S a lo largo del árbol de camino más corto entre el receptor y S. Además, el RP está recibiendo el tráfico desde S, pero este tráfico no alcanza a estos receptores por medio del árbol RP. Así que desde lo que concierne al receptor, este es el final del árbol de distribución.

3.5. Antecedentes

A principios de los años 90, la mayoría de los routers de Internet no sabían manejar tráfico multicast. Muchos routers eran configurados para mover paquetes unicast del Protocolo Internet (IP), información que tenia un solo y simple destino.

Las empresas manufactureras en un principio no querían invertir en el desarrollo de equipos que soportaran multicast, hasta que probaran la necesidad de los mismos.

En 1992, algunos emprendedores en la IETF (Internet Engineering Task Force) decidieron que lo que no podría hacerse en hardware, ellos lo harían en software. Por tal motivo crearon una “red virtual” (una red que corría sobre Internet) y escribieron un software que permitiera a los paquetes multicast atravesar la red. Este software no sólo envió datos a un sólo nodo de Internet, sino a varios nodos. De esta manera, nació MBone.

3.5.1. MBone

MBone (Multicast backBONE) es llamada una “red virtual” debido a que comparte el mismo medio físico (cables, routers y otros equipos) de Internet. MBone permite a los paquetes multicast viajar a través de los routers que están configurados para manejar sólo tráfico unicast. El esquema utilizado por MBone para transportar paquetes multicast sobre paquetes unicast es llamado “tunneling”.

Esta red (ver Figura 3-56 tomada de Steve Casner[15], 1994) se ha empleado mayoritariamente para el estudio de herramientas de audio/vídeo en conferencias multipunto, aunque en principio puede ser empleada para el intercambio de cualquier

[15] http://www.mbone.cl.cam.ac.uk/mbone/mbone-topology.html

tipo de información multimedia. Su principal ventaja, o característica, es la de proporcionar el intercambio de información de uno a muchos, pero sin los inconvenientes de tener que duplicar dicha información para cada uno de los receptores y en función del número de ellos.

MBone fue creada como una red experimental (y temporal), que eventualmente debería existir hasta cuando las características de enrutamiento multicast sean un estándar para los routers en Internet.

Pese a que el panorama ha cambiado rápidamente y que un gran número de ingenieros, tanto de empresas privadas como pertenecientes al ámbito académico y/o investigador, se han esforzando conjuntamente para convertir este experimento global en un servicio operativo, aun existen ciertas complicaciones que apuntan a que MBone seguirá siendo, por el momento, una red experimental en Internet. Esto debido a que MBone es principalmente “red virtual”; una red creada como la unión de múltiples “islas” interconectadas entre sí, la mayor parte de equipos de comunicaciones que interconectan la infinidad de redes que forman Internet aun no hablan el lenguaje del MBone, es decir, el IP multicast, o lo hacen de forma incompatible con otros. Por otro lado la comercialización de routers multicast ha sido difícil debido a que no hay capacidades eficientes de control de acceso a los árboles multicast (routers multicast y sus protocolos), y debido también a que los Proveedores de Servicios de Internet (Internet Service Provider - ISP) tienen dificultades en calcular cargos por tráfico multicast.

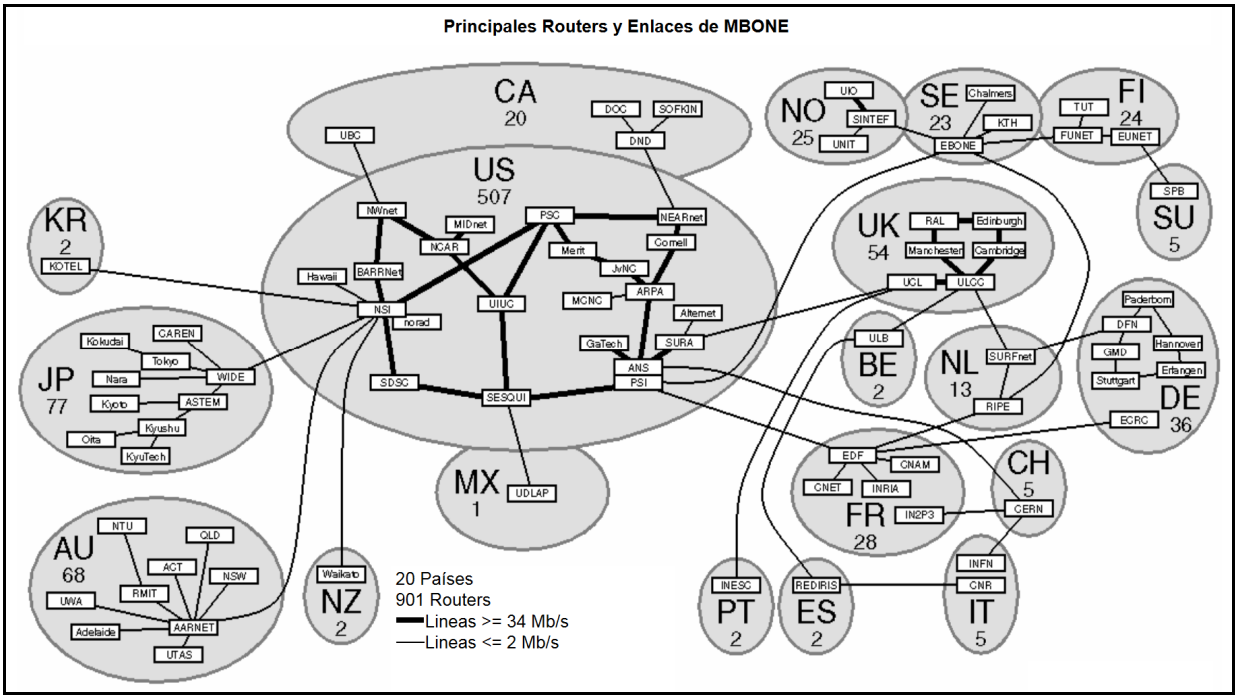

Figura 3-56: Topología de Red de MBone en 1994.

MBone está actualmente para el uso práctico de comunicaciones compartidas como la videoconferencia o ambientes de colaboración compartidos. Generalmente no conectados a ISPs, sino a universidades e institutos de investigación. Algunos

proyectos y redes de pruebas, tales como la de Internet2, ya han abandonado su conectividad con MBone.

MBone nació con DVMRP como su primer protocolo de enrutamiento multicast, y tras de él surgieron otros como MOSPF, PIM-DM, CBT y PIM-SM, entre otros. PIM-SM fue el protocolo que terminó prevaleciendo debido a que se adapta mucho mejor a sistemas con muchas subredes o ramas del árbol, y pocos usuarios en cada rama. Por otro lado, IGMP también ha ido madurando a lo largo de 3 versiones.

Para mayor información sobre MBone se puede consultar la página del Grupo de Trabajo[16] (WG) que le da seguimiento.

3.5.2. M6Bone

M6Bone[17] es un servicio de pruebas para multicast sobre IPv6, está dirigido a ofrecer una conectividad IPv6 multicast a los sitios interesados. Su principal objetivo es desarrollar un servicio avanzado sobre IPv6, con el fin de participar en la promoción del protocolo. Esto hace posible el uso de herramientas de video conferencias multicast en la red. El proyecto se inició en julio del 2001, con el soporte de la asociación Aristote[18], del grupo G6[19] (grupo francés de probadores de IPv6) y RENATER[20].

M6Bone es una red de túneles cuyos equipos bordes soportan IPv6 multicast. Estos túneles pueden ser:

- IPv6 multicast sobre IPv6 unicast.
- IPv6 multicast sobre IPv4 unicast.
- IPv6 multicast sobre GRE [73].

En un principio, cuando empezó el proyecto, muy pocos routers implementaban IPv6 multicast, por lo que una topología diferente a la de unicast IPv6 fue necesaria. Se dedicaron equipos (estaciones de trabajo con FreeBSD[21] y la pila Kame[22]) con IPv6 multicast, que al comienzo sólo conectaban túneles IPv6 sobre IPv6 o IPv6 sobre IPv4. Tampoco se implementó MSDP [74], por lo que M6Bone fue un sólo dominio PIM hasta que se desarrollo “embedded RP” [17]. El protocolo intra-dominio usado en M6Bone es PIM-SM [61].

Existen varios RP configurados en la red que pueden ser utilizados por la comunidad. Inicialmente no se implementaron las tablas de enrutamiento multicast, PIM-SM utilizaba las tablas de enrutamiento unicast para los chequeos RPF. Estas tablas de enrutamiento unicast eran pobladas utilizando RIPng [31]. Una vez implementadas las tablas de enrutamiento multicast, estas eran pobladas usando rutas multicast estáticas o MBGP [70].

[16] http://www.ietf.org/html.charters/mboned-charter.html
[17] http://www.6bone.net
[18] http://www.aristote.asso.fr
[19] http://www.g6.asso.fr
[20] http://www.renater.fr
[21] http://www.freebsd.org
[22] http://www.kame.net

La topología actual de M6Bone se puede observar en la Figura 3-57 (tomada de M6bone).

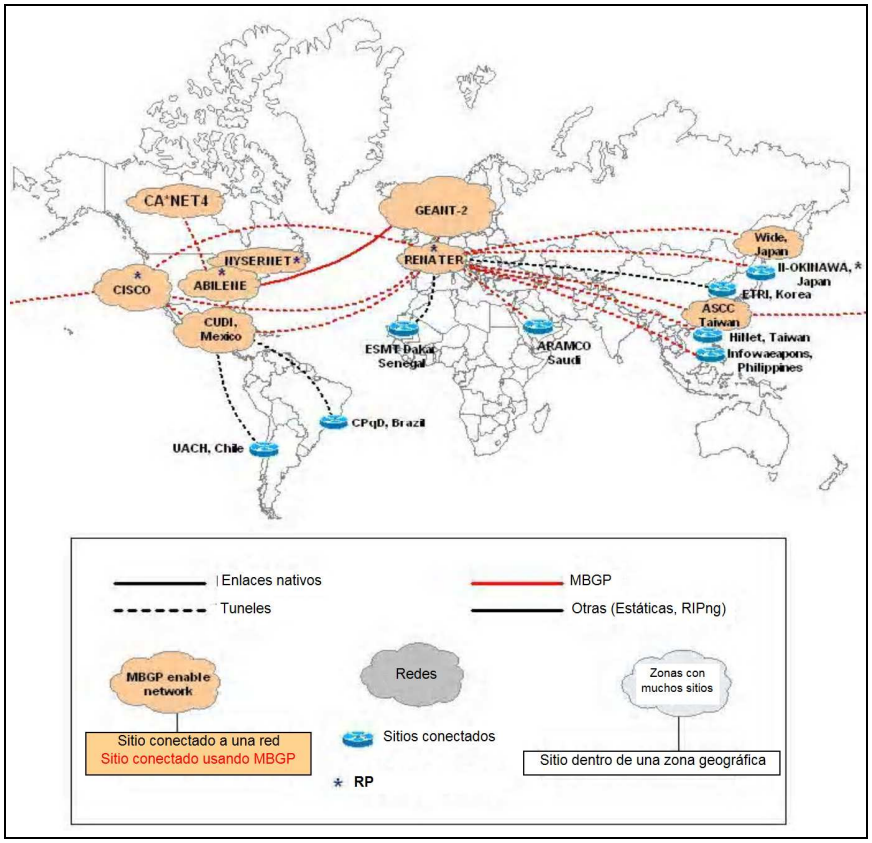

Figura 3-57: Topología Global de M6Bone.

Aplicaciones y Herramientas

Muchas aplicaciones que se iniciaron en MBone, se adaptaron para continuar trabajando con multicast sobre IPv6, otras surgieron bajo la plataforma de M6Bone. A continuación nombramos algunas de ellas:

- RAT(Robust Audio Tool): es una aplicación de código abierto de conferencias y flujo (streaming) de audio que permite a los usuarios participar en conferencias sobre Internet. Esto puede ser entre dos participantes directamente, o entre un grupo de participantes en un grupo multicast en común. RAT (ver Figura 3-58 tomada de UCL - Departamento de Ciencias de la Computación[23]) no requiere características especiales para comunicaciones punto-a-punto, sólo una conexión a la red y una tarjeta de sonido. Para conferencias multipartes RAT usa multicast y de allí todos los participantes deben residir en una red multicast. RAT está basada en estándares IETF, usando RTP [72] usando UDP/IP como protocolo de transporte. RAT está disponible para entornos Linux y Windows XP, así como para FreeBSD, HP-UX, IRIX, NetBSD, Solaris, SunOS y Windows 95/NT. Incluye una actualización para trabajar con IPv6.

[23] http://mediatools.cs.ucl.ac.uk/nets/mmedia/wiki/RatWiki

Figura 3-58: Interfaz gráfica de RAT.

- VAT6 (Visual Audio Tool con soporte IPv6): es una aplicación multimedia de audio conferencia multiparte en tiempo real sobre Internet. Está basado en [72] desarrollado por la IETF. Aunque VAT6 puede ejecutarse para conexiones unicast punto-a-punto, está diseñada principalmente para aflicciones de conferencia multiparte. Para hacer uso de las capacidades de conferencia, el sistema que lo hospede debe soportar multicast, e idealmente estar conectada a una red multicast como MBone. VAT6 provee sólo la porción de audio de una conferencia multimedia; las herramientas de video, pizarra electrónica y control de sesiones son implementadas en aplicaciones separadas.
- VideoLAN: es una solución completa de software para video "streaming", desarrollado por estudiantes de Ecole Centrale Paris y desarrollado bajo licencia GPL. VideoLAN está diseñado para el "streaming" de videos MPEG [75] en redes de gran ancho de banda. La solución de VideoLAN (ver Figura 3-59 tomada de VideoLAN[24]) incluye:

    - VLS (VideoLAN Server): trabaja con flujos MPEG-1, MPEG-2 y MPEG-4, DVDs, canales digitales satelitales, canales de televisión digital terrestres y video en vivo sobre redes unicast y multicast.
    - VLC (VideoLAN Client): puede ser usado como un servidor de "streaming" para archivos MPEG-1, MPEG-2 y MPEG-4, DVDs y video en vivo sobre redes unicast y multicast; o usado como un cliente para recibir, decodificar y mostrar flujos MPEG bajo múltiples sistemas operativos.

[24] http://www.videolan.org/vlc/streaming.html

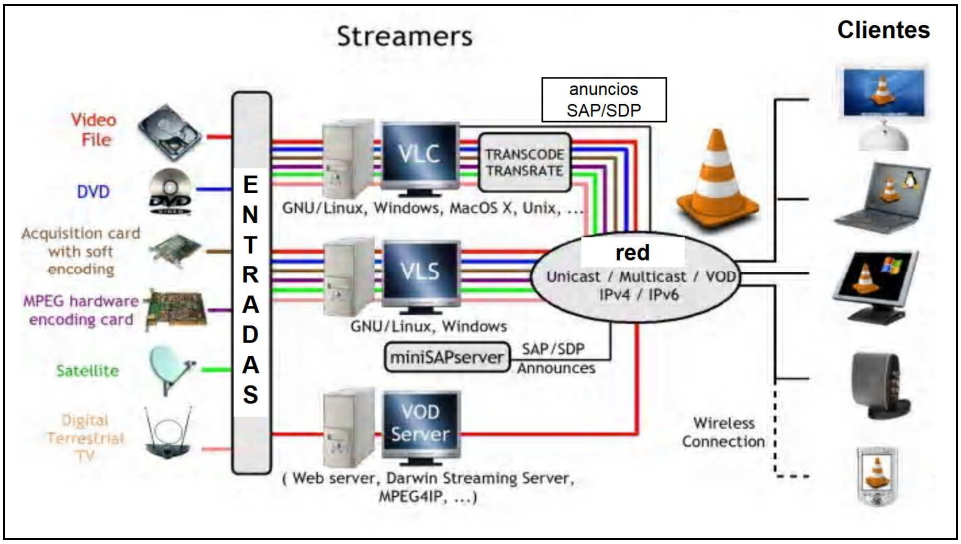

Figura 3-59: Solución Streaming de VideoLAN.

- Radio Surge: la estación estudiantil de la Universidad de Southampton ofrece "streaming" IPv6 de su contenido. Surge está conectado a la Red 6net[25] usando un túnel sobre la red IPv4 universitaria de la Escuela de Electrónica y Ciencias de la Computación. Surge cambió su servicio de "streaming" de un sistema Shoutcast[26] basado sólo IPv4 a una configuración dual basada en Icecast2[27] y Darkice[28] (ver Figura 3-60 tomada de Surge[29]). Darkice codifica el audio a formato MPEG y Ogg Vorbis[30] y se lo envía a Icecast2 usando la dirección IPv6 localhost (::1). Icecast2 acepta las peticiones HTTP de los clientes y envía un "stream" de audio de la opción elegida. Aunque en estos momentos no tiene soporte multicast, ofrece éste servicio usando "pcm6cast"[31], una herramienta desarrollada para transmitir y recibir ráfagas de audio PCM usando RTP sobre IPv6 multicast

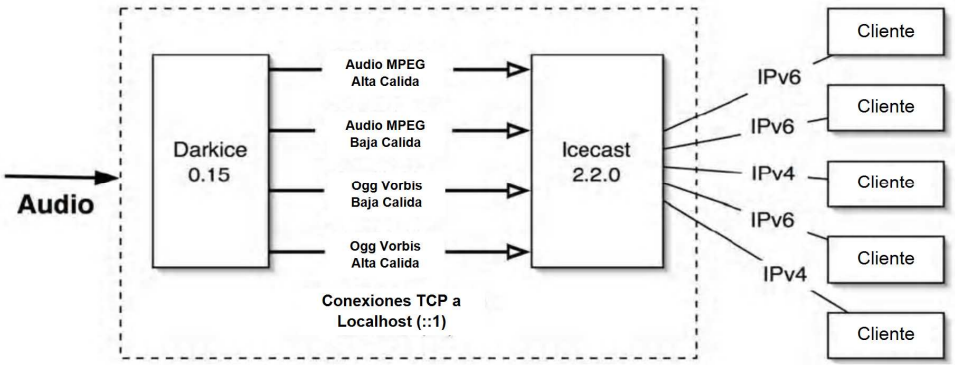

Figura 3-60: Servicio de Streaming Unicast.

[25] http://www.6net.org
[26] http://shoutcast.com/support/docs
[27] http://www.icecast.org
[28] http://darkice.tyrell.hu
[29] http://www.surgeradio.co.uk/onair/listen/advanced.html
[30] http://xiph.org/vorbis
[31] http://users.ecs.soton.ac.uk/njh/pcm6cast

- Radio Virgen: la Universidad de Southampton[32] y la estación de Radio Virgin[33] en UK configuraron un servidor con Linux 2.6 y Icecast2. Este servidor actúa como un intermediario, recibe varios “streaming” de audio de la radio Virgin, y los clientes los escuchan por conexiones IPv6 (ver Figura 3-61 tomada 6net[34]).

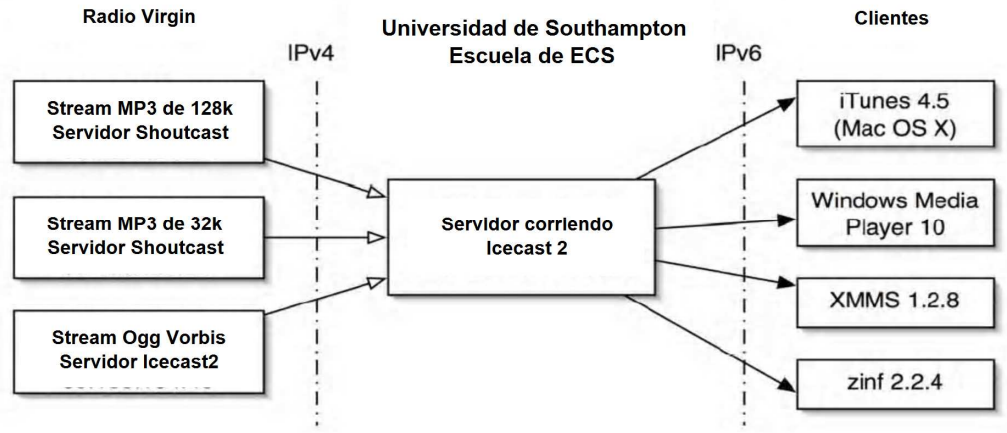

Figura 3-61: Servicio de Streaming de Radio Virgin.

[32] http://www.soton.ac.uk
[33] http://www.ipv6.ecs.soton.ac.uk/virginradio
[34] http://www.6net.org/publications/deliverables/D5.15.pdf

4. Marco Metodológico

La propuesta de implementación del servicio de hilos musicales sobre IPv6 multicast sigue una metodología que se regirá por las siguientes etapas:

- Estudio de la red actual de la UCV: consiste en el levantamiento de información de los dispositivos y componentes de red que conforman la plataforma actual de comunicación de la UCV.
- Definición de una infraestructura para un servicio multicast: a partir de los requerimientos mínimos para una infraestructura multicast sobre IPv6, se definen los equipos, enlaces de comunicación, protocolos y cualquier otro componente necesario.
- Diseño de un ambiente de pruebas: en base a la infraestructura actual de la red de la UCV, los componentes de red necesarios para servicios multicast y los equipos disponibles en el laboratorio, se propone una infraestructura de pruebas para la implementación del servicio de hilos musicales sobre IPv6.
- Implementación del ambiente de pruebas: se realizarán las configuraciones necesarias en los equipos de comunicaciones para el uso de la tecnología multicast y la de un servicio de hilos musicales sobre IPv6.

4.1. Red Actual de la Universidad Central de Venezuela

La red de datos de la Universidad Central de Venezuela (UCV) se encuentra en un proceso de adecuación y actualización tecnológica desde el año 2008, esto con el fin de obtener un red capaz de soportar la transmisión de voz, datos y video de alto desempeño, así como ofrecer un mejor servicio a todos los usuarios de la comunidad universitaria.

Según la Msc. Neudith Morales [87], coordinadora de la Dirección de Tecnología de Información y Comunicaciones de la UCV, el proceso de adecuación se basó en el diseño de una red con un backbone redundante capaz de soportar nuevas tecnologías, como QoS, a la vez que se incrementará el ancho de banda de los enlaces que parten del backbone hacia los usuarios; manteniendo siempre una estructura jerárquica y modular que permita la escalabilidad de la plataforma y facilite la detección y solución de fallas. Los componentes fundamentales de la estructura jerárquica mencionada son: el nivel de acceso, el nivel de distribución y el nivel núcleo de la red.

Las interfaces del nivel de acceso, en donde se encuentra a los dispositivos finales, tales como, estaciones de trabajo, impresoras y teléfonos IP; proveen acceso al resto de la red. El nivel de acceso puede incluir switches, puentes, concentradores y puntos de acceso inalámbrico. El objetivo principal del nivel de acceso es facilitar la conexión de los dispositivos finales a la red y controlar cuales dispositivos pueden comunicarse en la red. El nivel de distribución reúne la data recibida de los switches del nivel de acceso antes de transmitirla al nivel núcleo para el enrutamiento a su destino final. El nivel de distribución controla el flujo de la red usando políticas y delimitando dominios de difusión realizando funciones de enrutamiento entre VLANs. Finalmente, en una estructura jerárquica, el nivel del núcleo es el backbone de alta velocidad de la red,

provee conectividad entre los dispositivos del nivel de distribución, por lo que es importante para el núcleo contar con alta disponibilidad y redundancia en su estructura.

Para la fase de actualización tecnológica se plantea sustituir la mayor parte de los antiguos concentradores y switches de la red de datos de la Universidad por nuevos modelos que soporten mayores velocidades y la prestación de nuevos servicios (QoS, seguridad, VLANs, entre otros). Estos nuevos equipos estarán ubicados en los niveles de acceso, distribución y núcleo.

Hasta el momento del desarrollo de este trabajo, el núcleo de la red de datos de la Universidad estaba conformado por cuatros nodos: Principal, Ingeniería, Medicina y Ciencias; cada uno de estos nodos está ubicado físicamente en la facultad correspondiente con el nombre del mismo a excepción de Principal que se encuentra en el Rectorado. A cada unos de estos nodos se encuentran conectados una serie de subnodos que forman el nivel de distribución, luego a estos subnodos se conectan los switches y concentradores que dan acceso a los usuarios a la red (ver Figura 4-1 realizado por Antonio Sánchez).

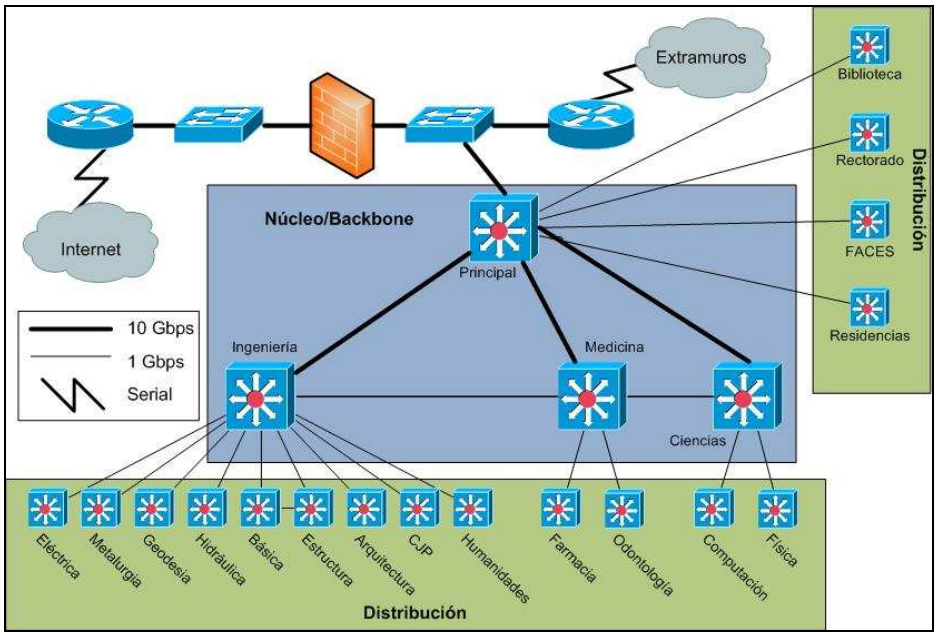

Figura 4-1: Infraestructura de Red de la UCV

4.2. Definición de una Infraestructura para un Servicio Multicast

El despliegue de una red multicast requiere de tres elementos importantes: la aplicación, la infraestructura de red y los dispositivos clientes. A continuación se describen cada uno de ellos en el contexto de esta investigación.

4.2.1. Aplicación

Para difundir el flujo de datos de audio se necesita una aplicación servidor capaz de manejar algún formato conocido, tal como: MPEGs, AAC, WMA, Real Audio, Vorbis, entre otros; además debe ser capaz de soportar IPv6 y multicast.

Hoy en día existen varias aplicaciones para el envío de flujos o "streaming" de datos multimedia (Multimedia Streaming), sobre una red IPv4 (Helix Server[35], QuickTime Streaming Server[36], Windows Media Service[37], VideoLAN VLC[38]), pero no todos soportan IPv6. Al discernir entre aquellas aplicaciones con soporte IPv6, se puede observar que no todas implementan multicast, dejando un grupo aun más reducido de aplicaciones disponibles tales como Helix Server, Windows Media Service y VideoLAN VLC.

Helix Server es una solución de software para la entrega de contenido streaming de audio y video a equipos PC o dispositivos móviles. Soporta diversas plataformas tales como Linux RHEL 4.0, Windows 2003 y Solaris 10, también la entrega en vivo o a demanda de múltiples formatos que incluyen Real Media, Windows Media, QuickTime, MP3, H.264, ACC, entre otros.

En su versión comercial, Helix Server está disponible en tres capacidades: 25 flujos, 100 flujos e ilimitado. En su versión gratuita, denominada Helix DNA Server, se distribuye bajo dos modalidades: RPSL (RealNetworks Public Source License) y RCSL (RealNetworks Community Source License).

En la Tabla 4-1, se muestran algunas características de estas versiones (tomada de la Comunidad Helix[39]).

Características	Helix DNA Server		Helix Server
	RPSL	RCSL	
Transporte y protocolo de flujo estándar en la industria	X	X	X
Difusión en vivo y a demanda	X	X	X
Sistema de administración, monitoreo y autenticación	X	X	X
Extensible con APIs estándar de la industria	X	X	X
Soporte MP3	X	X	X
Soporte RealAudio/RealVideo		X	X
IPv6	X	X	X
Detección automática de ancho de banda	X	X	X
Soporte de formatos universales (Ej.:WM, QT, MPEG-4)			X
Distribución de contenido inteligente de ancho de banda			X
Sistema de redundancia			X
Soporte al cliente vía telefónica, actualizaciones			X

Tabla 4-1: Comparación versiones Helix Server/Helix DNA Server.

[35] http://www.realnetworks.com/products/media_delivery.html
[36] http://www.apple.com/quicktime/streamingserver
[37] http://www.microsoft.com/windows/windowsmedia/forpros/serve/prodinfo.aspx
[38] http://www.videolan.org
[39] https://helix-server.helixcommunity.org/2006/devdocs/helix_server_comparision

Microsoft Windows Media Service (WMS) 9, que viene con los sistemas operativos Windows Server 2003, es una plataforma empresarial para el streaming en vivo o a demanda de contenidos de audio o video sobre Internet o una Intranet. Con WMS se puede configurar y administrar uno o más Servidores de Windows Media para la entrega de contenido a los clientes. Soporta los formatos de Windows Media, JPEG y MP3.

En adición al streaming, WMS tiene la habilidad de hacer caché y almacenar flujos de datos, solicitar autenticación, imponer varios limites de conexión, restringir acceso, usar múltiples protocolos, generar estadísticas de uso, entre otras. Puede manejar un alto número de conexiones concurrentes, soporta streaming unicast y multicast, es compatible con diversos clientes tales como Windows Media Player, VLC, MPlayer, entre otros.

La versión de WMS 2008, para Windows Server 2008, incluye un complemento de Cache/Proxy el cual puede ser usado para configurar servidores de Windows Media como Cache/Proxy o Proxy Reverso.

En la Tabla 4-2 se muestran algunas características de las versiones antes mencionadas (tomada de la Microsoft[40]).

Características	Windows Server			
	2003		2008	
	Standar	Enterprise/ DataCenter	Standar/ Web Server	Enterprise/ DataCenter
Inicio rápido avanzado		X	X	X
Avance rápido y rebobinado avanzado		X		X
Inicio automático de difusión	X	X	X	X
Compatibilidad con servidores de anuncio	X	X	X	X
Compatibilidad con servidores cache/proxy		X	X	X
Caché rápida	X	X	X	X
Reconexión rápida	X	X	X	X
Recuperación rápida		X	X	X
Método de autenticación Internet (Digest)		X	X	X
Compatibilidad con IGMPv3		X	X	X
Compatibilidad con IPv6	X	X	X	X
Entrega de contenido multicast		X		X
Compatibilidad con varios protocolos de control (MMS, HTTP, RTSP)	X	X	X	X
Compatibilidad con varios analizadores de multimedia (Windows Media, MP3)	X	X	X	X
Reproducir durante archivado		X	X	X
Entrega de contenido de unicast	X	X	X	X

Tabla 4-2: Comparación versiones Windows Media Service.

[40] http://www.microsoft.com/windows/windowsmedia/forpros/server/version.aspx

El proyecto VideoLAN fue iniciado en 1996, por estudiantes de Ecole Centrale Paris, como un proyecto de la Escuela de Ingeniería. La idea era ver televisión en PCs, y a su vez justificar la actualización de la red de Ecole Centrale Paris con una aplicación que necesitara el uso intensivo del ancho de banda.

Estos estudiantes empezaron escribiendo VLS (VideoLAN Server) y VLC (VideoLAN Client) como servidor y cliente de flujos MPEG-2, respectivamente. Estos dos programas se desarrollaron en forma modular, lo cual originó un núcleo conformado básicamente por funciones de comunicación utilizados por los módulos que permitió una fácil adaptación a distintos sistemas operativos.

Hoy en día VLC es un "reproductor multimedia altamente portable para varios formatos de audio y video (MPEG-1, MPEG-2, MPEG-4, DivX, MP3, ogg, etc.) así como de CDs., VCDs, y varios protocolos de streaming, además, puede ser usado como servidor de streaming unicast o multicast en una red IPv4/IPv6 de alto ancho de banda."

Junto con VLC se cuenta con una herramienta denominada VLMa[41] (VideoLAN Manager), una aplicación para administrar múltiples flujos de datos con una sola instancia de VLC, con una interfaz Web que utiliza tecnología Java.

En la Tabla 4-3 se muestran algunas características de las versiones antes mencionadas (tomada de VideoLAN[42]).

Características	VLS	VLC
Medios de entrada		
Unicast UDP/RTP		**X**
Multicast UDP/RTP		**X**
HTTP/FTP		**X**
MMS		**X**
TCP/RTP Unicast		**X**
Archivo	**X**	**X**
Video DVD	**X**	**X**
Video CD/DVD		**X**
Codificación MPEG	**X**	**X**
Formatos de Entrada		
MPEG (ES, PS, TS, PVA, MP3)		**X**
MPEG (sólo PS y TS)	**X**	
AVI		**X**
ASF/WMV/WMA		**X**
MP4/MOV/3GP		**X**
WAV		**X**
DTS, AAC, AC3/A52		**X**
FLV		**X**
Medios de Salida		
RTP/UDP	**X**	**X**

[41] http://www.videolan.org/vlma
[42] http://www.videolan.org/streaming-features.html

RTSP		**X**
Multicast	**X**	**X**
Archivo	**X**	**X**
HTTP		**X**
Formatos de Salida		
PS, TS, Ogg, ASF, MP4, QuickTime		**X**
Sólo TS	**X**	
Misceláneos		
Anuncios SAP/SDP	**X**	**X**
Soporte protocolo Bonjour		**X**
IGMPv3		**X**
IPv6	**X**	**X**
MLDv2		**X**

Tabla 4-3: Comparación versiones VLC y VLS.

Cualquiera de las tres aplicaciones antes descritas puede ser elegida como servidor de streaming para esta investigación. Por tal motivo se diseño una tabla comparativa (ver Tabla 4-4) que nos ayude a seleccionar el indicado para este trabajo. A cada característica (ver Tabla 4-5) se le asignó un peso: 0, 1, 2 ó 3, correspondiente a no aplica, regular, bueno o muy bueno, respectivamente.

Característica	VLC VideoLAN	Helix Server	Windows Media Service 9
Facilidad de Instalación	2	1	3
Facilidad de Configuración	1	3	3
Facilidad de Administración	1	3	3
Soporte IPv6	3	3	3
Soporte Multicast sobre IPv4	3	3	3
Soporte Multicast sobre IPv6	3	0	3
Código Abierto	3	0	0
Documentación	2	3	2
Formatos de Entrada	3	1	1
Formatos Soportados	3	1	1
Seguridad	1	2	3
Redundancia de Servidores	1	3	3
Soporte MLD	3	0	3
Total	**29**	**23**	**31**

Tabla 4-4: Comparación entre Aplicaciones de Streaming.

En base al cuadro comparativo anterior se definió que para esta investigación se utilizará como servidor de streaming el Windows Media Service 9.

Característica	Definición
Facilidad de Instalación	Provee de una aplicación que por medio de un asistente guie durante el proceso de instalación.
Facilidad de Configuración	Provee asistentes que guien durante el proceso de configuración. La configuración se realiza por medio de ventanas descriptivas.
Facilidad de Administración	Provee asistentes de configuración, reportes y mecanismo de detección de fallas por medio de ventanas y menús.
Sopote IPv6	Provee soporte de la pila TCP/IPv6.
Soporte Multicast sobre IPv4	Provee soporte para Multicast con la pila TCP/IPv4.
Soporte Multicast sobre IPv6	Provee soporte para Multicast con la pila TCP/IPv6.
Código Abierto	El software es distribuido y desarrollado libremente.
Documentación	La documentación para la instalación, configuración y administración es abundante y fácil de encontrar.
Formatos de Entrada	Soporte de varios formatos (MPEG, AVI, MP4, OGG, Real, FLV, etc.) de entrada al servidor para distribuir posteriormente.
Formatos Soportados	Formatos de audio (MP3, AAC, DTS, WMA, etc.) que puede distribuir o reproducir.
Seguridad	Provee mecanismos de autenticación y autorización.
Redundancia de Servidores	Permite configuraciones en cluster o de distribución de cargas.
Soporte MLD	Provee soporte del protocolo MLDv1/MLDv2

Tabla 4-5: Definición de Características.

Windows Media Services 9 (WMS9)

Un sistema de streaming basado en tecnologías de Windows Media consiste de 5 elementos:

- Servidor de Codificación (Windows Media Encoder): convierte contenido de audio y video en vivo al formato de Windows Media.
- Servidor de Servicios de Windows Media (Windows Media Services): encargado de distribuir el contenido por una red o por Internet.
- Servidor Web: presentación de los contenidos multimedia disponibles.
- Servidor de Archivos: repositorio del contenido pregrabado.
- Clientes: usuarios finales receptores del contenido.

En la Figura 4-2 (tomada de Microsoft[43]) se muestra un escenario típico de streaming de datos, donde el usuario hace clic en un vínculo de una página web para solicitar contenido. Posteriormente, en el caso de streaming unicast, el servidor web redirige la solicitud al servidor de Windows Media quien establece una conexión directa con el reproductor e inicia la transmisión del contenido directamente al usuario. Con streaming multicast, el servidor de Windows Media ya se encuentra difundiendo el contenido a un grupo multicast, y el servidor Web provee al reproductor del cliente los datos necesarios para unirse a ese grupo. Llegado a este punto, el servidor web ya no desempeña ningún papel en el proceso de streaming.

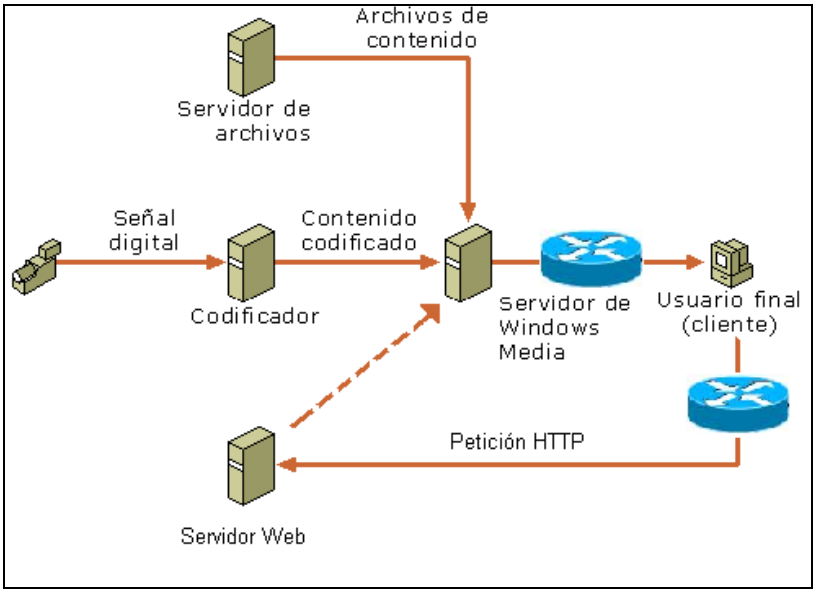

Figura 4-2: Escenario de un Sistema de Streaming con Tecnologías Windows Media

El escenario a implementar en este trabajo (ver Figura 4-3) posee las siguientes características:

- No utiliza un servidor de Windows Media Enconder: debido a que todo el contenido a difundir se encuentra pregrabado no se necesita este servicio.
- El Windows Media Services, servidor de archivos y Web se encuentran instalados en el mismo equipo.

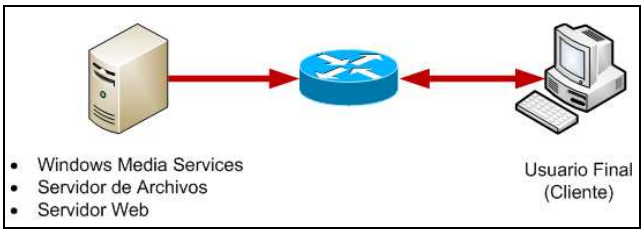

Figura 4-3: Escenario a Implementar

La entrega de contenido multimedia a los usuarios finales a través de la red puede realizarse mediante dos métodos:

[43] http://technet.microsoft.com/es-es/library/cc770711(WS.10).aspx

- Descarga: para entregar contenido a los usuarios mediante el método de descarga, normalmente se guarda el contenido en un servidor web y se proporciona a los usuarios un vínculo al contenido en una página web. Posteriormente, el usuario hace clic en el vínculo, descarga el archivo a su disco duro local y, finalmente, reproduce el contenido mediante un reproductor.
- Streaming: para entregar contenido a los usuarios mediante este método, el contenido se puede guardar en un servidor de Windows Media y, a continuación, asignar el contenido a un punto de publicación (ubicación del contenido que el servidor de streaming puede difundir a la red). Seguidamente, puede proporcionar a los usuarios el acceso al contenido (archivo de anuncio, dirección URL del punto de publicación) vía una página Web o mensaje de correo, por ejemplo. Cuando el usuario hace clic en el vínculo o en el archivo de anuncio, el reproductor se abre y se conecta al streaming.

A continuación se muestra en la Tabla 4-6 un cuadro comparativo entre ambos métodos.

	Descarga	Streaming
Reproducción del contenido multimedia	Se inicia una vez que todo el archivo se ha descargado al equipo cliente.	Se inicia poco después que empieza el streaming, se debe almacenar en el bufer los datos por si se produce retrasos.
Ancho de banda	Consume todo el ancho de banda necesario para la descarga.	Consumen el ancho de banda necesario para que la velocidad de transmisión sea la que el cliente necesita para procesar los datos.
Reproducción en vivo	No se puede, ya que primero se debe generar el archivo multimedia.	Es posible debido a que el streaming y el procesamiento se producen al mismo tiempo.

Tabla 4-6: Comparación entre los Métodos de Entrega de Contenido.

Se puede suministrar contenido basado en Windows Media desde un servidor que ejecute Windows Media Services o desde un servidor web. No obstante, un servidor de Windows Media está diseñado específicamente para la transmisión por secuencias (streaming) de contenido basado en Windows Media, lo cual no ocurre con un servidor web estándar. A continuación se presenta en la Tabla 4-7 las diferencias más resaltantes entre estos dos métodos.

	Servidor Web	Windows Media Services
Método de envío	Envía la mayor cantidad de datos que pueda, lo más rápido posible.	Suministro en tiempo real, no en ráfagas grandes, de tal manera que los reproductores reciban los paquetes inmediatamente antes de reproducirlos.
Regulación de entrega	No regula la entrega.	Regula la entrega de paquetes en función de la información que recibe mientras envía una secuencia a un reproductor y según la configuración de determinadas características
UDP	No pueden usar el protocolo UDP.	Si lo implementa.
Multicast	No soporta.	Si lo implementa.
Supervisión y registro	No soporta.	Permite recopilar información importante acerca de la sesión de transmisión de contenido multimedia y su audiencia

Tabla 4-7: Comparación entre los Métodos de Suministro de Contenido.

Antes de poder transmitir contenido se debe comunicar a los usuarios que el mismo se encuentra disponible, e informar a los reproductores los parámetros necesarios para poder conectarse e interpretar de manera correcta el contenido. La comunicación puede realizarse por medio de un correo electrónico, página web o mesaje de texto; y la información que necesita los reproductores por medio de un archivo de información de multidifusión (archivos *.nsc). Un archivo de información de multidifusión posee básicamente la siguiente información:

- Dirección IP de multidifusión.
- Puerto de multidifusión.
- Período de vida (TTL).
- Intervalo de corrección de errores predeterminado.
- Formatos de secuencia usados por el contenido que se entrega.

Esta información viene codificada y sólo puede ser decodificada por reproductores de WMP. Otra configuración importante en el servidor son los “Puntos de Publicación”, es decir, los medios a través del cual se distribuye el contenido (archivos de audio, video, etc.) a los usuarios.

Al momento de definir un punto de publicación se debe indicar un origen de media, este origen puede ser un archivo o conjunto de archivos, un directorio, lista de reproducción, codificador, entre otros. Para este trabajo se utilizará una lista de reproducción, el cual no es más que un archivo que hace referencia a piezas de contenido digital y permite organizarlos. La ventaja de utilizar como origen una lista de reproducción en vez de simplemente los archivos o directorios, es que la primera permite tener control sobre el orden de la reproducción, como por ejemplo indicar que se desea reproducir aleatoriamente los archivos seleccionados.

4.2.2. Infraestructura de red

Para implementar un sistema que soporte aplicaciones multicast, es necesario un conjunto de protocolos que interactúen entre sí y dispositivos de red que los soporten. A continuación se mencionan los protocolos y dispositivos necesarios para un servicio de hilos musicales sobre IPv6 multicast:

Protocolos

El protocolo base para todas las comunicaciones utilizadas en este trabajo es IPv6, debido a que es una tecnología relativamente nueva que trae consigo nuevas características de comunicación y enrutamiento multicast que mejoran a las de su predecesor (IPv4). También se necesita un protocolo para el enrutamiento de los paquetes multicast desde el origen hasta los destinos, para esto se recurrió a "Protocol Independent Multicast – Sparse Mode" (PIM-SM) debido a las siguientes consideraciones:

- Es el protocolo más desplegado en entornos multicast.
- Está definido formalmente en [61] y posee soporte para IPv6.
- Ha sido adoptado por las principales compañías fabricantes de dispositivos de red en el mundo, tales como: Cisco, 3Com, Juniper, entre otras.
- Existen desarrollos de routers en software con soporte PIM-SM para IPv6, como por ejemplo XORP[44] (eXtensible Open Router Platform).
- Soporta árboles de distribución compartidos y de origen, lo que permite ser utilizado por aplicaciones multicast de uno-a-muchos y muchos-a-muchos.
- Trabaja con protocolos de suscripción y mantenimiento simples, como MLDv1.

PIM-SM necesita de un protocolo de enrutamiento unicast subyacente que colabore en la creación los árboles de distribución multicast. El protocolo utilizado en este trabajo fue EIGRP [83], debido a que es el utilizado en la red de datos de la UCV.

Por otra parte, se requiere un protocolo para gestionar la membrecía a grupos multicast con los routers multicast, se considera el protocolo Multicast Listener Discovery versión 2 (MLDv2), que al igual que PIM-SM, se encuentra definido formalmente en un RFC y arrastra la experiencia de IGMP en ambientes multicast ahora con soporte IPv6.

Finalmente, con respecto a la aplicación cliente, esta debe soportar tanto IPv6 como MLDv1 para poder participar a una infraestructura multicast IPv6.

En la Figura 4-4, se muestra la distribución de los protocolos utilizados en este trabajo, basado en la pila de protocolos TCP/IP.

[44] http://www.xorp.org

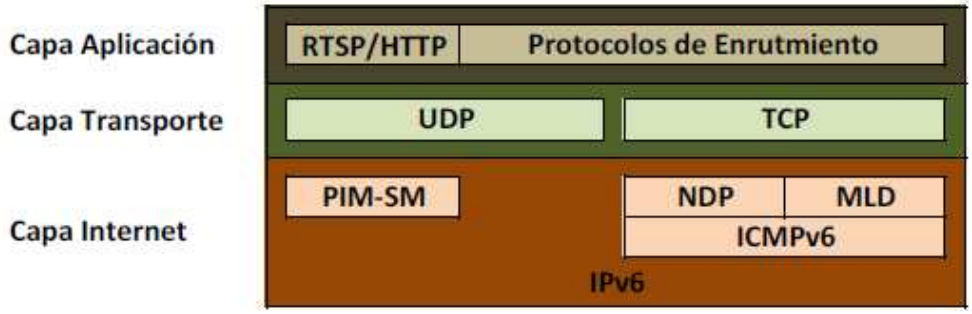

Figura 4-4: Pila de Protocolos Involucrados en PIM-SM

Dispositivos de red

Los dispositivos de red necesarios para una infraestructura multicast sobre IPv6 son:

- Adaptadores de Red: para comunicarse con el resto de la red, cada estación de trabajo debe tener instalada una interfaz de red. La velocidad mínima soportada debe ser de 10 Mbps, y la recomendada superior o igual a 100 Mbps. La velocidad del adaptador de red en el servidor debe ser de al menos 100 Mbps.
- Cableado: se recomienda que el cableado en el nivel de distribución y núcleo soporte velocidades de por lo menos 1 Gbps (UTP con categoría mayor o igual a 5e o fibra óptica), para el nivel de acceso el cableado debe soportar velocidades mayores a 10 Mbps (UTP con categoría 5).
- Switches: los switches de acceso deben poseer puertos de por lo menos 10/100 Mbps para la conexión con las estaciones de trabajo y de por lo menos 1 Gbps para la conexión con los switches de distribución. Los de distribución y núcleo de por lo menos 1 Gbps. También es recomendable que los switches soporten MLD Snooping para el tráfico multicast.
- Routers: los routers deben soportar IPv6, MLD, PIM-SM y EIGRP.

4.2.3. Dispositivos clientes

Los sistemas operativos de los equipos participantes en la red, deben soportar la pila IPv6, y poseer un cliente de audio IPv6 Multicast. Algunos de los sistemas operativos que actualmente cumplen con estos requerimientos son:

- Microsoft Windows XP
- Linux (basados en el kernel 2.6)
- Apple Mac OS X

Microsoft inició el soporte a IPv6 desde su versión XP para entornos de desarrollo y diseño, y con el Service Pack 2 incorporó todas las funcionalidades para el usuario final. Por su parte en Linux, el primer código de red relacionado con IPv6 fue agregado en el Kernel 2.1.8 en noviembre de 1996. En octubre del 2000, con la creación del proyecto USAGI[45] (UniverSAl playGround for IPv6), se empezó a mejorar el soporte para la pila IPv6 en Linux, basada principalmente en la implementación hecha en FreeBSD[46] por el proyecto KAME[47]. Ya para el desarrollo de la serie 2.5.x, USAGI trató de incluir todas

[45] http://www.linux-ipv6.org
[46] http://www.freebsd.org
[47] http://www.kame.net

las extensiones para el soporte IPv6, siendo en la serie 2.6.x que todas las extensiones fueron adoptadas.

En este mismo sentido, el cliente de audio a utilizar debe soportar la pila IPv6 y multicast. Entre los clientes disponibles que cumplen con estos requerimientos se encuentran MS Windows Media Player y VideoLAN VLC, ambos recomendados para las estaciones clientes.

4.3. Diseño de un ambiente de pruebas

El diseño del ambiente de pruebas se concibió en base a los recursos del Laboratorio de Internet2 de la Escuela de Computación (routers, switches, servidores y estaciones de trabajo) y la topología de red de la Universidad Central de Venezuela.

4.3.1. Equipos de Comunicaciones

Los dispositivos de red utilizados en el Laboratorio de Internet2 de la Facultad de Ciencias están conformados por cinco (5) routers y dos (2) switches. A continuación se presenta una descripción de cada uno de ellos.

Router Cisco 2811: La serie de routers 2800 (ver Figura 4-5 y 4-6) integran servicios de voz, datos, video, conectividad inalámbrica y seguridad. Se encuentra ubicada entre los dispositivos de rango medio, para pequeñas y grandes oficinas capaz de soportar aplicaciones de negocios de misión crítica.

Figura 4-5: Vista frontal de un Router Cisco 2811.

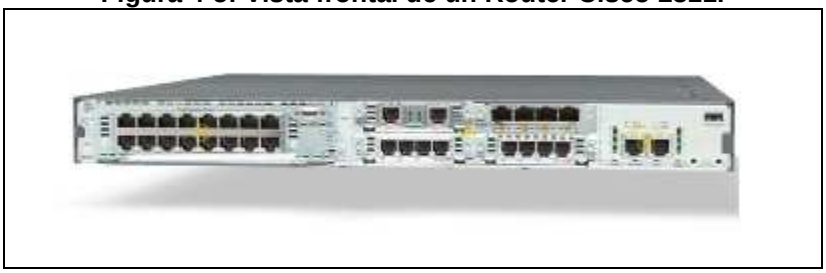

Figura 4-6: Vista trasera de un Router Cisco 2811.

Entre las características resaltantes del modelo 2811 se encuentran:

- Interfaces Ethernet 10/100 integradas: 2.
- Puertos Ethernet 10/100: hasta 32 puertos.
- Puertos USB: 2.
- Protocolos de Enrutamiento IPv4: RIP v1/v2, EIGRP, OSPF, BGP e IS-IS.

- Protocolos Multicast: PIM-SM y MLD.
- Protocolos de Enrutamiento IPv6: EIGRP, RIPng, OSPFv3 y IS-IS.

Switch Cisco 3750: esta serie (ver Figura 4-7) se encuentra ubicada entre los productos para organizaciones medianas y pequeñas. Son switches capa 3 (L3) y se pueden apilar (stack) entre ellos.

Figura 4-7: Vista frontal de Switch Cisco 3750.

Entre las características resaltantes de este modelo se encuentran:

- Switching Fabric: 32 Gbps.
- Stack de interconexión bidirecional: 32 Gbps.
- Puertos Ethernet 10/100: 24.
- Puertos GBIC/SFP: 2.
- Administración y configuración automatizada.
- Conectividad y filtrado: EtherChannel, Jumbo Frame (L2), entre otros.
- Soporte Capa 2: ISL/802.1Q, Private VLAN, VTP, entre otros.
- Soporte Capa 3: EIGRP, OSPF, BGP, RIP/RIPv2, IPv6, entre otros.

4.3.2. Servidor

El equipo que se utilizó como servidor para la aplicación de streaming posee las siguientes características:

- Procesador: Intel Core2 Duo de 2,3 GHz.
- Memoria: 2 GB / DDR2 / 800 MHz.
- Disco Duro: 250 GB / SATA II / 7.200 RPM.
- Interfaz de Red: 10/100/1000 Mbps PCIe.

Además de los elementos mencionados anteriormente, el envío exitoso de cualquier tráfico multimedia sobre una red LAN o WAN debe considerar tres componentes importantes:

- Ancho de Banda: cuanto ancho de banda la aplicación multimedia necesita y cual es el ancho de banda provisto por la infraestructura.

- Calidad de Servicio: nivel de servicio que la aplicación multimedia requiere y como este puede ser satisfecho por la red.
- Multicast: la aplicación multimedia utiliza técnicas de multicast y como la red puede soportar las mismas.

4.3.3. Ancho de banda

En nuestro caso, la aplicación multimedia difundirá audio digital en formato MP3, que es el de mayor utilización para este tipo de aplicaciones. El audio digital usa señales digitales para la reproducción de sonido, empieza con una señal de audio analógica que es convertida a señales eléctricas, y luego es codificada para combatir errores que pudieran ocurrir durante el almacenamiento o transmisión de la señal.

En este mismo sentido, MP3 es un formato de codificación de audio digital diseñado para reducir la cantidad de datos requeridos para representar una grabación de audio, y mantener un sonido fiel a la reproducción original del audio sin compresión. Normalmente utiliza una velocidad de muestreo de 44.100 Hz y un bitrate de 128/192 kbps.

En la Tabla 4-8 (tomada de Wikipedia[48]) se muestra algunas velocidades de muestreo comunes:

Velocidad de Muestreo	Uso Común
8.000 Hz	Telefonía estándar.
22.050 Hz	Radio.
44.100 Hz	CD, también común en formatos de audio MPEG-1 como MP3.

Tabla 4-8: Velocidades de Muestreo.

De esta manera la aplicación necesitará, por lo menos, 128 kbps de ancho de banda por cada canal de audio. Un canal de audio, en nuestro caso, es un flujo de datos que provee la información necesaria para reproducir audio en los clientes; equivalente a una frecuencia de una emisora de radio.

4.3.4. Calidad de servicio

La calidad de servicio (QoS, Quality of Service) se refiere a la capacidad para proveer un mejor servicio de red a un tráfico específico sobre varias tecnologías. Aunque un estudio exhaustivo de QoS está fuera del alcance de este documento, su configuración es importante para la conservación de ancho de banda, pérdida de paquetes, control de jitter y latencia (requerido para tráfico interactivo y en tiempo real).

Las aplicaciones de datos y multimedia tienen diferentes requerimientos de calidad de servicio. En los servicios de datos tradicionales de “mejor esfuerzo” como FTP o SMTP, las variaciones en la latencia (jitter) no son percibidas, mientras que los datos de audio y video son útiles sólo si ellos son entregados dentro de un periodo específico de

[48] http://en.wikipedia.org/wiki/Sampling_rate

tiempo. En general, la latencia y jitter son los dos principales parámetros que trabajan contra la entrega oportuna de los datos de audio y video.

- Latencia: representa la suma de retardos temporales dentro de una red. Las redes telefónicas están diseñadas para una latencia de ida y vuelta (round-trip) de menos de 400 ms. En redes que deben soportar aplicaciones multimedia la latencia comprometida debe ser menor a los 300 ms de ida y vuelta según [86].
- Jitter: es la entrega de datos con latencia variable.

4.3.5. Multicast

La utilización de aplicaciones que soporten multicast, y una red que soporte el tráfico de datos con esta característica es fundamental para el funcionamiento de aplicaciones multimedia.

Finalmente, y en base a los recursos disponibles en el laboratorio de Internet2, este proyecto de tesis dispondrá de los siguientes equipos:

- Un servidor para las transmisiones de streaming de audio.
- Dos switches para la configuración de VLANs.
- Cinco routers interconectados, uno de ellos designado como RP.
- Diez equipos clientes conectados a 3 subredes diferentes.

Para la asignación de las direcciones IPv6 a los distintos equipos y recursos de la red se utilizará el prefijo IPv6 2001:DB8::/32, el cual ha sido definido en [40] para uso de propósitos de documentación e investigación.

La infraestructura propuesta se muestra en la Figura 4-8, se definió de tal manera que simule la red actual de la UCV.

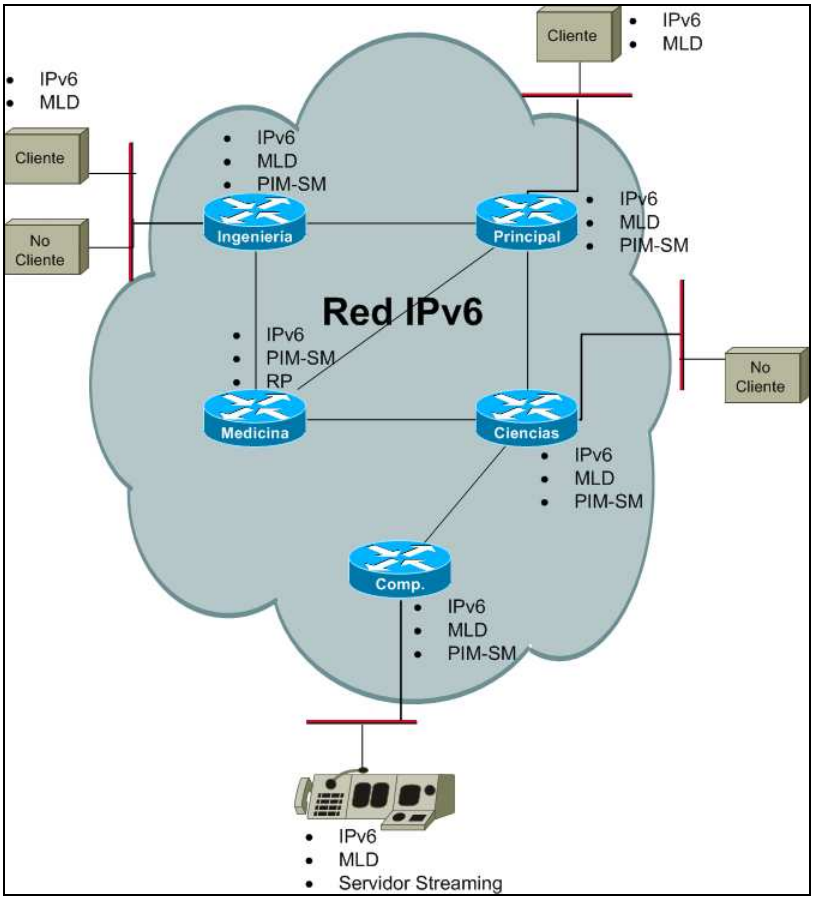

Figura 4-8: Infraestructura de Red Propuesta para el Ambiente de Pruebas

4.4. Implementación del Ambiente de Pruebas

Posterior al análisis realizado sobre los elementos de software y hardware necesarios para una infraestructura multicast sobre IPv6, se procede a describir el proceso de implementación de un ambiente de pruebas dividido en varias fases:

4.4.1. Instalación de la plataforma de telecomunicaciones

El primer paso para la instalación de la plataforma fue crear una red de datos para el ambiente de pruebas en base a la infraestructura propuesta (Figura 4.7). Para esto se procedió a identificar el número de interfaces seriales y puertos Ethernet disponibles en cada uno de los routers y el switch:

- Tres (3) routers tenían 4 puertos seriales y 2 FastEthernet.
- Dos (2) routers tenían 2 puertos seriales y 2 FastEthernet.
- Un (1) switch con 24 puertos FastEthernet.

Luego se realizó la conexión entre los routers y del switch según el diagrama físico que se muestra en la Figura 4-9.

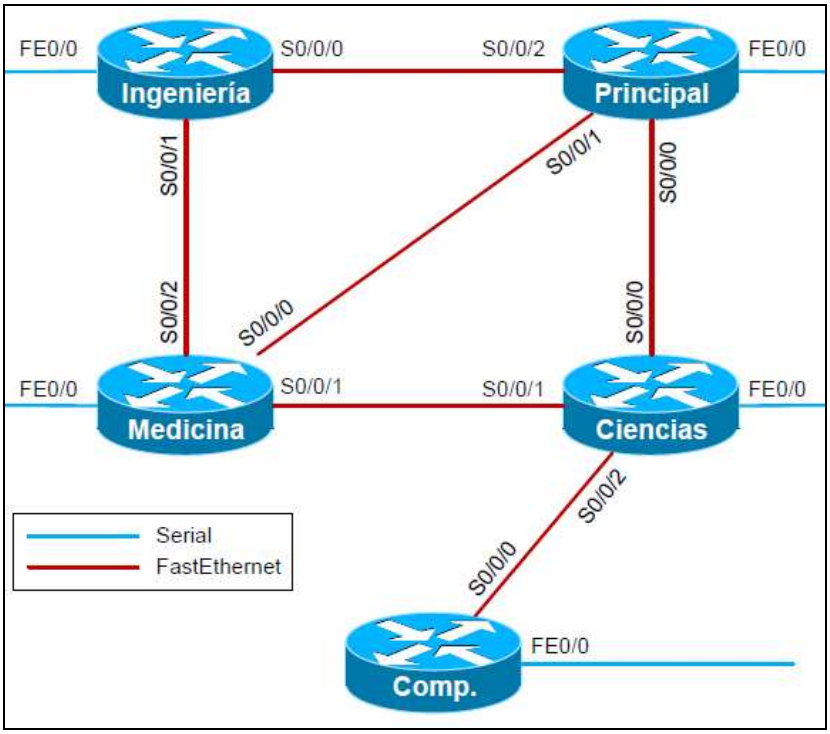

Figura 4-9: Diagrama Físico del Ambiente de Pruebas

En el rack del laboratorio los routers y el switch quedaron interconectados como se muestra en la Figura 4-10.

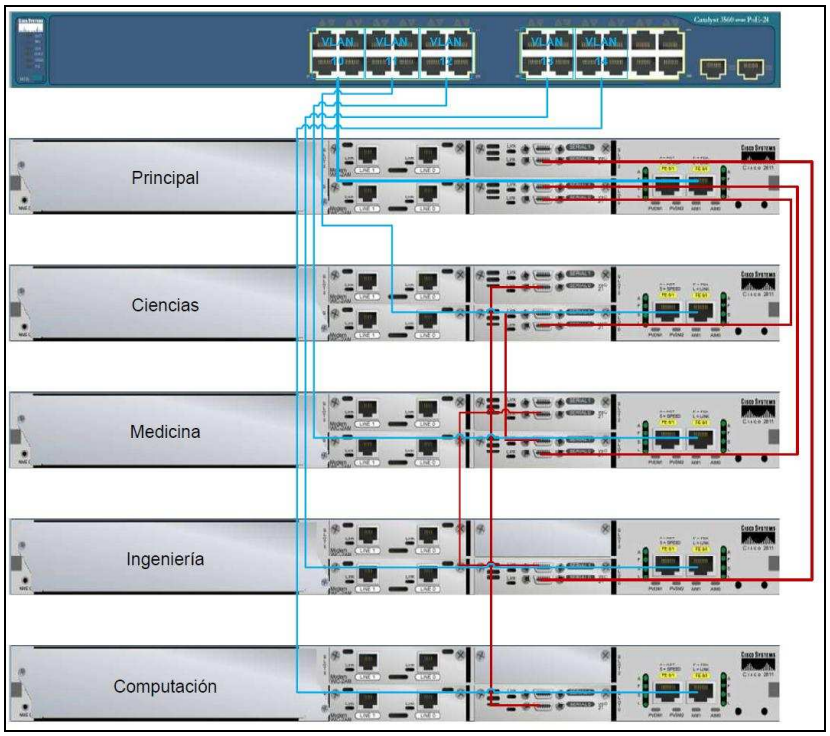

Figura 4-10: Interconexión de los Equipos del Ambiente de Pruebas

Se crearon 5 VLANs en el switch las cuales estaban asociadas a una interfaz de cada router, como se muestra en la Tabla 4-9.

Router	VLAN	Puertos del Switch
Principal	10	1,2,3,4
Ciencias	11	5,6,7,8
Medicina	12	9,10,11,12
Ingeniería	13	13,14,15,16
Computación	14	17,18,19,20

Tabla 4-9: Tabla de VLANs.

4.4.2. Configuración de la plataforma de telecomunicaciones

Antes de iniciar la configuración de los equipos, se definieron los siguientes parámetros:

- Direcciones IPv6 a utilizar para las conexiones punto-a-punto.
- Direcciones IPv6 a utilizar para las redes asociadas a las VLANs.
- Identificadores de los routers (router-id) para el protocolo de enrutamiento EIGRP.
- Número de sistema autónomo (ASN) a utilizar para el protocolo de enrutamiento EIGRP.
- Interfaces con PIM habilitado.
- Interfaces con MLD habilitado.

Luego se creó el diagrama lógico de la Figura 4-11, que sirvió de guía para la configuración de cada uno de los elementos de la red del ambiente de pruebas.

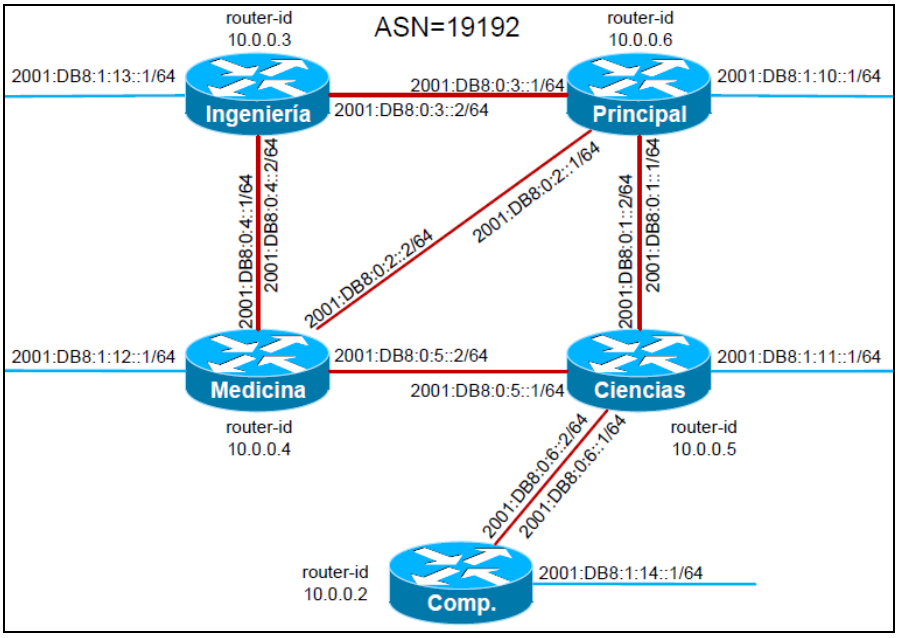

Figura 4-11: Diagrama Lógico del Ambiente de Pruebas

A continuación se muestra las instrucciones ejecutadas en cada uno de los componentes:

Switch

```
vlan 10
name Principal
!
vlan 11
name ciencias
!
vlan 12
name Medicina
!
vlan 13
name Ingenieria
!
vlan 14
name Computacion
!
ipv6 mld snooping vlan 10
!
ipv6 mld snooping vlan 11
!
ipv6 mld snooping vlan 12
!
ipv6 mld snooping vlan 13
!
ipv6 mld snooping vlan 14
!
interface FastEthernet1/0/1
 switchport access vlan 10
!
interface FastEthernet1/0/2
 switchport access vlan 10
!
interface FastEthernet1/0/3
 switchport access vlan 10
!
interface FastEthernet1/0/4
 switchport access vlan 10
!
interface FastEthernet1/0/5
 switchport access vlan 11
!
interface FastEthernet1/0/6
 switchport access vlan 11
!
interface FastEthernet1/0/7
 switchport access vlan 11
!
interface FastEthernet1/0/8
 switchport access vlan 11
!
interface FastEthernet1/0/9
 switchport access vlan 12
!
interface FastEthernet1/0/10
 switchport access vlan 12
!
interface FastEthernet1/0/11
 switchport access vlan 12
!
interface FastEthernet1/0/12
 switchport access vlan 12
!
interface FastEthernet1/0/13
 switchport access vlan 13
!
interface FastEthernet1/0/14
 switchport access vlan 13
!
interface FastEthernet1/0/15
```

```
 switchport access vlan 13
!
interface FastEthernet1/0/16
 switchport access vlan 13
!
interface FastEthernet1/0/17
 switchport access vlan 14
!
interface FastEthernet1/0/18
 switchport access vlan 14
!
interface FastEthernet1/0/19
 switchport access vlan 14
!
interface FastEthernet1/0/20
 switchport access vlan 14
!
```

Router Principal

```
hostname Principal
!
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 host ciencias 2001:DB8:0:1::2
ipv6 host medicina 2001:DB8:0:2::2
ipv6 host ingenieria 2001:DB8:0:3::2
ipv6 host computacion 2001:DB8:0:6::2
!
interface Serial0/0/0
 description Interfaz Conexion a Router de Ciencias
 no ip address
 ipv6 address 2001:DB8:0:1::1/64
 ipv6 eigrp 19192
 no shutdown
!
interface Serial0/0/1
 description Interfaz Conexion a Router de Medicina
 no ip address
 shutdown
 ipv6 address 2001:DB8:0:2::1/64
 ipv6 eigrp 19192
 no shutdown
!
interface Serial0/2/0
 description Interfaz Conexion a Router de Ingenieria
 no ip address
 ipv6 address 2001:DB8:0:3::1/64
 ipv6 eigrp 19192
 no shutdown
!
interface FastEthernet0/0
 description Interfaz LAN
 no ip address
 ipv6 address 2001:DB8:1:10::1/64
 ipv6 eigrp 19192
 no shutdown
!
ipv6 router eigrp 19192
 router-id 10.0.0.6
 no shutdown
!
ipv6 pim rp-address 2001:db8:0:1::1 acc-ucv-mcast-grp
!
Ipv6 access-list acc-ucv-mcast-grp
 permit ipv6 any FF05::100
 permit ipv6 any FF05::101
 permit ipv6 any FF05::102
 permit ipv6 any FF05::103
!
```

Router Ciencias

```
hostname Ciencias
!
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 host Principal 2001:DB8:0:1::1
ipv6 host Medicina 2001:DB8:0:5::2
ipv6 host Ingenieria 2001:DB8:0:3::2
ipv6 host Computacion 2001:DB8:0:6::2
!
interface Serial0/0/0
 description Interfaz Conexion a Router Principal
 no ip address
 ipv6 address 2001:DB8:0:1::2/64
 ipv6 eigrp 19192
 no shutdown
!
interface Serial0/0/1
 description Interfaz Conexion a Router Medicina
 no ip address
 ipv6 address 2001:DB8:0:5::1/64
 ipv6 eigrp 19192
 no shutdown
!
!
interface Serial0/2/0
 description Interfaz Conexion a Router Computacion
 no ip address
 ipv6 address 2001:DB8:0:6::1/64
 ipv6 eigrp 19192
 no shutdown
!
interface FastEthernet0/0
 description Interfaz LAN
 no ip address
 ipv6 address 2001:DB8:1:11::1/64
 ipv6 eigrp 19192
 no shutdown
!
ipv6 router eigrp 19192
 router-id 10.0.0.5
 no shutdown
!
ipv6 pim rp-address 2001:db8:0:1::1 acc-ucv-mcast-grp
!
Ipv6 access-list acc-ucv-mcast-grp
 permit ipv6 any FF05::100
 permit ipv6 any FF05::101
 permit ipv6 any FF05::102
 permit ipv6 any FF05::103
!
```

Router Medicina

```
hostname Medicina
!
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 host Principal 2001:DB8:0:2::1
ipv6 host Ciencias 2001:DB8:0:5::1
ipv6 host Ingenieria 2001:DB8:0:4::2
ipv6 host Computacion 2001:DB8:0:6::2
!
interface Serial0/0/0
 description Interfaz Conexion a Router Principal
 no ip address
 ipv6 address 2001:DB8:0:2::2/64
 ipv6 eigrp 19192
 no shutdown
!
interface Serial0/0/1
 description Interfaz Conexion a Router Ciencias
```

```
 no ip address
 ipv6 address 2001:DB8:0:5::2/64
 ipv6 eigrp 19192
 no shutdown
!
interface Serial0/2/0
 description Interfaz Conexion a Router Ingenieria
 no ip address
 ipv6 address 2001:DB8:0:4::1/64
 ipv6 eigrp 19192
 no shutdown
!
interface FastEthernet0/0
 description Interfaz LAN
 no ip address
 ipv6 address 2001:DB8:1:12::1/64
 ipv6 eigrp 19192
 no shutdown
!
ipv6 router eigrp 19192
 router-id 10.0.0.4
 no shutdown
!
ipv6 pim rp-address 2001:db8:0:1::1 acc-ucv-mcast-grp
!
Ipv6 access-list acc-ucv-mcast-grp
 permit ipv6 any FF05::100
 permit ipv6 any FF05::101
 permit ipv6 any FF05::102
 permit ipv6 any FF05::103
!
```

Router Ingeniería

```
hostname Ingenieria
!
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 host Principal 2001:DB8:0:3::1
ipv6 host Ciencias 2001:DB8:0:1::2
ipv6 host Medicina 2001:DB8:0:4::1
ipv6 host Computacion 2001:DB8:0:6::2
!
interface Serial0/0/0
 description Interfaz Conexion a Router Principal
 no ip address
 ipv6 address 2001:DB8:0:3::2/64
 ipv6 eigrp 19192
 no shutdown
!
interface Serial0/0/1
 description Interfaz Conexion a Router Medicina
 no ip address
 ipv6 address 2001:DB8:0:4::2/64
 ipv6 eigrp 19192
 no shutdown
!
interface FastEthernet0/0
 description Interfaz LAN
 no ip address
 ipv6 address 2001:DB8:1:13::1/64
 ipv6 eigrp 19192
 no shutdown
!
ipv6 router eigrp 19192
 router-id 10.0.0.3
 no shutdown
!
ipv6 pim rp-address 2001:db8:0:1::1 acc-ucv-mcast-grp
!
Ipv6 access-list acc-ucv-mcast-grp
 permit ipv6 any FF05::100
 permit ipv6 any FF05::101
 permit ipv6 any FF05::102
```

```
 permit ipv6 any FF05::103
!
```

Router Computación

```
hostname Computacion
!
ipv6 unicast-routing
ipv6 multicast-routing
ipv6 host Principal 2001:DB8:0:1::1
ipv6 host Ciencias 2001:DB8:0:6::1
ipv6 host Medicina 2001:DB8:0:5::2
ipv6 host Ingenieria 2001:DB8:0:3::2
!
interface Serial0/0/0
 description Interfaz Conexion a Router Ciencias
 no ip address
 ipv6 address 2001:DB8:0:6::2/64
 ipv6 eigrp 19192
 no shutdown
!
interface FastEthernet0/0
 description Interfaz LAN
 no ip address
 ipv6 address 2001:DB8:1:14::1/64
 ipv6 eigrp 19192
 no shutdown
!
ipv6 router eigrp 19192
 router-id 10.0.0.2
 no shutdown
!
ipv6 pim rp-address 2001:db8:0:1::1 acc-ucv-mcast-grp
!
Ipv6 access-list acc-ucv-mcast-grp
 permit ipv6 any FF05::100
 permit ipv6 any FF05::101
 permit ipv6 any FF05::102
 permit ipv6 any FF05::103
!
```

4.4.3. Instalación del Sistema Operativo Microsoft Windows 2003

La instalación del sistema operativo se realizó por medio de un CD de instalación de Windows 2003 Server Enterprise Edition en Español, contemplando las siguientes consideraciones:

- El sistema de archivos elegido fue NTFS.
- El número de particiones creadas fueron dos (2), una para los archivos de sistema de Windows (C:\) con 20 GB de espacio en disco, y otro para los archivos de datos (D:\) con el resto del espacio en disco.
- Se instaló la última versión Service Pack para Windows 2003 Server para el momento (SP2).
- Se instaló el protocolo de red para el soporte IPv6 (Microsoft TCP/IP versión 6).

La única configuración excepcional realizada durante la instalación del sistema operativo es la dirección IPv6 de la interfaz de red, la cual se hizo de la siguiente manera:

- Iniciar una consola de comandos de Windows
  `Inicio → Ejecutar → cmd.exe`
- Ingresar a la consola de netsh
  `c:\>netsh`

- Consultar el índice de la interfaz con soporte IPv6.
  `netsh>interface ipv6 show interface`
- Asignar la dirección IPv6 a la interfaz.
  `netsh>interface ipv6 add address 4 2001:db8:1:14::10`

Posterior a la instalación del SP2, se realizó una actualización automática del sistema por medio de servicio de Windows Update de Microsoft.

4.4.4. Instalación del Servidor de Streaming Windows Media Server 9

La instalación del servicio de Windows Media Server 9 se realiza por medio de la opción "Agregar o quitar componentes de Windows" de la interfaz "Agregar o quitar programas" ubicada en el "Panel de Control" de Windows (ver Figura 4-12). Es necesario contar con el CD de instalación de la versión instalada, Windows 2003 Server Enterprise en este caso.

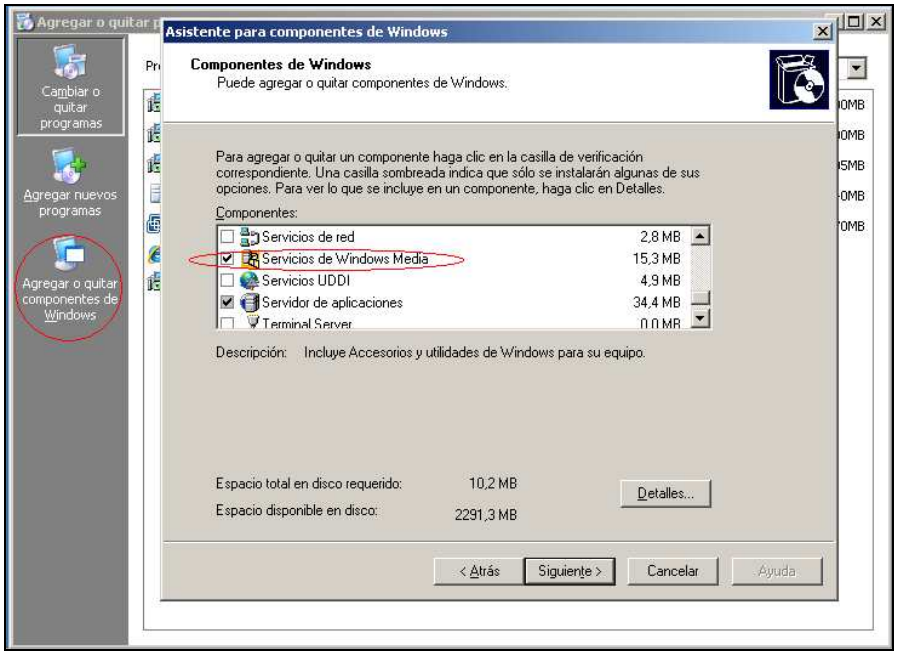

Figura 4-12: Asistente para Componentes de Windows

Una vez iniciado el "Asistente para componentes de Windows" se selecciona el componente "Servicios de Windows Media", y se verifica en el botón "Detalles" que todos los subcomponentes estén seleccionados como se muestra en la Figura 4-13.

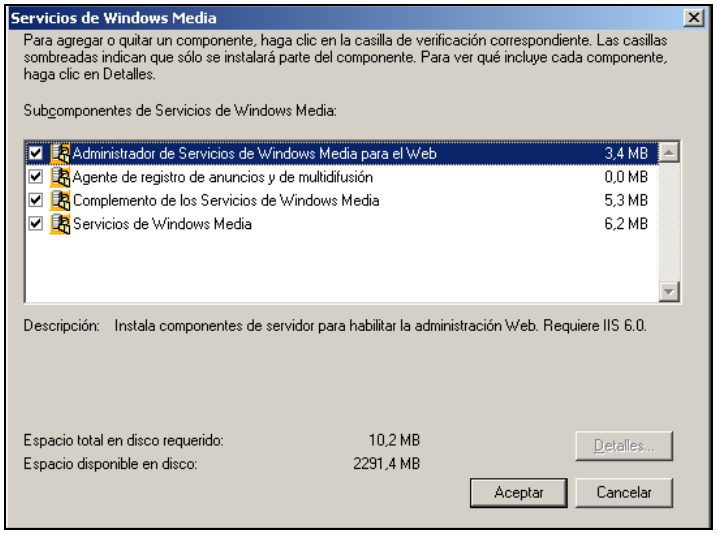

Figura 4-13: Subcomponentes del Servicio de Windows Media

Una vez instalado el servicio de Windows Media, se volvió a realizar una actualización automática del sistema por medio de servicio de Windows Update de Microsoft, para descargar las últimas actualizaciones del sistema.

4.4.5. Configuración del Servidor de Streaming Windows Media Server 9

Una vez instalado el Windows Media 9, el acceso a la interfaz de administración se hace por medio del enlace “Servicio de Windows Media” ubicado en el panel de “Herramientas Administrativas” de Windows Server 2003. Inicialmente la interfaz de administración muestra como raíz la instancia de Windows Media instalada en el equipo (WMS), bajo dicha raíz se listan tres ítems: Solución de Problemas, Administración de proxy-cache y Puntos de Publicación, como se muestra en la Figura 4-14.

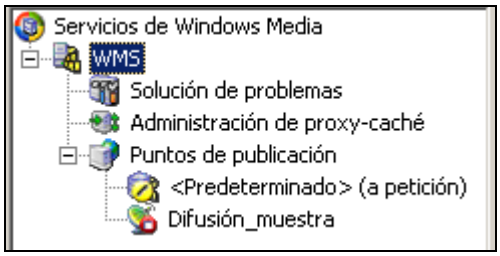

Figura 4-14: Subcomponentes del Servicio de Windows Media

Configuración de las Propiedades del Servidor

Algunas de los valores de las propiedades de WMS se cambiaron de su valor por defecto original (protocolos no utilizados, límites, orígenes de datos, entre otros) como se muestra en la Tabla 4-9.

Propiedad	Valor Inicial	Valor Final
Protocolo de control de servidor MMS de WMS	Habilitado	Deshabilitado
Analizador de multimedia de WMS	Habilitado	Deshabilitado
Analizador de medios con formato FF/RW avanzado de WMS	Habilitado	Deshabilitado
Origen de datos de red de WMS	Habilitado	Deshabilitado
Origen de datos de descarga HTTP de WMS	Habilitado	Deshabilitado
Origen de datos de inserción de WMS	Habilitado	Deshabilitado
Autor de datos de unidifusión de WMS	Habilitado	Deshabilitado

Tabla 4-9: Tabla de Configuraciones Iniciales.

Para acceder a las propiedades del servidor, se selecciona la raíz (WMS), luego en la ventana de detalles (panel derecho) se elige la pestaña “Propiedades” y ahí la casilla de verificación “Mostrar todas las categorías de componente”.

Creación de los Puntos de Publicación

Se deshabilitaron los dos puntos de publicación (Predeterminado y Difusión_muestra) que de forma predeterminada WMS instala, luego se crearon los cuatro (4) puntos nuevos que se describen a continuación:

- HiloMusicalRock:
  - Género: rock en inglés.
  - Directorio: D:\wmpub\WMRoot\Rock
  - Lista de Reproducción: lst_rock.wsx
  - NSC: rock.nsc
  - Dirección IPv6 Multicast: FE05::100
- HiloMusicalEspañol:
  - Género: pop/rock en español.
  - Directorio: D:\wmpub\WMRoot\Espanol
  - Lista de Reproducción: lst_espanol.wsx
  - NSC: espanol.nsc
  - Dirección IPv6 Multicast: FE05::101
- HiloMusical60-70-80s:
  - Género: 60s, 70s y 80s.
  - Directorio: D:\wmpub\WMRoot\60-70-80s
  - Lista de Reproducción: lst_60-70-80s.wsx
  - NSC: 60-70-80s.nsc
  - Dirección IPv6 Multicast: FE05::102
- HiloMusicalNewAge:
  - Género: New Age.
  - Directorio: D:\wmpub\WMRoot\NewAge
  - Lista de Reproducción: lst_newage.wsx
  - NSC: newage.nsc
  - Dirección IPv6 Multicast: FE05::103

Para crear las listas de reproducción se realizó el siguiente procedimiento:

- Se ejecutó el editor de listas de reproducción ubicado en c:\Windows\system32\ windows media\server\admin\mmc\wmseditor.exe.
- En el icono de “Agregar Elemento” se eligió “Multimedia”.
- Se seleccionó todos los archivos a reproducir en cada directorio.
- Se guardó la lista de reproducción con el nombre correspondiente.

Cada punto de publicación se creó siguiendo el procedimiento que se describe a continuación:

- Se seleccionó el subcomponente “Puntos de publicación” y en el menú se eligió:

```
Acción -> Agregar punto de publicación (Avanzado)
```

- En la ventana de configuración se establecieron los siguientes valores:
  - Tipo de punto de publicación: Difusión.
  - Nombre del punto de publicación: nombre del punto de acuerdo a lo establecido anteriormente (Ej.: HiloMusicalRock).
  - Ubicación del contenido: lista de reproducción de acuerdo a lo establecido anteriormente (Ej.: D:\wmpub\WMRoot\Rock\rock.wsx).
- En la ventana de detalles (panel derecho), se seleccionó la pestaña “Propiedades” y se estableció los siguientes valores:
  - General
    - Habilitar división de transmisión por secuencias: Deshabilitado.
    - Iniciar el punto de publicación cuando el primer cliente se conecte: Deshabilitado.
    - Habilitar cache rápida: Deshabilitado.
    - Habilitar inicio automático de difusión: Habilitado.
    - Habilitar inicio rápido avanzado: Habilitado.
  - Transmisión por secuencias de multidifusión de WMS
    - Autor de datos de multidifusión de WMS: Habilitado.
      - ❖ General
        - ✓ Dirección IP: dirección IPv6 (Ej.:FF05::102)
        - ✓ Puerto: 30000
        - ✓ TTL: 32 (Intranet)
      - ❖ Avanzado
        - ✓ Realizar multidifusión desde la dirección IP de la tarjeta de interfaz de red: dirección IPv6 de la interfaz del servidor (2001:db8:1:14::10).
    - Funciones de Red
      - ❖ Habilitar almacenamiento en búfer: deshabilitar.
- Luego se seleccionó la pestaña “Anuncio”, y en la sección “Conectar a transmisión por secuencia de multidifusión”, se ejecutó el “Asistente para anuncios de multidifusión” con las siguientes propiedades:
  - Se habilitó el complemento de autor de datos de multidifusión de WMS (en caso de no estarlo).
  - Archivos creados: se seleccionó la opción “Archivos de información de multicast (.nsc).

- Formatos de transmisión por secuencia: se debe seleccionar todos los archivos para que el sistema pueda identificar la información codificación que requieren los reproductores en los clientes.
- Registro de multicast: no se habilitó.
- URL del archivo de información de multicast: http://2001:db8:1:14::10/Rock.nsc
- Crear un archivo para el multicast: No.
- Finalmente dejar activado sólo la opción “Iniciar punto de publicación cuando finalice el asistente”.

Organización y Normalización de los Archivos de Audio

Para la organización de los archivos dentro de los directorios, se definió una estructura en donde cada uno de ellos se agrupa por autor (artista o grupo), y estos a su vez por álbum, cuando fue posible, como se muestra en la Figura 4-15.

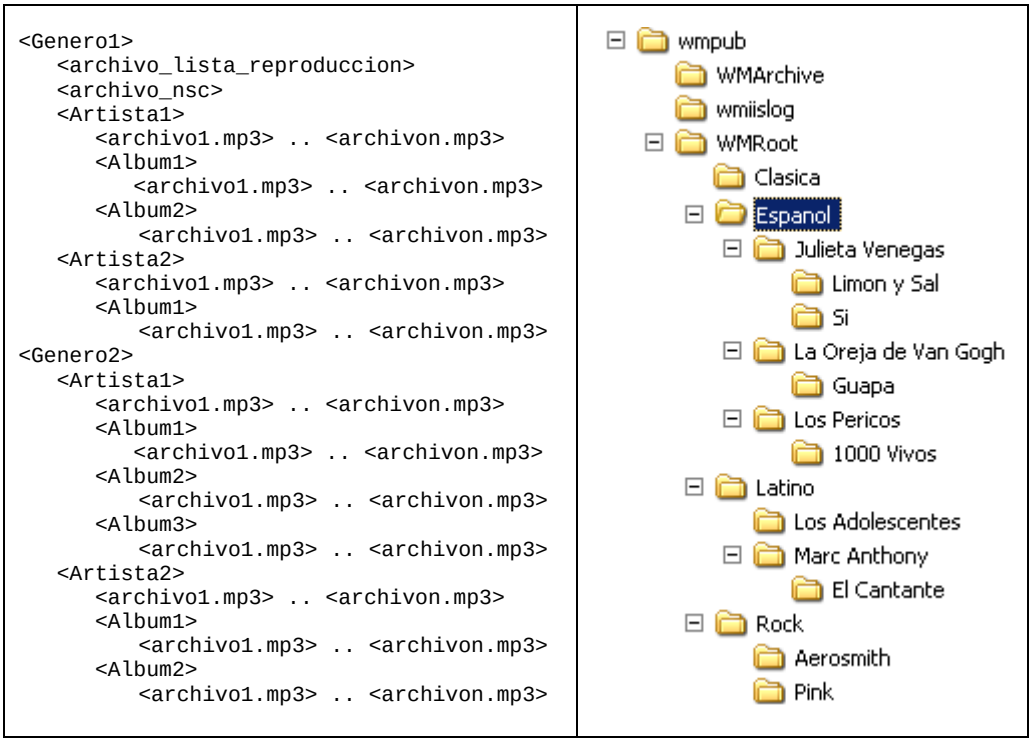

Figura 4-15: Estructura de Directorios de Archivos MP3

Para los archivos de audio, la estructura que se definió se muestra a continuación:

<ArtistaGrupo>-<NombreMúsica>.mp3 { - Aerosmtih - Angel.mp3
- Julieta Venegas - Limón y Sal.mp3

Se creó de esta manera con el fin de poder identificar la información relevante en los nombres de los archivos de audio. Se utilizó la aplicación MP3Tag[49] (ver Figura 4-16) para modificar los nombres de varios archivos simultaniamente.

[49] http://www.mp3tag.de/en/

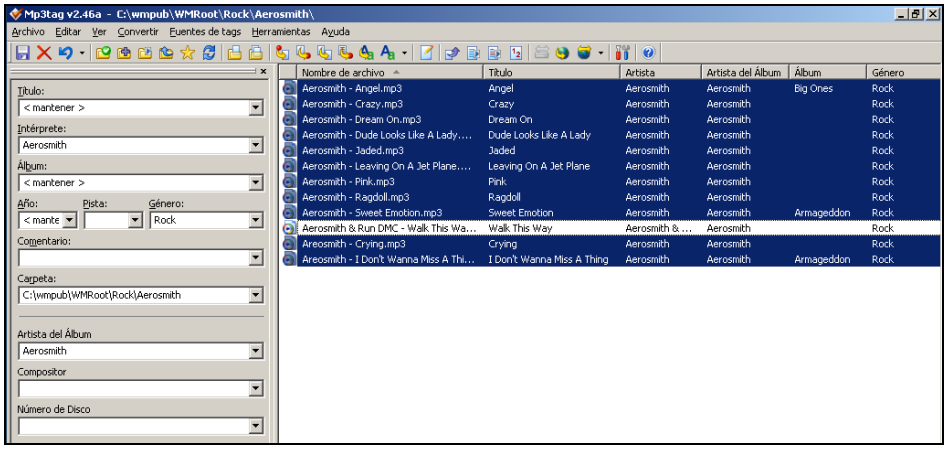

Figura 4-16: Extracción de Archivos MP3 desde un CD con CDex.

La recopilación de los archivos de audio se llevó principalmente por dos vías distintas:

- Internet: por medio de aplicaciones punto-a-punto.
- Medios Digitales: por medio de CD de música, reproductores MP3/MP4, dispositivos USB, archivos compartidos.

Ambas vías conformaron un repositorio inicial de archivos de audio con diferentes características; bitrate de 128, 192 y 360 kbps, niveles de audio de que variaban entre los 85 y 110 dB, nombres de archivos con estructuras variadas e información como nombre del artista, título, álbum, entre otros incompletos.

Es por esto que se definió para los archivos de audio un conjunto de parámetros estándar que se nombran a continuación:

- Bitrate: 128 kbps (CBR).
- Velocidad de Muestreo: 44.100 MHz.
- Nombre del Archivo: según la estructura que se describe más adelante.
- Nivel de Audio del Archivo: 90 dB.

La obtención de los archivos en formato MP3 a partir de CDs u otros medios se realizó con la ayuda de la aplicación CDex (ver Figura 4-17), la cual permite extraer la data digital directamente de un CD de audio o recodificar archivos de audio ya comprimidos, este proceso es llamado frecuentemente Ripping[50]. A los archivos extraídos se les asignó, por medio de la misma aplicación, los parámetros definidos anteriormente.

[50] http://en.wikipedia.org/wiki/Ripping

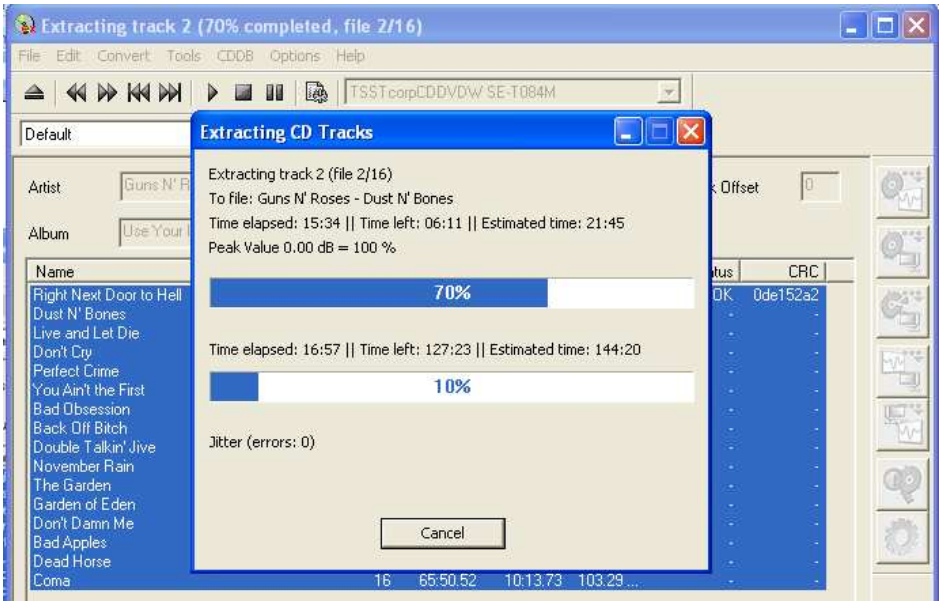

Figura 4-17: Extracción de Archivos MP3 desde un CD con CDex.

Para normalizar a un mismo nivel de sonido a los archivos de audio, se utilizó la aplicación MP3Gain[51] (ver Figura 4-18), un programa que analiza y ajusta archivos MP3 de tal manera que tengan el mismo volumen. Esto con el fin de que durante la reproducción de los archivos de audio, no se escuchen unos más altos que otros. El nivel de audio se estableció a 90 dB para todos los archivos de audio.

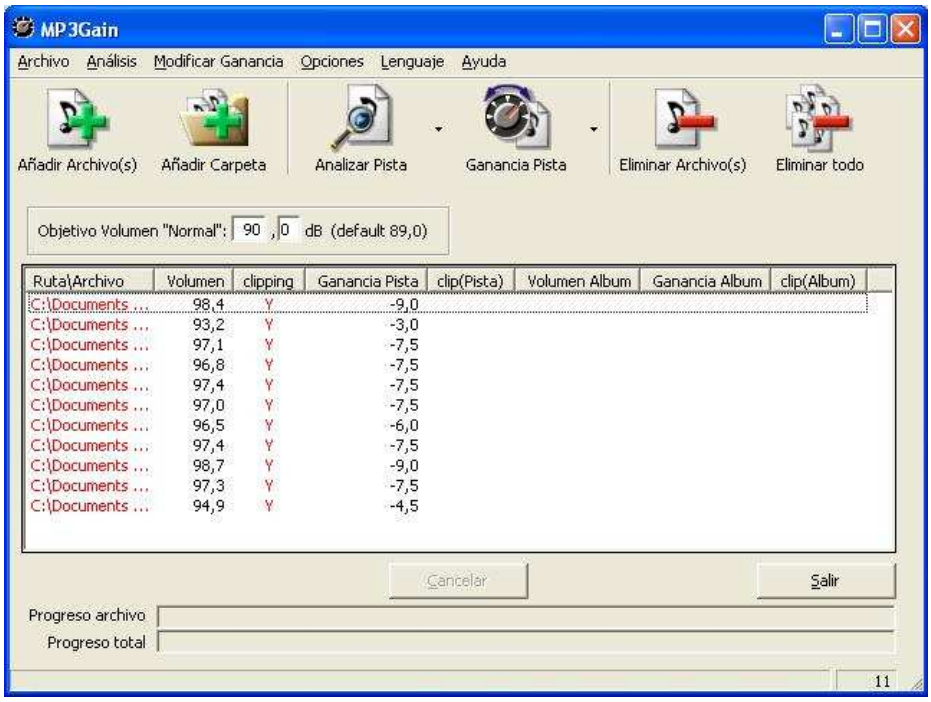

Figura 4-18: Cambio del Nivel de Audio de Archivos MP3 con MP3Gain.

[51] http://mp3gain.sourceforge.net/

4.4.6. Creación y Publicación de la Página HTML del Servicio de Hilo Musical

El acceso a los streaming de audio del servidor se realizó por medio de una página Web en donde se publicó los enlaces a cada uno de los Hilos Musicales habilitados. Al elegir cualquiera de los enlaces, se carga el control de audio del reproductor de WMP el cual reproducirá el archivo difundido por el servidor en ese momento.

Este control contiene un conjunto de parámetros configurables cuya descripción se pueden encontrar en Microsoft[52], de estos se utilizaron los que se muestran en la Tabla 4-10.

Parámetro	Valor
URL	http://<servidorWMS>/<Archivo>.nsc
enableContextMenu	False
uiMode	Mini
Name	Player

Tabla 4-10: Tabla de Parámetros de WMP Utilizados.

Para la publicación de la página (ver Figura 4-19) se utilizó como servidor Web el Internet Information Server v6 (IIS6), y para la resolución de nombre de dominio a direcciones IPv6 se utilizó el servidor DNS, ambos incluidos en la distribución de Windows Server 2003.

Figura 4-19: Página Web del Servicio de Hilos Musicales.

[52] http://msdn.microsoft.com/en-us/library/dd564581(v=VS.85).aspx

4.4.7. Configuración de los Clientes.

Debido a que la información contenida en los archivos de información de multidifusión (archivos .nsc) sólo pueden ser decodificados por reproductores WMP, el equipo cliente debe poseer las siguientes características mínimas:

- Sistema Operativo: Windows XP SP2.
- Windows Media Player: versión 9 (durante las pruebas se utilizó la versión 11).
- Navegadores:
  - Internet Explorer: versión 7.
  - Firefox: versión 3, además requiere del plugin de Windows Media Player[53] para poder ejecutar el componente.
- Soporte IPv6 (Microsoft TCP/IP versión 6).

Para la configuración de la dirección IPv6, se utilizó el siguiente procedimiento:

- Iniciar una consola de comandos de Windows
  `Inicio → Ejecutar → cmd.exe`
- Ingresar a la consola de netsh
  `c:\>netsh`
- Consultar el índice de la interfaz con soporte IPv6.
  `netsh>interface ipv6 show interface`
- Asignar la dirección IPv6 a la interfaz.
  `netsh>interface ipv6 add address 4 2001:db8:1:14::50`

Finalmente para acceder a la página del Hilo Musical se inicia un navegador Web, y se ingresa la siguiente dirección URL http://musica.ciens.ucv.ve.

[53] https://addons.mozilla.org/es-ES/firefox/browse/type:7

5. Conclusiones y Recomendaciones

Los resultados obtenidos en el desarrollo del presente Trabajo Especial de Grado, permiten destacar las siguientes conclusiones:

- IPv6 trae consigo una gran cantidad de mejoras en su implementación para tráficos multimedias, tales como manejo de calidad de servicio mejorada, no fragmentación en los routers intermedios, mayor cantidad de direcciones multicast, alcances que permiten contención de tráfico dentro de un dominio.

- La tecnología IPv6 multicast es un método de transmisión eficiente para tráficos en donde existe unos pocos emisores pero un gran número de receptores. Tanto la utilización del ancho de banda como los requerimientos de hardware necesarios para este tipo de transmisiones son menores en comparación a unicast.

- La infraestrucutura para un servicio IPv6 multicast debe definir una aplicación, una infraestructura de red y unos clientes del servicio.

- Windows Media Services 9 satisface todas las necesidades requeridas para el streaming de audio sobre IPv6 Multicast en equipos Windows XP/Vista/7.

- La implementación realizada se podría extender a toda la UCV. La Dirección de Información y Comunicación de la UCV puede ampliar la Red Interna de Sonido a todo la universidad utilizando este servicio.

Las recomendaciones que se pueden mencionar se basan en la investigación y los resultados obtenidos durante la implementación de este Trabajo Especial de Grado.

- Aunque PIM-SM permite la implementación de muchos servicos multicast, es importante investigar sobre otros protocolos que atienden a necesidades de transmisión más específicas tales como PIM-SSM y PIM-BiDir.

- La implementación de este trabajo permite trasmitir sólo en el dominio autónomo de la UCV, se podrían realizar investigaciones posteriores para transmisiones inter-dominios de tal manera que el producto de esta investigación, asi como cualquier otra pueda llegar a otras redes multicast, como la de REACCIUN2.

- Implementar políticas de QoS para garantizar la entrega de los paquetes multicast cuando exista congestión en la red.

- El proceso de normalización de los archivos de audio MP3 debe realizarse en un equipo distinto del servidor de streaming, debido a que demandan gran utilización de memoria y procesador.

- Durante la implementación en producción de un servidor de WMS se debe considerar:

- Capacidad del Procesador y Número de Procesadores: debido a que WMS genera muchas operaciones I/O, un incremento del número de procesadores no necesariamente incrementará el poder de procesamiento del servidor. Los mejores resultados vienen de la administración de la utilización del procesador, el cual en promedio no debería exceder de un 25%. Por tal motivo se debería evitar en el servidor:
  - La manipulación de listas de reproducción.
  - La ejecución de operaciones de uso intensivo del CPU.
  - Mantener aplicaciones abiertas tales como la consola de administración del WMS.

- Origen de Datos: WMS soporte el streaming de varios origines, la instalación por defecto permite acceso de contenido desde la red (proveniente de otro WMS o codificadores), descargas HTTP, y orígenes desde archivos de datos (almacenados local y remotamente). Para estos últimos se debe tomar en cuanta:
  - Evitar almacenar los archivos de contenido multimedia en el mismo disco duro donde se instaló el sistema operativo.
  - Deshabilitar las operaciones de paginación de archivos en el disco duro donde se almacena el contenido multimedia.
  - Cuando sea posible, almacenar el contenido multimedia en discos duros locales o sistemas de almacenamiento que soporten “file buffering” de Windows Server 2003.

- Ancho de Banda: Uno de los principales causas de los cuellos de botella es la capacidad total de las interfaces de red del servidor, en configuraciones unicast WMS puede alcanzar el 95% de la capacidad de las interfaces de red, por lo que es recomendable utilizar interfaces de 1Gbps. En ambientes multicast las interfaces a 100 Mbps son suficientes. Otras recomendaciones con respecto a las interfaces de red son:
  - Use interfaces de red dedicadas para la entrada y salida de tráfico si el origen del contenido es almacenado remotamente.
  - Las interfaces de red deben soportar transferencias full-duplex.

- Memoria del Sistema: es importante monitorear la memoria utilizada normalmente por el servidor WMS, una vez identificado la utilización promedio se debe proveer por lo menos un 30% más. Si el servidor de WMS excede los 2 GB de utilización de memoria, es recomendable reiniciar el servicio o distribuir la carga entre servidores adicionales.

6. Referencias

RFCs, Estándares y Drafts

[1] S. Deering, R. Hinden, “Internet Protocol, Version 6 (IPv6) Specification”, RFC 2460, Diciembre 1988.

[2] J. Postel, “Internet Protocol”, STD 5, RFC 791, Septiembre 1981.

[3] P. Srisuresh, K. Egevang, “Traditional IP Network Address Translator (Traditional NAT)”, RFC 3022, Enero 2001.

[4] V. Fuller, T. Li, “Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan”, BCP 122, RFC 4632, Agosto 2006.

[5] W. Simpson, “The Point-to-Point Protocol (PPP)”, STD 51, RFC 1661, Julio 1994.

[6] R. Droms, “Dynamic Host Configuration Protocol”, RFC 2131, Marzo 1997.

[7] A. Durand, C. Huitema, “The H-Density Ratio for Address Assignment Efficiency An Update on the H ratio”, RFC 3194, Noviembre 2001.

[8] S. Kent, K. Seo, “Security Arquitecture for the Internet Protocol”, RFC 4301, Diciembre 2005.

[9] Y. Rekhter, B. Moskwitz, D. Karrenberg, G. J. de Groot, E. Lear, “Address Allocation for Private Internets”, RFC 1918, Febrero 1996.

[10] R. Hinden, S. Deering, “IP Version 6 Addressing Architecture”, RFC 4291, Febrero 2006.

[11] R. Hinden, S. Deering, E. Nordmark, “IPv6 Global Unicast Address Format”, RFC 3587, Agosto 2006.

[12] S. Deering, B. Haberman, T. Jinmei, E. Nordmark, B. Zill, “IPv6 Scoped Address Architecture”, RFC 4007, Marzo 2005.

[13] C. Huitema, B. Carpenter, “Deprecating Site Local Addresses”, RFC 3879, Septiembre 2004.

[14] R. Hinden, B. Haberman, “Unique Local IPv6 Unicast Addressing”, RFC 4193, Octubre 2005.

[15] IEEE, “Guidelines for 64-bits Global Identifier (EUI-64) Registration Authority”, http://standards.ieee.org/regauth/oui/tutorials/EUI64.html, Marzo 1997.

[16] M-K. Shin., Y-G. Hong, J. Hagino, P. Savola, E. M. Castro, “Application Aspect of IPv6 Transition”, RFC 4038, Marzo 2005.

[17] P. Savola, B. Haberman, “Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address”, RFC 3956, Noviembre 2004.

[18] B. Haberman, D. Thaler, “Unicast-Prefix-based IPv6 Multicast Address”, RFC 3306, Agosto 2002.

[19] IANA, “Internet Protocol Version 6 Multicast Address”, http://www.iana.org/assignments/ipv6-multicast-addresses, Noviembre 2001.

[20] D. Plummer, “Ethernet Address Resolution Protocol: Or converting network protocol address to 48.bit Ethernet address for transmission on Ethernet hardware”, STD 37, RFC 826, Noviembre 1982.

[21] D. Mills, “Network Time Protocol (Version 3) Specification, Implementation and Analysis”, RFC 1305, Marzo 1992.

[22] S. Thomson, T. Narten, T. Jinmei, “IPv6 Stateless Address Autoconfiguration”, RFC 4862, Septiembre 2007.

[23] T. Narten, E. Nordmark, W. Simpson, H. Soliman, “Neighbor Discovery for IP Version 6 (IPv6)”, RFC-4861, Septiembre 2007.
[24] M. Crawford, “Router Renumbering for IPv6”, RFC 2894, Agosto 2000.
[25] F. Baker, E. Lear, R. Droms, “Procedures for Renumbering an IPv6 Network without a Flag Day”, RFC 4192, Septiembre 2005.
[26] A. Conta, S. Deering, M. Gupta, Ed. “Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification”, RFC 4443, Marzo 2006.
[27] J. McCann, S. Deering, J. Mogul, “Path MTU Discovery for IP version 6”, RFC 1981, Agosto 1996.
[28] S. Deering, W. Feener, B. Haberman, “Multicast Listener Discovery (MLD) for IPv6”, RFC 2710, Octubre 1999.
[29] R. Vida, L. Costa, “Multicast Listener Discovery Version 2 (MLDv2) for IPv6”, RFC 3810, Junio 2004.
[30] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, “Dynamic Host Configuration Protocol for IPv6”, RFC 3315, Julio 2003.
[31] G. Malking, R. Minnear, “RIPng for IPv6”, RFC 2080, Enero 1997.
[32] G. Malkin, “RIP version 2”, RFC 2453, Noviembre 1998.
[33] R. Coltun, D. Ferguson, J. Moy, “OSPF for IPv6”, RFC 2740, Diciembre 1999.
[34] J. Moy, “OSPF Version 2”, STD 54, RFC 2380, Abril 1998.
[35] E. Nordmark, R. Giligan, “Basic Transition Mechanisms for IPv6 Host and Router”, RFC 4213, Octubre 2005.
[36] P.V. Mockapetris, “Domain names – concepts and facilities”, RFC 1034, Noviembre 1987.
[37] P.V. Mockapetris, “Domain names – implementation and specification”, RFC 1035, Noviembre 1987.
[38] S. Thomson, C. Huitema, V. Ksinant, M. Souissi, “DNS Extensions to Support IP Version 6”, RFC 3596, Octubre 2003.
[39] B. Carpenter, K. Moore, “Connection of IPv6 Domains via IPv4 Clouds”, RFC 3056, Febrero 2001.
[40] G. Huston, A. Lord, P. Smith, “IPv6 Address Prefix Reserved for Documentation”, RFC 3849, Julio 2004.
[41] G. Tsirtsis, P. Srisuresh, “Network Address Translation – Protocol Translation (NAT-PT)”, RFC 2766, Febrero 2000.
[42] C. Huitema, “Teredo: Tunneling IPv6 over UDP thorugh Network Address Translations (NATs)”, RFC 4380, Febrero 2006.
[43] S. Deering, “Host Extensions for IP Multicasting”, RFC 1112, Agosto 1989.
[44] J. Postel, “User Datagrama Protocol”, STD 6, RFC 768, Agosto 1980.
[45] J. Postel, “Transmission Control Protocol”, STD 7, RFC 793, Septiembre 1981.
[46] IANA, “Internet Multicast Address”, http://www.iana.org/assignments/multicast-addresses.
[47] D. Meyer, “Administratively Scoped IP Multicast”, RFC 2365, Julio 1998.
[48] D. Meyer, P. Lothberg, “GLOP Addressing in 233/8”, RFC 3180, Septiembre 2001.
[49] IEEE, “Token Ring Access Method and Physical Layer Specifications”, IEEE Standard 802.5-1989, 1989.
[50] ANSI, “Fiber Distributed Data Interface (FDDI)”, ANSI X3T9.5, ISO 9384, 1989.
[51] T. Pusateri, “IP Multicast over Token-Ring Local Area Network”, RFC 1469, Junio 1993.

[52] D. Katz, “Transmission of IP and ARP over FDDI Networks”, STD 36, RFC 1390, Enero 1993.
[53] W. Fenner, “Internet Group Management Protocol, Version 2”, RFC 2236, Noviembre 1997.
[54] B. Cain, S. Deering, I. Kouvelas, B. Fenner, A. Thyagarajan, “Internet Group Management Protocol, Version 3”, RFC 3376, Octubre 2002.
[55] D. Waitzman, C. Partridge, S. Deering, “Distance Vector Multicast Routing Protocol”, RFC 1075, Noviembre 1988.
[56] J. Moy, “Multicast Extensions to OSPF”, RFC 1584, Marzo 1994.
[57] J. Moy, “OSPF Version 2”, RFC 1583, Marzo 1994.
[58] A. Adams, J. Nicholas, W. Siadak, “Protocol Independent Multicast – Dense Mode (PIM-DM): Protocol Specification (Revised)”, RFC 3973, Enero 2005.
[59] A. Ballardie, “Core Based Trees (CBT) Multicasr Routing Architecture”, RFC 2201, Septiembre 1997.
[60] A. Ballardie, “Core Based Trees (CBT version 2) Multicasr Routing –Protocol Specification”, RFC 2189, Septiembre 1997.
[61] B. Fenner, M. Handley, H. Holbrook, I. Kouvelas, “Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised)”, RFC 4601, Agosto 2006.
[62] M. Crawford, “Transmission of IPv6 Packets over Ethernet Networks”, RFC 2464, Diciembre 1998.
[63] C. Partridge, A. Jackson, “IPv6 Router Alert Option”, RFC 2711, Octubre 1999.
[64] M. Christensen, K. Kimball, F. Solensky, “Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches”, RFC 4541, Mayo 2006.
[65] H. Holbrook, B. Cain, “Source-Specific Multicast for IP”, RFC 4607, Agosto 2006.
[66] M. Handley, I. Kouvelas, T. Speakman, L. Vicisano, “Bidirectional Protocol Independent Multicast (BIDIR-PIM)”, RFC 5015, Octubre 2007.
[67] S. Bhattacharyya, “An Overview of Source-Specific Multicast (SSM)”, RFC 3569, Julio 2003.
[68] D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei, “Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification”, RFC 2117, Junio 1997.
[69] D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharma, L. Wei, “Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification”, RFC 2362, Junio 1998.
[70] T. Bates, R. Chandra, D. Katz, Y. Rekhter, “Multiprotocol Extensions for BGP-4”, RFC 4760, Enero 2007.
[71] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, Audio-Video Transport Working Group, RTP: A Transport Protocol for Real-Time Applications, RFC 1889, Enero 1996.
[72] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications”, STD 64, RFC 3550, Julio 2003.
[73] D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, “Generic Routing Encapsulation (GRE)”, RFC 2784, Marzo 2000.
[74] B. Fenner, D. Meyer, “Multicast Source Discovery Protocol (MSDP)”, RFC 3618, Octubre 2003.
[75] ISO/IEC, “Moving Picture Experts Groups (MPEG)”, http://www.chiariglione.org/mpeg, 1998.

[76] R. Hinden, S. Deering, “Internet Protocol Version 6 (IPv6) Addressing Architecture”, RFC 3513, Abril 2003.
[77] Z. Albanna, K. Almeroth, D. Meyer, M. Schipper, “IANA Guidelines for IPv4 Multicast Address Assigments”, BCP 51, RFC 3171, Agosto 2001.
[78] N. Bhaskar, A. Gall, J. Lingard, S. Venaas, “BootStrap Router (BSR) Mechanism for PIM”, draft-ietf-pim-sm-bsr-11.txt, Julio 2007, Expira: Enero 2008.

Libros

[79] B. Williamson, “Developing IP Multicast Networks”, 1ra. Ed., Cisco Press, 2000.
[80] T. Boyles, C. Hucaby, “Cisco CCNP Switching Exam Certification Guide”, 1ra. Ed., Cisco Press, 2001.
[81] C. Popoviciu, E. Levy-Abegnoli, P. Grossetete. “Deploying IPv6 Networks”, 1ra Ed., Cisco Press, 2006.
[82] T. Miyoshi, Y. Tanaka, K. Sezaki, “Topological design comparison for multicast network”, GLOBECOM ’99, 1999.
[83] Ivan Pepelnjak, “EIGRP Network Design Solutions: The Definitive Resource for EIGRP Design, Deployment, and Operation”, Cisco System, 2000.

Páginas Web

[84] C. Kosierok, “The TCP/IP Guide”, http://www.tcpipguide.com
[85] Cisco, “Introduction to Ipv6”, http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/prod_presentation0900aecd80311dff.pdf

Tesis/Publicaciones

[86] S. Kim, J. Lee, T. You, K. Kim, Y. Choi, “HAT: A High-quality Audio Conferencing Tool using MP3 Codec”, http://mmlab.snu.ac.kr/publications/docs/Hat(sykim).pdf
[87] J. Contreras, “Estudio de Factibilidad para el Uso de un Sistema de Comunicación Multimedia Vía IP como Apoyo a la Educacación a Distancia en SADPRO-UCV”, 2008.