IMPLEMENTACIÓN DE UNA RED PARA TRANSMITIR VIDEO STREAMING DE IPV6 A IPV4

JOHANA KATHERINE JUNCA ORTIZ

FUNDACIÓN UNIVERSITARIA SAN MARTÍN
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE ELÉCTRONICA Y TELECOMUNICACIONES
BOGOTÁ, COLOMBIA
NOVIEMBRE 2008

IMPLEMENTACIÓN DE UNA RED PARA TRANSMITIR VIDEO STREAMING DE IPV6 A IPV4

JOHANA KATHERINE JUNCA ORTIZ

MONOGRAFÍA DE GRADO

ASESOR TÉCNICO
ING. JOHN PABLO CRUZ BASTIDAS

FUNDACIÓN UNIVERSITARIA SAN MARTÍN
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE ELÉCTRONICA Y TELECOMUNICACIONES
BOGOTÁ, COLOMBIA
NOVIEMBRE 2008

Nota de Aceptación:

_____
John Pablo Cruz Bastidas
Asesor

_____
Ramsés Martínez
Jurado

_____
Germán Macías
Jurado

Bogotá, noviembre de 2008.

Párrafo de Dedicatoria

Este proyecto esta dedicado a los seres más importantes en mi vida, mis padres mi hermana y mi abuelita que en paz descanse.

AGRADECIMIENTOS

En primer lugar quiero dar gracias a Dios por darme la sabiduría y fortaleza de afrontar esta etapa de mi vida y por permitir que los seres que nombro a continuación estuvieran junto a mí.

Los motores de mi vida son mis padres, a ellos muchas gracias por enseñarme, darme la oportunidad de recibir una educación, por no dejarme derrotar y brindarme el apoyo emocional y económico, a mi hermana por darme ánimo cada vez que veía más lejos la realización de mi proyecto. A mis amigas Luisa, Lina, Angélica, Juliana y Jenny por estar ahí cuando las necesite, porque siempre creyeron en mi y en cada derrota me mostraron el lado positivo y me ayudaron a encontrar solución a los problemas.

A mis compañeros de universidad que durante todos estos meses me apoyaron y colaboraron aportándome su conocimiento, como lo son Mónica, Jahiner, Tatiana, Orlando, Wilson Peña, Irina, Jonathan, Diana, Diego P entre otros que siempre estuvieron pendientes.

No obstante para la realización de este encontré apoyo en muchas personas, cada una de ellas aportaron un granito de arena ya sea para darme ánimo, estar pendientes o colaborándome con cualquier tipo de información, a todos ellos muchas gracias.

De igual forma agradezco a mi asesor John Pablo cruz, quien estuvo dispuesto siempre a colaborarme con cualquier duda, y me guio óptimamente para el desarrollo del proyecto.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

1. RESUMEN

En los últimos años la transmisión de video streaming ha tenido mucho auge en las comunicaciones, debido a que esta tecnología nos permite visualizar en tiempo real cualquier video o audio en la pantalla del computador, sin embargo hoy en día en algunos lugares del mundo permite ser visualizada en teléfonos móvil (celulares). El medio streaming es utilizado para agilizar la descarga y ejecución de un video o audio en Internet, actualmente este servicio es implementado con el protocolo de Internet IPv4, en el cual la transmisión se realiza óptimamente, no obstante las comunicaciones siempre están realizando mejoras a lo ya creado.

Por ello se creo una versión mejorada de IPv4, llamada protocolo de Internet versión 6 o de la nueva generación. Aunque este protocolo se creo en un principio para aumentar la capacidad de direccionamiento, los diseñadores aprovecharon para reparar algunos otros errores que tiene el IPv4, por ejemplo en la transmisión de un video streaming, IPv6 tiene una mejora sobre el protocolo IPv4, puesto que el permite el aumento de direcciones y da oportunidad para gestionar la calidad de servicio (GoS); en el campo del encabezamiento es donde identifica el flujo de trafico y este permitirá a los routers distinguir los datos en un tiempo real, de los correos electrónicos y de la transferencia de archivos(FTP), por lo tanto la descarga de video y la ejecución se realizara en un tiempo menor.

Una pregunta que surgió en el momento de implementar IPv6 fue: ¿Cómo realizar la transmisión de Internet publica, basada en IPv4, a IPv6? Sabiendo de antemano que no se puede pretender asignar un día, un momento exacto, para apagar todas las maquinas existentes en el mundo y actualizarlas, por lo tanto, se presenta como solución consistente la introducción de unos nodos con IPv6, utilizando la estructura ya existente de IPv4, a través de una Dual Stack o un tunnel lo que es más fácil y confiable el enrutamiento entre las dos versiones.

2. INTRODUCCIÓN

Las necesidades de comunicación están cambiando y el resultado es la creciente demanda de los servicios de contenido multimedia sobre redes actuales y su rápida evolución. Es también indiscutible la implantación definitiva del protocolo IP desde los ámbitos empresariales a los domésticos, en este momento existen dos versiones de este protocolo conocidas como IPv4 e IPv6.

Actualmente utilizamos la versión 4 del protocolo de Internet (IPv4) el cual es la base del Internet, este nos permite usar direcciones de 32 bits, es decir 2^{32} que equivale a 4.294.967.267 direcciones únicas, en su mayoría dedicadas a redes locales (LAN), no obstante por el crecimiento que ha tenido el Internet muchas de estas direcciones han sido desperdiciadas, debido a que en un principio se asignaron grandes bloques de direcciones omitiendo que estas se pueden dividir en subredes para que de esta manera no se desperdiciaran tantas de estas. Otros inconvenientes que presenta este protocolo son en cuanto a la seguridad ya que se han tenido que desarrollar protocolos externos, tales como SSH o SSL, de igual manera en la autoconfiguración y movilidad.

Un servicio que aumenta la demanda rápidamente es el streaming de video, día a día se quiere realizar una transmisión más limpia y a una mayor velocidad. La tecnología streaming acelera el proceso de descarga y ejecución de un video en Internet, lo que permite visualizar los archivos en un tiempo real, sin necesidad de descargar primero y luego observar.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar e implementar una red para la transmisión de video streaming de IPv6 a IPv4.

3.2 OBJETIVOS ESPECÍFICOS

- Seleccionar el equipo de transmisión para llevar a cabo el desarrollo del proyecto.
- Diseñar y realizar una conexión que permita la interacción entre IPv6/IPv4.
- Realizar la configuración apropiada, en el equipo de transmisión para comunicar IPv4 e IPv6.
- Definir el tipo de enrutamiento a utilizar
- Implementar un nodo dual stack y/o un túnel que permitan enviar y recibir datagramas de IPv4 e IPv6
- Realizar las pruebas correspondientes utilizando un sniffer para analizar las tramas de IPv4 e IPv6

4. MARCO REFERENCIAL

4.1 ANTECEDENTES

La demanda de las comunicaciones han ido creciendo a través de los años, por eso el hombre se vio obligado a implementar nuevas tecnologías. En las últimas décadas el medio de comunicación mas utilizado es el internet, ya que es una red global que permite el intercambio de información. El internet nace en Estados Unidos aproximadamente hace 30 años, esparciéndose por todo el mundo, creando así el acceso mundial a información.

El internet facilita la comunicación, proporcionando el intercambio de datos, y como es de conocimiento de todos, es más económico y rápido. No obstante cada vez se desarrollan nuevas tecnologías para brindar un mejor servicio. Es por ello que nace la IP (internet protocol) que es un protocolo no orientado a conexión que permite la trasmisión de datos a través de la red. El direccionamiento es tal ves uno de los aspectos mas complejos de este protocolo, lo cual se refiere a la asignación de la dirección IP, como se dividen y agrupan la subredes de los equipos. La dirección IP es un número físico que identifica de manera lógica y jerárquicamente a una interfaz de un dispositivo de red.

Actualmente la versión más utilizada para el direccionamiento es la IPv4, que permite usar direcciones de 32 bits, limitándola a 2^{32} = 4.294.967.296 direcciones únicas. Sin embargo debido al crecimiento que ha tenido internet, se hizo necesario crear una nueva versión que permita utilizar un mayor número de direcciones, esta es llamada IPv6, que usa direcciones de 128 bits, es decir 2^{128} que equivale aproximadamente a 16 trillones de direcciones.

Igualmente por dicho crecimiento de usuarios de internet, han surgido diversas aplicaciones, entre ellas están los servicios multimedia, de allí el video streaming, el cual permite que se pueda ver video en tiempo real sin la necesidad de descargarlo primero.

4.2 MARCO TEÓRICO

4.2.1 Protocolo de Internet (IP) [MILLA2003]

El Protocolo Internet está diseñado para su uso en sistemas interconectados de redes de comunicación de ordenadores por intercambio de paquetes. El protocolo Internet proporciona los medios necesarios para la transmisión de bloques de

datos llamados datagramas desde el origen al destino, donde origen y destino son hosts identificados por direcciones de longitud fija. El protocolo Internet también se encarga, de la fragmentación y el reensamblaje de grandes datagramas para su transmisión a través de redes de trama pequeña.

El protocolo IP define los mecanismos de la distribución de paquetes no fiable y sin conexión en redes heterogéneas. Por lo tanto, se pueden producir perdidas, duplicaciones y desordenes de los datagramas, que tendrán que ser tratados en los niveles superiores. Entre las funciones más importantes de IP está encapsular el paquete procedente de capas o niveles superiores en un datagrama y encaminar dichos datagramas.

La versión actual de IP es la 4. La siguiente generación del protocolo Internet surgió en el seno de IETF (Grupo de Trabajo en Ingeniería de Internet) en el año 1994, principalmente por la falta de direcciones de IP que anunciaba un cuello de botella insalvable al crecimiento de la red Internet. El documento final que recoge el estándar IPv6 fue publicado en el año 1996 y las últimas revisiones, principalmente en su cabecera, han tenido lugar durante el año 2000. El nombre formal de este protocolo es IPv6

La versión IPv6 puede ser instalada como una actualización de software en los dispositivos de red de Internet e interoperar con la versión actual IPv4. IPv6 está diseñado especialmente para redes de alto rendimiento, como por ejemplo las redes ATM, pero manteniendo la eficiencia en redes de bajo ancho de banda, como en redes inalámbricas. Además, ofrece una plataforma para la nueva funcionalidad de Internet que será necesaria en un futuro inmediato. La necesidad de migrar a IPv6 está originada por las nuevas tendencias en el mundo actual de las telecomunicaciones, que podemos resumir en: La creciente movilidad de los usuarios de Internet, que desean acceder a los mismos servicios en cualquier momento y desde cualquier lugar. Las redes domesticas con avanzados sistemas de tele vigilancia, control, y seguridad. La convergencia de voz, video y datos, en infraestructuras basadas en IP.

Por lo tanto son muchos los asuntos que debían ser considerados en el diseño de IPv6. Por ejemplo, el nuevo protocolo debía ser capaz de soportar grandes redes y ofrecer un sencillo y rápido mecanismo de migración para la base de sistemas IPv4 instalados. En efecto, uno de los problemas de IPv4 es la gran dimensión de las tablas de encaminamiento en la red troncal de Internet, que la hace ineficaz y perjudica considerablemente los tiempos de respuesta. En IPv6 el encaminamiento en la red troncal es más eficiente, debido a una jerarquía de direccionamiento basada en la agregación, y a que la fragmentación y desfragmentación de los paquetes se realiza de extremo a extremo. Sin embargo, la principal razón que originó la necesidad de IPv6 fue la evidente falta de direcciones, derivada del crecimiento de la red Internet. El límite en el espacio de estas fue agravado por la falta de coordinación en la delegación de direcciones, dejando grandes espacios discontinuos.

En IPv6 el espacio de direcciones se incrementa de 32 a 128 bits, soportando más niveles de jerarquías de direccionamiento, un mayor número de nodos direccionales, y la autoconfiguración de las direcciones.

No obstante, la falta de direcciones no es igual en todos los puntos de la red. Por ejemplo, es casi inapreciable por el momento en Norteamérica, mientras que en zonas como en Europa y Asia, la situación es crítica. Sin embrago, este problema es creciente, debido principalmente al desarrollo de la telefonía móvil y la inminente aparición comercial de la tercera generación de comunicaciones móviles o UMTS (Universal Mobile Telecommunications System). Los móviles se convertirán en dispositivos siempre conectados a Internet y será necesario asignarles una dirección IP fija y única.

La solución adoptada por los proveedores de servicios Internet para solventar los problemas de direcciones IP ha sido proporcionar a sus clientes direcciones IP privadas, es decir, no reconocidas en Internet, mediante mecanismos de traslación de direcciones o NAT (Network Address Translation). Es decir, se usa una sola dirección IP pública para toda una red privada. No obstante, este mecanismo no puede utilizarse en los terminales móviles, además, muchas aplicaciones son incapaces de ser utilizadas mediante este tipo de direcciones, especialmente las relacionadas con la autenticación y la seguridad de las comunicaciones.

Pese a esto, IPv4 presenta otros problemas o dificultades que la nueva versión soluciona o mejora. Por ejemplo, IPv4 no está preparado para soportar las nuevas aplicaciones de la red Internet como la transmisión de video y audio en tiempo real, ni mecanismos de seguridad avanzada sobre los datos transmitidos.

Para reducir el tiempo de procesamiento de los paquetes, se ha simplificado el formato de la cabecera de IPv4 y se ha introducido el concepto de flujo, consiguiendo que los routers, además de encaminar, puedan conmutar algunos de los paquetes que procesan. Por otro lado, se ha mejorado el mecanismo de codificación de los campos optativos en la cabecera, dando una mayor flexibilidad para la introducción de nuevas opciones futuras. Finalmente, IPv6 ha mejorado las capacidades de autenticación y privacidad de los datos transmitidos. De esta forma, en IPv6 una cabecera de autenticación garantiza que un paquete procede del origen que realmente se indica, mientras que en IPv4 el paquete podría venir de un origen distinto al indicado en la cabecera.

La transición de IPv4 a IPv6 no tendrá lugar de la noche a la mañana. Las dos versiones de IP deberán coexistir durante muchos años. Básicamente, IPv6 puede ser implementado como una actualización software en los nodos IPv4 actuales, comenzando un periodo de transición para minimizar los costos de nuevos equipos y proteger las fuertes inversiones realizadas. Sin embargo, es difícil saber cuándo migrarán las operadoras en Internet a la tecnóloga IPv6. En la actualidad la gran mayoría de las operadoras utiliza nodos IPv4, y con esta situación, donde

casi todo el tráfico debería adaptarse a redes basadas en IPv4, la motivación para el cambio es muy baja.

Las nuevas características de autoconfiguración, que hacen que las redes IPv6 sean más fáciles de configurar y mantener que las redes IPv4, pueden ser atractivas para nuevas operadoras que han de realizar un despliegue de infraestructura muy rápido. Por otro lado, para facilitar la migración es importante que las aplicaciones IPv4 existentes sean capaces de operar también con las aplicaciones IPv6; por ejemplo, los navegadores de Internet deben ser capaces de comunicarse utilizando IPv6 e IPv4. El principal problema es, que mientras los sistemas IPv6 son compatibles hacia atrás, es decir, pueden enviar, encaminar y recibir paquetes IPv4, los sistemas IPv4 actuales no son capaces de manejar paquetes IPv6. Lo ideal sería declarar unos días de inactividad, durante los cuales todas las máquinas de Internet serían desactivadas y se migraría de IPv4 a IPv6. No obstante, una tarea así, con millones de máquinas y de administradores de redes implicados, es prácticamente imposible.

Para dar solución a esta limitación se tiene la opción de introducir una dual stack completa de protocolos, IPv4 e IPv6, en los nodos IPv6. De esta forma, este nodo IPv6/IPv4 puede enviar y recibir paquetes IPv6 e IPv4. Cuando trabaje con un nodo IPv4, el nodo IPv6/IPv4 puede utilizar paquetes IPv4; cuando trabaje con un nodo IPv6, puede utilizar paquetes IPv6. Los nodos IPv6/IPv4 deben tener tanto direcciones IPv6 como IPv4. Deben ser capaces también de descubrir si otro nodo es capaz de utilizar IPv6 o sólo IPv4. Esto se puede conseguir utilizando el protocolo de resolución de nombres de dominio (DNS), que puede devolver una dirección IPv6 si el nombre del nodo que se está resolviendo es capaz de utilizar IPv6, o bien una dirección IPv4 en caso contrario. Por supuesto, si el nodo que hace la petición DNS únicamente puede utilizar IPv4, DNS devolverá sólo una dirección IPv4.

Según este método, si cualquiera de los nodos intermedios sólo puede operar con IPv4, se deben utilizar paquetes IPv4. Por ello, es posible que la comunicación entre dos nodos extremos IPv6 tenga lugar con paquetes IPv4. Lo que se hace es que ambos extremos envían paquetes IPv6, pero cuando estos lleguen a un nodo IPv4, todo el paquete IPv6 será encapsulado en el campo de datos del paquete IPv4 y se llevará cabo un mapeo o correspondencia de direcciones, perdiendo la información relevante de los campos de la cabecera IPv6.

4.2.2 Protocolo de Internet versión 4 (IPv4) [VERD2000]

El protocolo IP facilita un sistema sin conexión y no fiable de entrega de datagramas entre dos ordenadores cualesquiera conectados a Internet.

La primera versión del protocolo de Internet que se implemento fue la IPv4. El cual usa direcciones de 32 bits. Los bits se dividen en dos campos: el campo de subred, que identifica la subred a la que está conectado el sistema, y el campo de sistema, que identifica al equipo dentro de la subred.

4.2.2.1 Cabecera IPv4

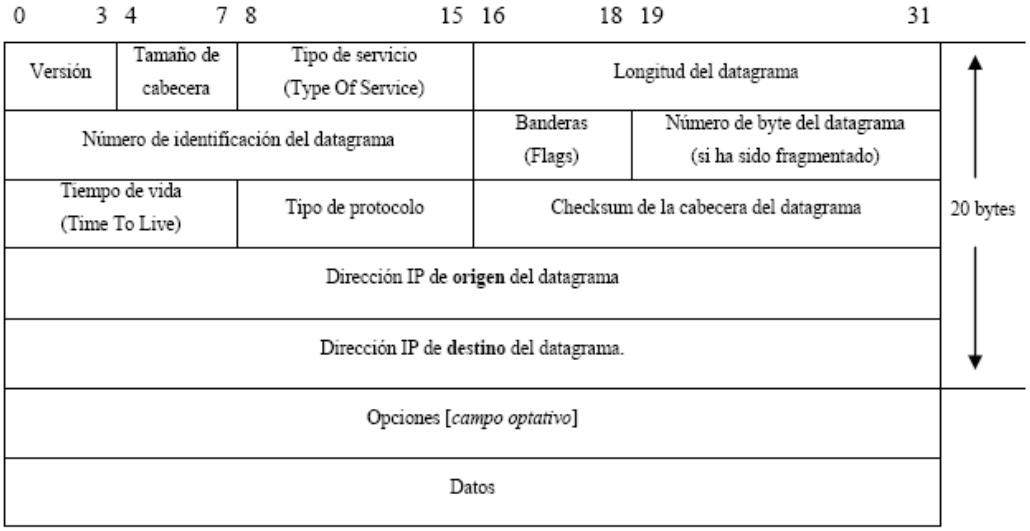


Figura 1. Cabecera IPv4 [STAL2000]

- **Versión (4 bits):** Sirve para identificar a que versión específica. Esta información sólo es utilizada por los routers y capa IP de origen y final del datagrama. Esto permite la coexistencia de diferentes versiones del protocolo IP de una forma transparente al usuario. La versión actual es la 4 (conocida también cómo IPv4).

- **Tamaño de la cabecera Internet (IHL, Internet Header Length) (4 bits):** Longitud de la cabecera enumerada en palabras de 32 bits. Son 4 bits (2^4 = 16 posiciones, 0 al 15) que indican el número de palabras de 32 bits que ocupa la cabecera. Estos 4 bits de tamaño máximo, nos limitan a un tamaño de cabecera máximo de 60 bytes (15 * 32 bits = 60 bytes). No obstante, el valor usual de este campo es 5 (5 * 32 bits = 20 bytes).

- **Tipo de servicio (8 bits):** Define los parámetros de seguridad, prioridad, retardo y rendimiento. Se compone de 8 bits. Los primeros 3 bits tienen una

función obsoleta y no se contemplan actualmente. Los 4 bits siguientes definen el tipo de servicio y el último bit no se utiliza actualmente y debe tener valor 0. Solo 1 de los 4 bits del tipo de servicio puede estar activo a la vez. El tipo de servicio determina la política a seguir en el envío del datagrama por Internet. Las opciones posibles son minimizar el retraso, maximizar el rendimiento, maximizar la fiabilidad del transporte y minimizar el costo del transporte.

- **Longitud del datagrama (16 bits):** Es un número de 16 bits (2^{16} = 65536) que indica la longitud total del datagrama. Este valor es muy importante, ya que nos permite saber que tamaño de memoria debemos reservar para la recepción del datagrama. Además, nos indica el número de bytes a leer, lo que nos permite un simple control de error. De esta forma, si el valor es incorrecto, el número de bytes leídos será como máximo de 65535, acotando el error. Además nos limita el número de bytes a enviar en un datagrama: 65535 – 20 = 65515 bytes. Si el tamaño del datagrama, es mayor que el tamaño máximo del paquete de red, se fragmenta en N trozos.

- **Número de identificación del datagrama (16 bits):** Es un número de 16 bits que en caso de fragmentación de un datagrama nos indica su posición en el datagrama original. Esto nos permite recomponer el datagrama original en la máquina de destino. Este valor nos indica que un datagrama puede ser fragmentado en un máximo de 65535 fragmentos.

- **Banderas (3 bits):** Son 3 bits. El primero permiten señalar si el datagrama recibido es un fragmento de un datagrama mayor. El segundo especifica si el datagrama no debe fragmentarse y el tercero no se utiliza actualmente.

- **Número de byte en el datagrama (13 bits):** Nos indica la posición en bytes que ocupan los datos en el datagrama original. Sólo tiene sentido si el datagrama forma parte de uno mayor que ha sido fragmentado. Este campo tiene un máximo de 13 bits (2^{13}= 8192, como nos indica el desplazamiento en bytes 8192 * 8 bits = 65536). De esta forma, podemos reconstruir el datagrama original con los fragmentos.

- **Tiempo de vida (8 bits):** Es un campo de 8 bits que indica el tiempo máximo que el datagrama será válido y podrá ser transmitido por la red. Esto permite un mecanismo de control para evitar datagramas que circulen eternamente por la red. Este campo se inicializa en el ordenador de origen a un valor (máximo 2^8 = 256) y se va decrementando en una unidad cada vez que atraviesa un router. De esta forma, si se produce un bucle y/o no alcanza su destino en un máximo de 255 “saltos”, es descartado. Entonces se envía un datagrama ICMP (Protocolo de Control de Mensajes de Internet) de error al ordenador de origen para avisar de su pérdida.

- **Tipo de protocolo:** Es un valor que indica a que protocolo pertenece el datagrama (TCP, UDP, ICMP...). Es necesario debido a que todos los servicios de Internet utilizan IP como transporte, lo cual hace necesario un mecanismo de discriminación entre los diferentes protocolos.

- **Checksum de la cabecera del datagrama:** Es una suma de comprobación que afecta sólo a la cabecera del datagrama IP. El resto de protocolos TCP, UDP, IGMP... tienen su propia cabecera y checksum. Su función es simplemente la de un mecanismo de control de errores. De esta forma, si se encuentra un error en el checksum de un datagrama IP, este es simplemente descartado y no se genera ningún mensaje de error. Esto implica que es deber de las capas superiores el control del flujo de los datagramas. Asegurándose que estos lleguen correctamente al destino, ya sea utilizando un protocolo fiable (TCP) o implementando internamente algún tipo de control.

- **Dirección origen (32 bits):** Está formada por dos números de 32 bits. Codificada para permitir una asignación variable de bits para especificar la red y el sistema final conectado a la red.

- **Dirección destino (32 bits):** Está formada por dos números de 32 bits. Ocurre lo mismo que en el campo anterior.

- **Opciones (variable):** Contiene las opciones solicitadas por el usuario que envía los datos.

- **Datos (variable):** El campo de datos debe tener una longitud múltiplo de 8 bits. La máxima longitud de un datagrama es de 65.535 octetos.

4.2.2.2 Direccionamiento IPv4 [MILLA2003]

La dirección IP es un número que me identifica el computador y la red. Pertenece la capa 3 del modelo OSI. En su versión 4, las direcciones IP constan de 32 bits, los cuales se dividen en cuatro octetos, cada uno con un valor decimal entre 0 y 255.

Existen cinco diferentes clases de red, las cuales proporcionan flexibilidad en la asignación de direcciones a los host y me permite una mezcla de tamaños de red en un conjunto de redes, clasificadas como se observa en la tabla1 y 2, estas son:

- **Clase A:** En el primer octeto se asigna la dirección de red y en los tres restantes los host, es decir pocas redes, con muchos computadores. El primer bit más significativo es 0. El número total de bits dedicados a la red es de 7, con lo cual se tienen hasta 128 redes, en cada una de las cuales

puede haber hasta más de 16 millones de servidores diferentes. Los propietarios típicos de estas direcciones son grandes compañías o países enteros, como por ejemplo IBM o Japón.

- **Clase B:** Los dos primeros octetos hacen referencia a la red y los dos restantes a los host, es decir, un número equivalente entre redes y computadores. Los dos primeros bits son 10. El número de bits dedicados a la red es de 14, con lo cual se tienen hasta unas 16.000 redes, en cada una de las cuales puede haber hasta más de 65.000 servidores diferentes. Los propietarios de este tipo de redes son grandes compañías.

- **Clase C:** Los tres primeros octetos hacen referencia a la red y los dos restantes a los host, es decir, muchas redes con pocos computadores. Los tres primeros bits son 110. El número total de bits dedicados a la dirección de red es de 22, con lo cual se tienen hasta casi 2 millones de redes, con hasta 255 servidores diferentes en cada una de ellas. Los propietarios son compañías medianas o pequeñas.

- **Clase D:** Los cuatro primeros bits son 1110. Se utilizan para el multicasting, es decir, para tráfico de datos con varios destinatarios, como por ejemplo, las videoconferencias o las noticias de radio a través de Internet.

- **Clase E:** Los cuatro primeros bits son 1111. Se utiliza con fines experimentales.

Las redes pueden ser divididas en redes más pequeñas de carácter local, denominadas subredes, a través de un proceso conocido como subnetting. El subnetting proporciona al administrador varios beneficios, como una flexibilidad adicional, un uso más eficiente de las direcciones de red, y la capacidad de soportar tráfico de broadcast (El tráfico de broadcast nunca atraviesa los routers).

La subred es creada tomando parte de los bits correspondientes al campo de servidor, denotándolos por campo de subred. El número de bits varía y viene especificado por la máscara de subred. El enmascaramiento de subred aislada asigna un 1 binario a los bits que pertenecen a la parte de red, y un 0 binario a los bits que pertenecen a la parte de la dirección local. La máscara de subred local será utilizada por los routers aplicando una operación and lógica sobre los paquetes que reciben, con el fin de encaminar en función de la dirección de red.

El concepto contrario al subnetting es el supernetting o CIDR (Classless Inter-Domain Routing). Debido a los pocos niveles de jerarquía de las direcciones, que sólo consideran una parte de subred y otra de sistema, las tablas de encaminamiento de las redes troncales de Internet han crecido enormemente, reduciendo la eficiencia de los routers. El supernetting divide las direcciones en bloques de tamaño variable.

En la tabla 1. Se indica el número de redes y hosts equivalente a cada clase de direccionamiento IPv4 y en la tabla 2 se encuentra el rango de direccionamiento de dichas clases

Clase	Redes	Hosts	Primer octeto
A	128	16 millones	0-127
B	16.000	65.000	128-191
C	2 millones	255	192-223
D	Multicasting	-	224-239

Tabla 1. Clases de red IPv4 [MILLA2003]

CLASE	RANGO		
A	0.0.0.0	Hasta	127.255.255.255
B	128.0.0.0	Hasta	191.255.255.255
C	192.0.0.0	Hasta	223.255.255.255
D	224.0.0.0	Hasta	239.255.255.255
E	240.0.0.0	Hasta	247.255.255.255

Tabla 2. Clases de direcciones IPv4 [VERD2000]

Este tipo de direccionamiento, nos permite una gran flexibilidad a la hora de definir redes que posteriormente conectaremos a Internet. Así, una clase A sería ideal para redes muy grandes, ya que permite 128 redes (2^7) de 16.777.216 (2^{24}) ordenadores cada una. Mientras que una clase B permite 16.384 (2^{14}) redes con 65.535 ordenadores, y una clase C permite 2.097.152 (2^{21}) redes de 256 ordenadores.

Las clases D (multicast) y E (reservada) se utilizan para diferentes posibilidades como la de tener ordenadores en redes diferentes y que se vieran como si estuvieran en la misma.

La subdivisión de bits en cada una de las clases de direccionamiento IPv4 se muestra en la siguiente figura:

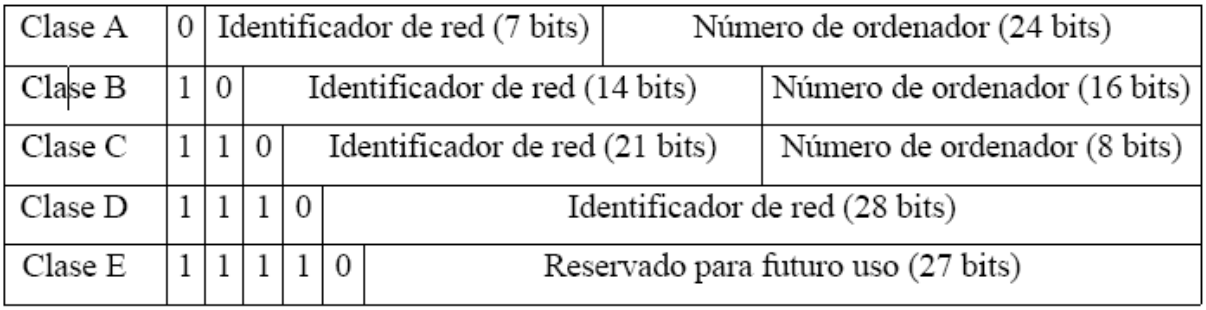


Figura 2. Subdivisión de los 32 bits para las clases A, B, C, D y E. [VERD2000]

4.2.2.3 Seguridad en IPv4 [VERD2000]

La seguridad en la versión 4 de IP no fue contemplada en su diseño original, con lo que al querer introducir ampliaciones en las especificaciones IP se encontraron muchos problemas, entre ellos la gran cantidad de software que debía modificarse para adoptar esta ampliación debido al gran tamaño que ya tenía Internet. Además se tardó mucho tiempo en finalizar las nuevas especificaciones, con lo que al desarrollarse el comercio electrónico, las empresas de venta por Internet puesto que no podían modificar ninguna definición de los protocolos (IP, TCP, UDP...) fueron desarrollando e imponiendo los suyos en los niveles que podían modificar, los correspondientes a la capa de aplicación.

A continuación se describen algunas de las soluciones de seguridad adoptadas:

SSL (Secure Socket Layer) es un protocolo ampliamente utilizando que se basa en una arquitectura de tipo cliente/servidor y que permite una comunicación segura entre dos aplicaciones. Este protocolo permite la negociación de un algoritmo de cifrado y de las claves necesarias para asegurar un canal de seguridad entre el cliente y el servidor. Este canal tiene tres propiedades principalmente:

- El canal garantiza la privacidad. Después del negociado de la clave privada todos los mensajes son cifrados.

- El canal garantiza la autenticidad. El servidor siempre se autentifica mientras que los clientes pueden hacerlo o no.

- El canal garantiza la fiabilidad. Los mensajes incluyen una integridad proporcionada por el uso del sistema MAC.

S-HTTP (Secure Hypertext Transfer Protocol): Es una extensión del protocolo HTTP utilizado en el servicio WWW que proporciona seguridad en el intercambio de documentos multimedia. Proporciona servicios de confidencialidad, autenticidad, integridad y no repudio (poder demostrar a una tercera persona que la información recibida proviene realmente del emisor). Asimismo permite múltiples algoritmos de cifrado (DES, DESX, IDEA y RC2) y de intercambio de claves (RSA, Kerberos, Out-band e Inband)

SET (Secure Electronic Transaction): Es un protocolo desarrollado por las empresas VISA [WWW30] y MASTERCARD [WWW21] para las transacciones electrónicas. Soporta los protocolos DES y RSA para el intercambio de claves y el cifrado de datos, además proporciona los siguientes servicios:

- Transmisiones confidenciales.
- Autenticación de los dos usuarios.
- Comprobación de la integridad en los pagos y las cantidades.
- Autenticación cruzada (del comerciante ante el usuario y del usuario al comerciante).

4.2.3 Protocolo de Internet versión 6 (IPv6) [VERD2000]

El principal motivo que llevo a crear una nueva versión del protocolo de Internet, es debido a la falencia en la asignación de direcciones en los últimos años, ya que con IPv4 se asigna 2^{32} direcciones, que equivale a 4.294.967.267 direcciones únicas, mientras que con ipv6 se pueden asignar hasta 128 bits de direcciones. No obstante se aprovechó en mejorar otras fallas de IPv4.

Esta nueva revisión del protocolo IP se numerará con la versión 6. No se la denominará versión 5 para evitar posibles confusiones, ya que anteriormente a esta revisión se hicieron algunas pruebas añadiendo extensiones a la versión 4. Estas extensiones experimentales no acabaron de formalizarse en una nueva versión del protocolo, con lo que para evitar posibles conflictos de numeración y/o confusión, se optó por elegir el número de versión 6.

El surgimiento de IPv6 se da a principios de los 90´s, cuando en 1991 el Internet Engineering Task Force (EITF) empezó a trabajar en un nuevo protocolo que resolviera en primer lugar lo anteriormente nombrado, que es referente a la saturación de dirección IPv4 y adicionar a este nuevo protocolo características que no se tuvieron en cuenta en el diseño de IPv4. En 1992 surgió una nueva área de investigación llamada Internet Protocol Next Generation (IPng) considerada por el EITF para el desarrollo de este nuevo protocolo.

El 1993 fue distribuido el RFC 1550 [8], el cual invitaba a todos los interesados a participar dando comentarios acerca de cualquier requerimiento específico que consideraran pertinente incluir en IPng. En el RFC 1726 [9], el grupo IPng definió un conjunto de criterios que debían ser tomados en cuenta en el proceso de evolución del IPng y son las siguientes:

- Escalabilidad: El nuevo protocolo debería ser capaz de identificar y direccionar por lo menos 10^{12} sistemas finales y 10^{9} redes individuales.

- Flexibilidad topológica: La arquitectura de enrutamiento y protocolos para IPng debían permitir utilizar muchas topologías distintas de red.

- Rendimiento: Para IPng los host deberían ser capaces de transferir datos a tasas comparables a las alcanzadas con IPv4 utilizando niveles similares de recursos máquina.

- Servicio robusto: El servicio de red junto con los protocolos de control y enrutamiento para IPng deberían ser suficientemente robustos.

- Transición: Debían existir mecanismos para realizar la transición de IPv4 hacia IPng de manera transparente para los protocolos y aplicaciones de las capas superiores.

- Independencia del medio: Este nuevo protocolo debe trabajar a través de una Internet con diferentes medios LAN, WAN y MAN, así como distintas velocidades de conexión, que van desde algunos bits/segundo hasta cientos de giga bits/segundo.

- Servicio de datagramas no confiables: En nuevo protocolo debía soportar un servicio no confiable de entrega de datagramas.

- Configuración, Operación y Administración: Este nuevo protocolo también debía permitir conexiones fáciles, además de operación y configuración ampliamente distribuida. También debía permitir la configuración automática de host y enrutadores.

- Operación segura: IPng también debía proveer una capa de red segura (IPSec).

- Acceso y documentación: Los protocolos que definen a IPng, sus protocolos asociados y protocolos de enrutamiento deberían ser publicados en los RFC, así como estar disponibles libremente y no requerir licencia para su implementación.

- Nombrado único: IPng debía asignar a todos los objetos de la capa IP de manera global nombres de Internet únicos.

- Multicast: IPng debía soportar transmisión de paquetes Unicast y Multicast.

- Extensibilidad: IPng debía ser capaz de evolucionar para cubrir las necesidades futuras del Internet. Así mismo, conforme este evolucione, debería permitir diferentes versiones de él, que puedan coexistir sobre la misma red.

- Servicio de red: IPng debía permitirle a la red asociar paquetes con clases de servicio en particular y proveerlas con los servicios especificados por esas clases.

- Movilidad: El protocolo debía soportar huéspedes, redes e Inter redes móviles.

- Protocolo de control: El protocolo debía incluir soporte elemental para probar y depurar redes.

- Redes privadas: Por último, IPng debía permitir a los usuarios construir redes privadas sobre la infraestructura básica de red, soportando ambas, redes basadas ó no basadas en IP.

Finalmente después de analizar cada uno de los anteriores puntos en 1995 se resumieron en los siguientes tres criterios:

- Arquitectura Común para el Protocolo de Internet de la Siguiente Generación (CATNIP).
- Protocolo de Internet Simple Plus (SIPP).
- TCP/IP con Direcciones más Grandes (TUBA).

CATNIP proponía una concordancia entre Internet, OSI y los protocolos Novell. Para lograrlo integraba protocolos de red tales como IP, Novell's Internetwork Packet Exchance (IPX) e ISO Connectionless Network Protocol (CLNP). El diseño de CATNIP permitía un gran número de protocolos de transporte, tales como el ISO Transport Protocol, class 4 (TP4), Connectionless Transport Protocol (CLTP), TCP, UDP, y Novell's Sequenced Packet Exchange (SPX), sin embargo los revisores de esta propuesta sintieron que CATNIP solo cumplía con cinco de los criterios establecidos, dos más no eran cumplidos y no tenían una conclusión acerca de los criterios restantes.

SIPP, por su parte proponía una evolución a IPv4, por esto, todas las funciones de IPv4 que les parecieron buenas fueron mantenidas en su nueva propuesta,

también fue aumentado el tamaño de las direcciones de 32 a 64 bits de longitud y lo mejor de todo, su instalación sería como una actualización de software. SIPP además sería interoperable con IPv4. En cuanto a esta propuesta, los revisores decidieron que SIPP cumplía con diez de los criterios clave, dos criterios no eran cumplidos y no tenían una conclusión acerca de los criterios restantes.

TUBA proponía remplazar IPv4 con CLNP, lo cual traía consigo dos beneficios inmediatos: incremento en el espacio de direcciones y permitir a protocolos de la capa de transporte operar de manera transparente. Los revisores de TUBA determinaron que esta propuesta cumplía con cinco de los criterios clave, no cumplía un criterio y no tenían una conclusión acerca de los criterios restantes.

Como resultado de las revisiones a estas tres propuestas se decidió elegir a SIPP, incorporarle direcciones de 128 bits de longitud y hacer algunas otras modificaciones. El resultado final a todas estas modificaciones es lo que se conoce actualmente como IPv6 ó IPng.

4.2.3.1 Cabecera IPv6

La nueva cabecera del protocolo IP versión 6, no es mas que una evolución de la anterior versión. No se han introducido grandes cambios de contenido o estructura, sino que simplemente se ha mejorado y optimizado con los conocimientos y experiencias adquiridas durante los últimos 20 años. Se han suprimido algunos campos redundantes u obsoletos y se han ampliado algunas características para hacer frente a las nuevas necesidades de los usuarios (comunicaciones en tiempo real, seguridad...).

La nueva estructura de la cabecera del protocolo IP versión 6 mostrado en la figura 4, se caracteriza principalmente por dos particularidades:

- **Direcciones de 128 bits**. Se ha creado una nueva estructura de direccionamiento que aumenta su tamaño de 32 bits a 128 bits. Este aumento es consecuencia del gran aumento que ha sufrido Internet en los últimos años, agotando el número de direcciones existentes y colapsando las tablas de encaminamiento de los routers.

- **Campos de longitud fija**. Con el objetivo de minimizar el tiempo necesario para procesar y encaminar los datagramas por Internet, se adopta un formato fijo. De esta forma se agiliza el tráfico de datagramas y se suprimen opciones poco utilizadas. No obstante se mantiene la posibilidad de especificar opciones, pero ya sin formar parte de la cabecera IP como ocurría anteriormente.

El encabezado de un paquete IPv6 consta de dos partes: Un encabezado IPv6 base y una extensión de encabezados opcionales, tal y como puede verse en la figura 3:

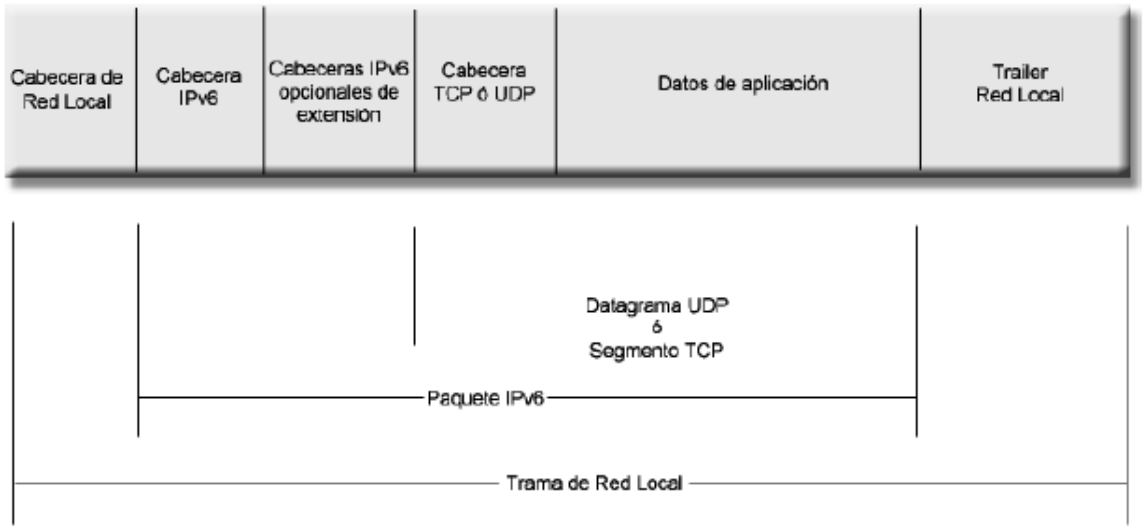


Figura 3 Formato de una trama IP

Un paquete IPv6 puede tener cero, uno o más encabezados opcionales. Cada encabezado opcional tiene una longitud múltiplo de 8 bits y deben ser colocadas en el orden mostrado en la tabla 3.

El protocolo IP versión 6 sigue siendo al igual que las versiones anteriores, un protocolo no fiable y sin conexión. Esto continua siendo así debido a que la experiencia ha enseñado que este sistema funciona y da flexibilidad a la comunicación. Además permite que sean los protocolos de las capas superiores los encargados de mantener un estado de conexión o fiabilidad según crean necesario, manteniendo la estructura en capas del modelo TCP/IP.

El único campo que se mantiene en la misma posición y con el mismo significado que en formatos anteriores es el de versión, debido a que durante el tiempo de implantación de la nueva versión convivirán simultáneamente la versión 4 y 6. De esta forma, los routers podrán saber rápidamente si el datagrama que reciben es de una versión u otra.

Se han suprimido seis campos (tamaño de cabecera, tipo de servicio, número de identificación del datagrama, banderas, numero de byte del datagrama fragmentado y el checksum) respecto la versión 4 del protocolo IP. Además se han redefinido los campos de longitud del datagrama, tiempo de vida y de tipo del protocolo. Como se observa en la figura 4.

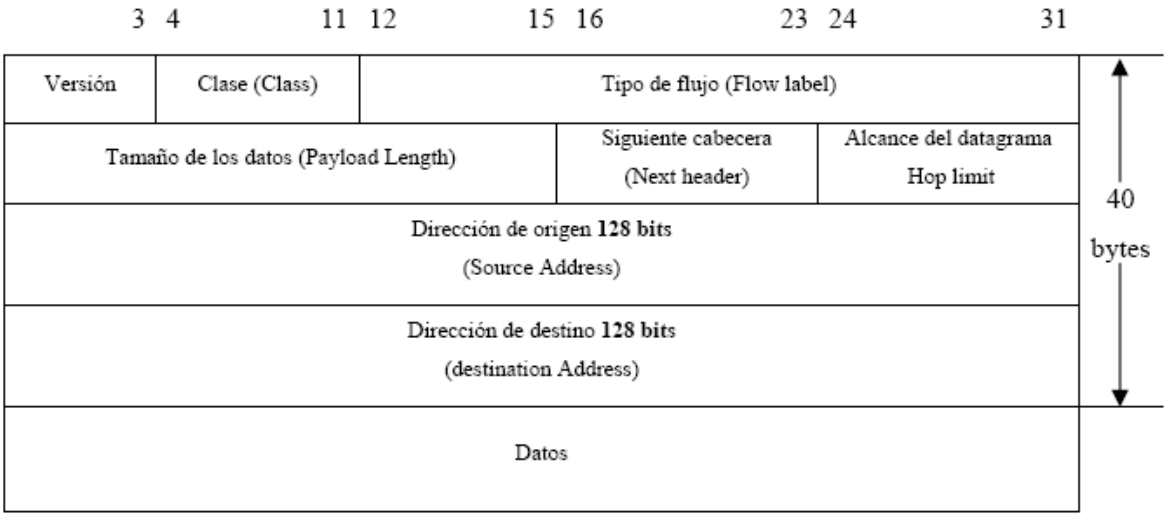


Figura 4. Estructura de un datagrama IPv6. [VERD2000]

- **Versión (4 bits):** Se sigue manteniendo como el primer campo del datagrama. Esto es así para mantener la compatibilidad con formatos anteriores y porque permite de una forma sencilla y rápida discriminar que versión de datagrama se recibe, facilitando a los routers el proceso de discriminar entre versión 4 y versión 6.

- **Clase:** Es un número de 8 bits que hace referencia a la prioridad del datagrama. Este campo es una de las nuevas aportaciones para conseguir algunos tipos de aplicaciones (videoconferencia, telefonía…) puedan realizarse en tiempo real.

- **Tipo de flujo:** Se compone de 16 bits, que permiten especificar que una serie de datagramas deben recibir el mismo trato. Esto es aplicable por ejemplo a una serie de datagramas que van del mismo origen al mismo destino y con las mismas opciones. Junto con el campo de clase permiten aplicaciones en tiempo real.

- **Tamaño de los datos:** Al igual que en la versión 4, es un número de 16 bits, lo que permite un tamaño máximo en principio de 2^{16} = 65536 bytes (64K). No obstante, a diferencia de la versión 4, este número hace referencia sólo al tamaño de los datos que transporta, sin incluir la cabecera

- **Siguiente cabecera: E**s un valor de 8 bits que indica al router si tras el datagrama viene algún tipo de extensión u opción. Este campo substituye al campo de banderas de la versión 4. De esta manera, en lugar de complicar la cabecera IP con la interpretación de los diferentes bits de opciones, se sitúan fuera del datagrama básico. En la versión 6 del protocolo IP se definen una serie de cabeceras de extensión que se colocan justo después

de los datos en forma de cadena y que permiten al usuario personalizar el tipo de datagrama. De tal forma que podemos tener varias extensiones de cabecera tan solo indicando en el campo de siguiente cabecera de cada una de ellas el tipo de la cabecera que vendrá a continuación.

- **Alcance del datagrama:** Es un número de 8 bits que indica el número máximo de routers que puede atravesar un datagrama hasta llegar a su destino. Este campo es el equivalente al tiempo de vida (TTL) de la versión 4. Cuando un datagrama llega a un router y es encaminado hacia otro ordenador, este campo es decrementado en una unidad. Este campo es necesario para evitar que los datagramas circulen infinitamente por la red, eliminándose al llegar a 0 (su valor máximo es de 2^8 = 256). De este tamaño podemos deducir que para que exista comunicación entre dos ordenadores conectados a Internet deben de estar alejados como máximo por 255 routers. Es sorprendente que aunque se haya ampliado considerablemente (de 32 bits a 128 bits) el número de ordenadores que pueden conectarse a Internet, se mantenga la esperanza de que la distancia entre dos ordenadores no crecerá por encima de este valor

4.2.3.1.1 Cabeceras del protocolo IP versión 6 [VERD2000]

La cabecera IP versión 6 no contiene ningún tipo de opciones a diferencia de la versión 4. No obstante, en algunos casos se hace necesario poder especificar algunas características especiales a los routers intermedios para que traten el datagrama IP de una forma determinada. No todos los datagramas son datos que circulan de un usuario a otro por Internet, algunos son mensajes entre los diferentes routers (Ejemplo: comunicar que está congestionado o fuera de servicio para que no le envíen más datagramas).

Un ejemplo típico podría ser la necesidad de especificar por que routers debe circular el datagrama. Si queremos una ruta fija entre dos ordenadores, ya sea porque no nos fiamos de los demás o simplemente porque queremos medir el rendimiento entre dos puntos, necesitamos especificar por dónde encaminarlo, evitando que sean los routers intermedios los que tomen la decisión. La manera de hacerlo es indicar en el campo siguiente cabecera de datagrama IP el número correspondiente a la cabecera que colocaremos tras el datagrama de esta forma, el router sabe que antes de encaminar el datagrama, debe de tener en cuenta esa información extra.

- **Cabecera de encaminamiento** tiene la misma función que en la versión 4. Son cuatro bytes (valor máximo de cada opción 2^8 = 256) de cabecera a los que se añade una serie de direcciones de 128 bits que corresponden a los routers por los que debe pasar el datagrama hasta llegar a su destino. El primer campo es el de siguiente cabecera, la versión 6 utiliza un sistema de

cadena dónde se pueden especificar múltiples cabeceras. A continuación viene el tamaño de la cabecera que es el tamaño total de la cabecera en palabras de 64 bits (incluyendo todas las direcciones especificadas). El tipo de encaminamiento es la política que se debe seguir en el encaminamiento, actualmente sólo existe el tipo 0 (si el router aparece en la lista de direcciones especificadas, se quita de la lista, decrementa el campo de segmentos restantes y busca cual de la lista está mas cerca para enviar el datagrama. Si no aparece en la lista, se limita a encaminarlo ignorando esta opción). El número de segmentos restantes es un valor que indica el número de direcciones de encaminamiento que aún restan. De esta forma, al llegar a 0 significa que el datagrama ha alcanzado su destino. Lo anterior descrito se observa en la figura 5.

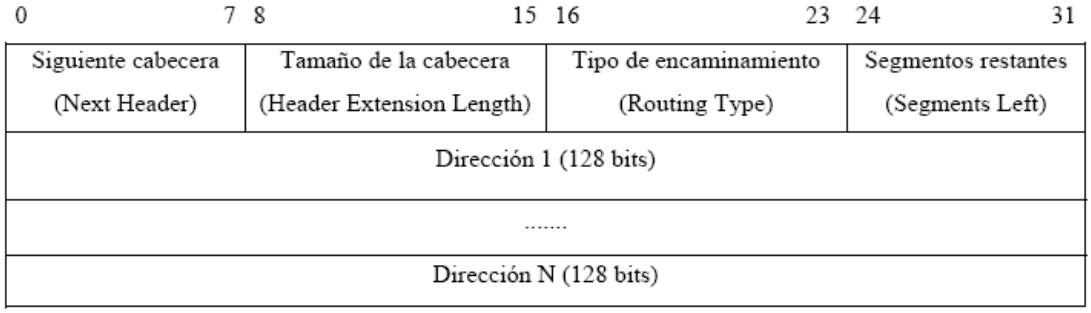


Figura 5. Cabecera de encaminamiento (tipo 0). [VERD2000]

- **Cabecera de fragmentación:** En la versión 6 se diferencia respecto a la de la versión 4 en que no existe un bit de fragmentación, ya que no se fragmentan los datagramas. La experiencia ha demostrado que todo y la gran versatilidad de la fragmentación implementada en la versión anterior (si un router recibe un datagrama de tamaño superior al que puede enviar, lo fragmentaba en varios datagramas de menor tamaño superior al que puede transmitir, lo descarta y envía al origen un datagrama de error ICMP.

  No obstante existe una cabecera de fragmentación para que en el origen (y no los routers intermedios como en la versión 4) pueda fragmentar un tamaño de datos superior al soportado por su red (Maximum Transfer Unit, MTU) en varios de tamaño inferior que son independientes entre si y pueden ser reenviados por separados en caso de necesidad. El primer campo de siguiente cabecera indica el siguiente tipo (si hay) de cabecera que nos encontraremos. El siguiente campo también es un byte que actualmente esta reservado y debe ser puesto a 0. El campo de desplazamiento de fragmento indica los 13 bits más significativos del desplazamiento, asumiendo pues que la fragmentación es en múltiplos de 64. En la versión 4 se usaban también 13 bits, pero eran los menos significativos, obligando a multiplicar por 8 para obtener el desplazamiento total del byte, cosa que ahora no es necesaria. Los 2 bits siguientes están reservados para futuros usos. Finalmente el último bit

es el bit de más fragmentos, que es puesto a1 en todos los fragmentos y a 0 en el último. Esta cabecera es representada en la figura 6.

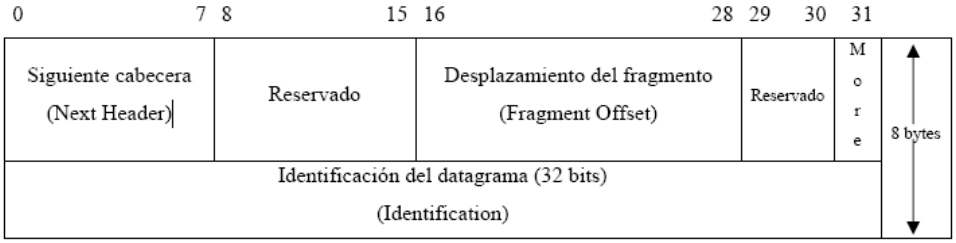


Figura 6. Cabecera de fragmentación de datagramas. [VERD2000]

- **Cabecera de opciones de destino:** Nos permite añadir opciones extra a los datagramas para que sean procesadas únicamente por el destinatario, como se muestras en la figura 7. Con este formato se permite que aquellos routers intermedios que no necesiten interpretarlas puedan evitarlas sin perder tiempo de proceso. El primer campo es como siempre el de siguiente cabecera, que nos permite indicar la presencia de más cabeceras. A continuación tenemos el campo de tamaño de la cabecera que en 8 bits especifica el tamaño de la cabecera en palabras de 64 bits sin incluir los primeros 64 bits. Esto permite tener un valor 0 en este campo, ya que si el tamaño cubriera toda la longitud, cada router debería examinar este campo para asegurarse que no es 0. Las opciones son procesadas por el destinatario del datagrama, y su formato obliga a que sean múltiplos de 64 bits para poder ser especificadas en el campo de tamaño de la cabecera.

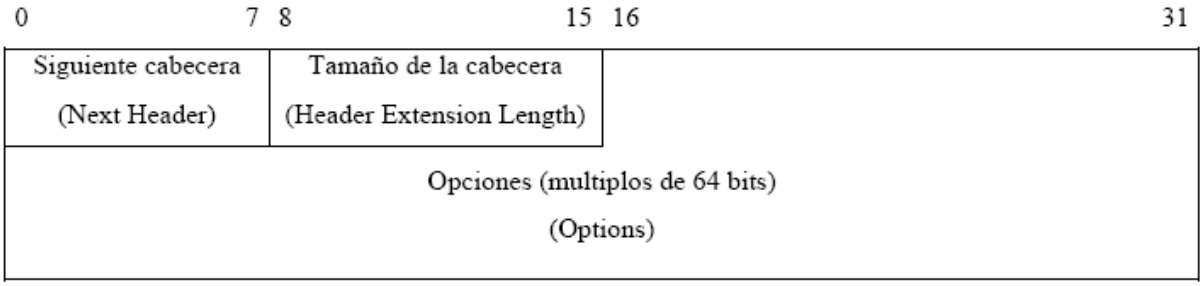


Figura 7. Cabecera de opciones de destino. [VERD2000]

- **Cabecera de opciones entre saltos:** Permite especificar opciones que serán procesadas por todos los routers intermedios. Su formato es el mismo que el de la cabecera de opciones de destino, aunque a diferencia de esta tan sólo es interpretada por el destinatario del datagrama. Cuando un datagrama llega una cabecera extra, especifica en el datagrama que tipo de cabecera le sigue con un código numérico.

- **Cabecera de autenticación**: Es una de las novedades más importantes en la versión 6 del protocolo IP. Se observa en la figura 8. Debe estar situada entre la cabecera IP y los datos del datagrama. La presencia de una cabecera de autenticación no modifica de ninguna manera el comportamiento del resto de protocolos de nivel superior como TCP o UDP. Esta cabecera tan solo proporciona una seguridad implícita del origen del datagrama. De esta forma los protocolos superiores deben rechazar los paquetes que no estén adecuadamente autenticados. El primer campo indica la siguiente cabecera que nos encontraremos tras esta. A continuación nos encontramos el tamaño de los datos especificado en palabras de 32 bits y un campo de 16 bits reservado que debe ser inicializado a 0. Después nos encontramos con el índice de parámetros de seguridad y el campo de número de secuencia que ocupan 32 bits cada uno. Finalmente vienen los datos de autenticación que es un campo de longitud variable.

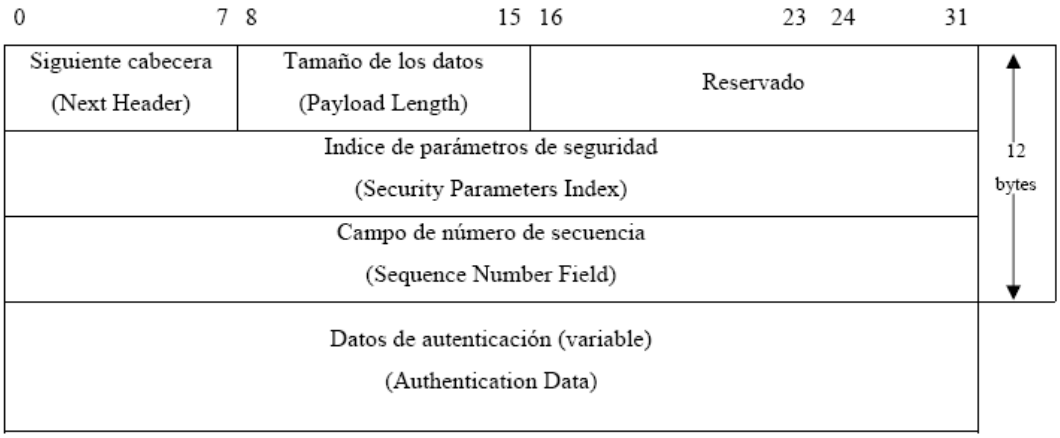


Figura 8. Cabecera de autenticación de la versión 6. [VERD2000]

Tal y como se ha visto, un datagrama puede incluir mas de una cabecera. Esto no debería suponer ningún problema para los routers intermedios encargados de encaminarlo hasta su destino. De esta forma, las cabeceras son procesadas por los routers a medida que estas llegan, sin ineficiencias. Este sistema de proceso ha sido comparado con las distintas capas de una cebolla, dónde cada cabecera es una capa. De todas formas es importante señalas que hay algunas cabeceras con mayor importancia que otras, como la cabecera de autenticación que obliga a descartar todo el datagrama si es incorrecta o la cabecera de fragmentación que obliga al reensamblamiento de datagramas.

Tenemos pues que el orden de las diferentes cabeceras es importante, y pese a no existir un formato rígido para establecer este orden, si que hay una recomendación en cuanto al orden adecuado de estas, como se muestra en la tabla 3:

Orden	Cabecera	Características
1	Cabecera IPv6	Encabezado del paquete IPv6
2	Cabecera de opciones *Hop by Hop*	Contiene información opcional que debe ser analizada por cada nodo a lo largo de la ruta del paquete
3	Cabecera de opciones de Destino	Contiene opciones que serán procesadas por el primer destino que aparezca en el campo de dirección destino, más destinos subsecuentes que aparezcan listados en la cabecera de enrutamiento
4	Cabecera de Enrutamiento	Este encabezado opcional lista todos los nodos intermedios que deben ser visitados por el paquete en su trayecto hacia el nodo destino
5	Cabecera de Fragmentación	Es utilizada por un emisor IPv6 para enviar un paquete que es más grande que la Unidad Máxima de Transmisión (MTU) más pequeño de los nodos intermedios hacia el destino
6	Cabecera de Autenticación	Provee integridad de datos y autenticación del origen de los datagramas IP, con esto se logra tener protección contra reenvío de paquetes
7	Cabecera de Encapsulación de seguridad de la carga	Está diseñado para proveer confidencialidad, autenticación del origen de los datos, integridad sin conexión y servicio anti-reenvío
8	Cabecera de opciones de Destino (2)	Contiene opciones que serán procesadas solamente por el destino final
9	Cabecera de protocolos de capas superiores	Encabezados de protocolos de transporte tales como TCP ó UDP deben ir aquí

Tabla 3. Orden en el que deben ser colocados los encabezados de extensión IPv6

La presencia de cualquiera de estas cabeceras es opcional, con lo que por ejemplo no es necesario la especificación de una cabecera de opciones entre saltos (posición 2), si queremos insertar una cabecera de opciones de destino (posición 3).

Observamos que la cabecera de opciones de destino se repite en dos posiciones distintas (3 y 7) esto es debido a que si necesitamos enviar datagramas encapsulados (Tunneling) y queremos que estas opciones sean utilizadas por los routers intermedios debemos enviar estas opciones antes que las de encaminamiento.

Por otro lado, si queremos pasar información que sólo sea interpretada por el destinatario del datagrama debemos colocar estas opciones justo antes de la cabecera del protocolo del nivel superior (posición 7).

4.2.3.2 Direccionamiento en IP versión 6 [VERD2000]

Una de las características más relevantes de la versión 6 del protocolo IP es el aumento de las direcciones de 32 a 128 bits. Una manera sencilla de entender este aumento sería coger el sistema de direccionamiento utilizado en la versión 4 y aumentarlo simplemente añadiéndole más bits. Pero esto no seria cierto, puesto que uno de los motivos de este cambio es el de la ineficiente gestión de las direcciones, haciendo lento el encaminamiento por Internet. De esta forma, en la versión 6 se definen tres tipos de direcciones:

1 Unicast. Las direcciones unicast identifican a una única interfaz, es decir, un paquete enviado a una dirección unicast será entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales. Existen tres tipos de direcciones unicast:

- Global: Las direcciones Unicast Globales son direcciones de Internet, es decir, tienen significado y pueden ser enrutadas por Internet, ya sea de manera nativa si así lo permite la infraestructura de red, ó por medio de túneles.

- Sitio: Este tipo de direcciones identifica una interfaz dentro de un dominio IPv6, pero no pueden ser enrutadas fuera de él, ya que pierden significado.

- Local: Este tipo de direcciones sirven para identificar una interfaz únicamente dentro de un mismo segmento de red (LAN), fuera de él pierden totalmente su valor.

2. Multicast. Las direcciones anycast identifican un grupo de interfaces, de forma que un paquete enviado a una dirección anycast será entregado a un miembro cualquiera del grupo, siendo generalmente el más cercano según la distancia asignada en el protocolo de encaminamiento.

3. Anycast. Las direcciones multicast identifican, al igual que las anycast, a un grupo de interfaces, pero un paquete enviado a una dirección multicast es enviado a todas las interfaces del grupo. Las direcciones de broadcast no existen en IPv6, su misión ha sido suplantada por las direcciones multicast. Este tipo de agrupación no existía en la versión 4.

Las direcciones IP de la versión 6 están compuestas por 128 bits. Los diseñadores del protocolo optaron por representarlas en 8 agrupaciones de 16 bits. De esta forma se puede utilizar la notación hexadecimal, que permite una representación más compacta que una ristras de 128 unos y ceros. Todo y esta simplificación, continúa siendo bastante complicada de manipular y recordar.

Para compactar estas direcciones tan voluminosas, se aceptaron una serie de simplificaciones, tal y como se muestran en la figura 9:

• Supresión de los ceros redundantes situados a la izquierda.

• Simplificación de los ceros consecutivos mediante el uso del prefijo '**::**'. Este prefijo tan sólo puede ser utilizado una vez en una misma dirección.

• Para las direcciones IP versión 6 obtenidas añadiendo 96 ceros a la dirección IP versión 4 (10.0.0.1 -> 0:0:0:0:0:0:A00:1) se permitirá el uso de la notación decimal (::10.0.0.1).

• La especificación de un prefijo de direccionamiento en la versión 6 se realizará mediante la forma dirección IPv6/prefijo (Si tenemos el prefijo de 40 bits FEDC:BA98:76 en la dirección FEDC:BA98:7600::1 se especificará como FEDC:BA98:7600::1/40). Se debe tener mucho cuidado con las simplificaciones siempre que se indican prefijos, ya que puede pasar que con el prefijo de 64 bits FEDC:BA98:0: y la dirección FEDC:BA98:0

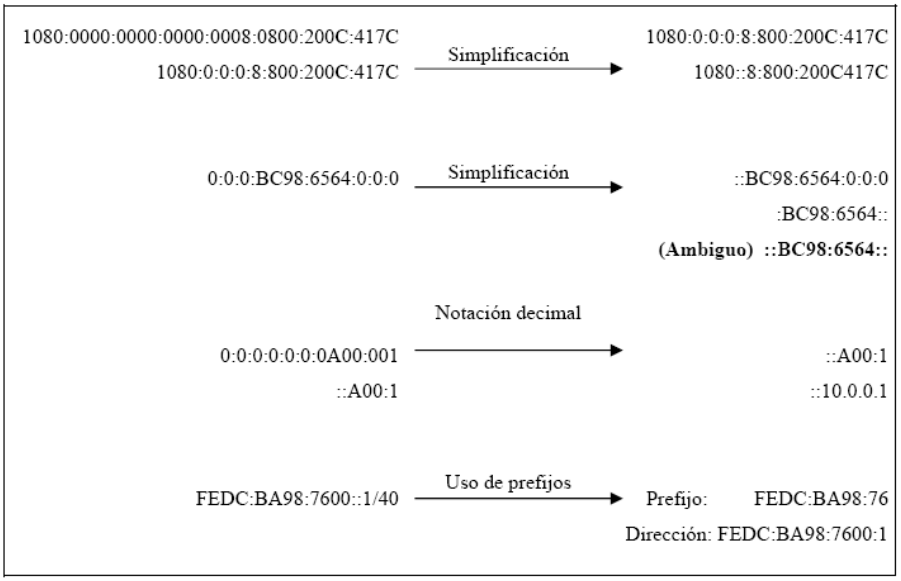


Figura 9.Simplificaciones en el direccionamiento IP versión 6. [VERD2000]

4.2.3.2.1 Direcciones Unicast [VERD2000]

El grupo de direcciones unicast representa aquellas direcciones que identifican un único punto final en una comunicación. Este grupo de direcciones presenta cinco subtipos de direcciones especiales:

- **Dirección no especificada:** Está compuesta por 16 bytes nulos (0:0:0:0:0:0:0:0) y sólo puede utilizarse como dirección inicial mientras se inicializa y se recibe una dirección fija. También puede utilizarse para funciones internas que requieran la especificación de una dirección IP.

- **Dirección interna:** Se define como 15 bytes nulos y un byte con el último bit a 1 (0:0:0:0:0:0:0:1). Esta dirección es interna y de ninguna forma puede circular por la red o ser dirección de origen o destino de un datagrama. Su utilidad viene dada para los ordenadores que no dispongan de una conexión de red y deseen simular el comportamiento de conexión a una red mediante una dirección fantasma que nunca saldrá del propio ordenador.

- **Direcciones tipo IP versión 4** Son aquellas direcciones que se obtienen añadiendo un prefijo de 96 ceros a una dirección IP versión 4 (10.0.0.1 pasaría a ser en la versión 6 ::10.0.0.1).

- **Direcciones locales reservadas:** Son direcciones reservadas para intranets. Estas direcciones no son válidas por Internet y tan sólo sirven para que una organización pueda crear una organización de sus redes basada en un esquema TCP/IP sin la necesidad de estar conectados a Internet (en la versión 4 de IP, existen diferentes clases reservadas para este mismo fin, como por ejemplo 192.168.XXX.YYY)

- **Direcciones de inicialización locales reservadas:** Son direcciones que pueden utilizar los ordenadores conectados a una misma red local mientras se inicializa y no tiene asignada una dirección IP. Se diferencia de la dirección no especificada (0:0:0:0:0:0:0:0) en que a diferencia de esta, la dirección de inicialización local si puede circular por la red, permitiendo por ejemplo obtener el sistema operativo de un servidor en la misma red. Esta característica ya existe en la versión 4 del protocolo IP, que actúa conjuntamente con los protocolos ARP y RARP [Ric98-1]. Estas direcciones se construyen con el prefijo FE80::/10 y 64 bits que representan la dirección física (MAC Address) de la tarjeta de red.

4.2.3.2.2 Direcciones Multicast [VERD2000]

Las direcciones de tipo multicast fueron ya añadidas a la versión 4 del protocolo IP en 1988 con la definición de la clase D. Aprovechando la experiencia obtenida desde entonces, y viendo su viabilidad se decidió añadirlas en la especificación de la versión 6. Este tipo de direcciones se caracteriza por ser comunes a un grupo de ordenadores (la misma dirección es compartida por todos los integrantes del grupo) de forma que un datagrama enviado a esta dirección será distribuido a todos los integrantes del grupo. Estas direcciones se forman mediante el prefijo FF**XY**:ZZZZ:ZZZZ:ZZZZ:ZZZZ:ZZZZ:ZZZZ:ZZZZ/16.

En la figura 10, se observa que el símbolo **X** agrupa un conjunto de 4 bits denominado banderas dónde se especifican una serie de opciones, aunque actualmente los tres primeros están reservados y deben ser inicializados a 0 y el cuarto denominado transitorio e especifica si la dirección es local y una vez finalizada la comunicación debe liberarse (valor 0) o si la dirección es fija y debe conservarse (valor 1). El símbolo **Y** también agrupa 4 bits que definen el alcance de la comunicación, evitando que los datagramas de una videoconferencia local salga a Internet o viceversa.

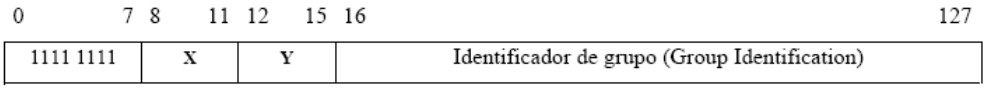


Figura 10. Formato de una dirección de tipo multicast. [VERD2000]

4.2.3.2.3 Direcciones Anycast [VERD2000]

Una de las nuevas características presentes en la versión 6 de IP es la inclusión de un nuevo tipo de direcciones denominado anycast (ver formato en la figura 11). Este tipo de direcciones aún en fase experimental se diferencia de las direcciones multicast en que el datagrama no es entregado a todos los miembros del grupo, sino que se entrega al integrante del grupo más cercano del origen del datagrama.

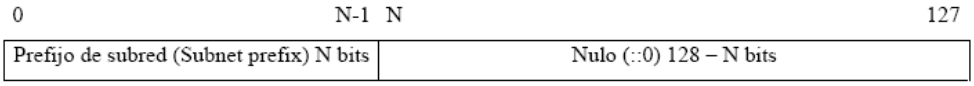


Figura 11. Formato de una dirección de tipo anycast.

El formato de este tipo de direcciones es muy sencillo debido a que toda la carga se centra en el sistema de encaminamiento. De esta forma, para cada router debe guardar un solo registro que le indica cual es el miembro más cercano a él del grupo especificado, y al recibir un datagrama con una dirección de destino anycast comprobar la existencia de este registro especial en su tabla de encaminamiento o encaminar normalmente el datagrama.

4.2.4 Comparación de los protocolos actuales de Internet [VERD2000]

Como ya se ha dicho anteriormente, la versión 4 del protocolo IP es robusta y fiable. Además funciona adecuadamente y permite una independencia de los protocolos de las capas superiores (TCP, UDP...). Se debe plantear seriamente las necesidades actuales y futuras para asegurarnos que una revisión del protocolo es necesaria y aportara ventajas. Esto es esencial debido al gran número de ordenadores conectados a Internet que utilizan TCP/IP. Lo que implica

que cualquier modificación de cualquiera de estos protocolos afecte a una gran variedad de ordenadores y sistemas operativos, abarcando desde obsoletos VAX con VMS hasta modernos supercomputadores CRAY con sistemas operativos paralelos.

La versión 4 del protocolo IP utiliza un sistema de direcciones de 32 bits (2^{32}=4.294.967.296) subdivididas en cinco clases. Con una simple revisión del crecimiento de Internet en los últimos 5 años, podemos observar que las direcciones a este ritmo se agotarán sobre los años 2005/2007.

Además las necesidades actuales han variado sensiblemente respecto a las iníciales de 1978. En aquel momento tanto el número de ordenadores conectados como las expectativas de crecimiento eran mucho más moderados de lo que han sido realmente, y por tanto la suposición de que un tamaño de 32 bits sería suficiente parecía razonable
.
De esta manera, podemos justificar la revisión de la versión 4 del protocolo IP desde dos puntos de vista principalmente:

1. **Técnicamente**: El sistema de direccionamiento es insuficiente para la demanda actual y futura prevista. Las tablas de encaminamiento (tablas de direcciones que almacenan los routers de forma interna, y que se utilizan para saber hacia dónde deben encaminar un datagrama) son excesivamente grandes debido a la gran cantidad de direcciones existentes actualmente y al sistema de encaminamiento utilizado, que obliga a los routers a mantener grandes cantidades de direcciones excesivamente la circulación por Internet, ya que los routers deben consultar para cada datagrama estas tablas.

2. **Socialmente**: Las necesidades de los usuarios de Internet han aumentando espectacularmente, exigiendo nuevas capacidades (seguridad, privacidad, comercio electrónico, velocidad...) que la versión 4 no puede proporcionar.

En la siguiente tabla se pueden ver algunas diferencia entre las dos versión del protocolo IP:

IPv4	IPv6
Las direcciones de fuente y destino tienen una longitud de 32 bits (4 bytes).	Las direcciones de fuente y destino tienen una longitud de 128 bits (16 bytes).
El protocolo de seguridad es opcional.	Costa de un protocolo de seguridad
No hay identificaron de flujo de paquetes para QoS que dirige los routers presentes en IPv4.	La identificación del flujo del paquete para QoS que dirige los routers esta dentro IPv6, usando el campo de la etiqueta del flujo.
La fragmentación es realizada por el host que se encarga de enviar y los routers direccionan, retardando el funcionamiento de los routers	La fragmentación es realizada por el hots que envía
El tamaño del paquete de la capa de acoplamiento no tiene ningún requisito y debe poder volver a montar un paquete de 576 byte.	La capa de acoplamiento debe soportar un paquete de 1.280 bytes y debe poder volver a montar un paquete de 1.500 bytes.
La cabecera incluye una suma de comprobación	La cabecera no incluye una suma de comprobación
La cabecera incluye opciones	Todos lo datos opcionales se mueven a la cabecera de extensión IPv6.
ARP usa difusión ARP para resolver el direccionamiento en IPv4 en la capa de acoplamiento	ARP, las tramas de petición son reemplazadas por mensajes multicast.
Internet Group Management Protocol (IGMP) es usado para administrarla subset local de los miembros	IGMP es reutilizado con el Multicast Listener Discovery (MLD).
ICMP Router Discovery es usado para determinar la dirección de IPv4 del gateway.	ICMPv4 Router Discovery es reemplazado con ICMPv6 Router, solicitando al router los mensajes anunciados
Las direcciones de Broadcast son usadas para enviar el tráfico a todos los nodos.	No hay direccionamiento broadcast IPv6. es usada la dirección multicast para la conexión local de todos los nodos

Tabla 4. Comparación IPv4 e Ipv6 [DAVI2003]

4.2.5 Mecanismos de transición [KAND2000]

La conversión de redes IPv4 a IPv6 tardará un largo período de tiempo, por lo que en el diseño de IPv6 se han tomado en cuenta mecanismos que permitan la coexistencia y comunicación de ambos protocolos.

Estos mecanismos de transición se dividen en tres clases principales:

• Dual Stack: Este mecanismo de transición permite a un enrutador, *host* o servidor utilizar un *stack* IPv4 y un *stack* IPv6 simultáneamente, lo que trae consigo dos grandes ventajas: por un lado un nodo con *dual stack* puede comunicarse con nodos que solo tienen un stack IPv4 de manera nativa y por el otro también puede comunicarse con nodos que solo tengan habilitado el stack IPv6 de manera nativa. Su principal desventaja es la necesidad de contar con una infraestructura de red que soporte el tráfico IPv6 de manera nativa.

• Túneles: Este mecanismo de transición permite a un enrutador IPv6, *host* IPv6 o servidor IPv6 comunicarse con otras redes IPv6 a través de la infraestructura IPv4 actual. Esta técnica consiste en encapsular los paquetes IPv6 dentro de paquetes IPv4 y entonces enviarlos sobre una red IPv4 a un nodo IPv4 destino el cual se encargará de extraer los paquetes IPv6 y entregarlos a su destino final. La principal ventaja de éste mecanismo de transición es que solo es necesario tener un Dual Stack en los nodos que servirán como extremos del túnel. Su principal desventaja es el retardo adicional ocasionado por el encapsulado y desencapsulado de paquetes IPv6 en datagramas IPv4, así como el tráfico de un mayor número de paquetes ocasionado por la reducción de espacio para datos en los datagramas IPv4 que contienen dentro paquetes IPv6.

• Traducción de protocolos: Este mecanismo de transición permite a un nodo que solo cuenta con el stack IPv6 habilitado dentro de una red IPv6 comunicarse con otro nodo que solo tiene el stack IPv4 habilitado dentro de una red IPv4. Sin embargo, ésta técnica requiere tener habilitados mecanismos de traducción entre IPv4 e IPv6 en las orillas de ambas redes (enrutadores). La principal desventaja es que todo el peso de este mecanismo de transición recae en los dispositivos encargados de hacer dicha traducción, a los que no siempre se tiene acceso.

4.2.5.1 Dual Stack [MUÑO2004]

La dual stack es probablemente la forma mas directa de introducir nodos Ipv4/Ipv6. Este mecanismo de transición como ya se había mencionado anteriormente, permite a un nodo utilizar un *stack* IPv4 y un *stack* IPv6 simultáneamente teniendo dos grandes ventajas: por un lado un nodo con Dual Stack puede comunicarse con nodos que solo tienen Stack IPv4 de manera nativa

y por el otro también puede comunicarse con nodos que solo tengan habilitado el Stack IPv6 de manera nativa.

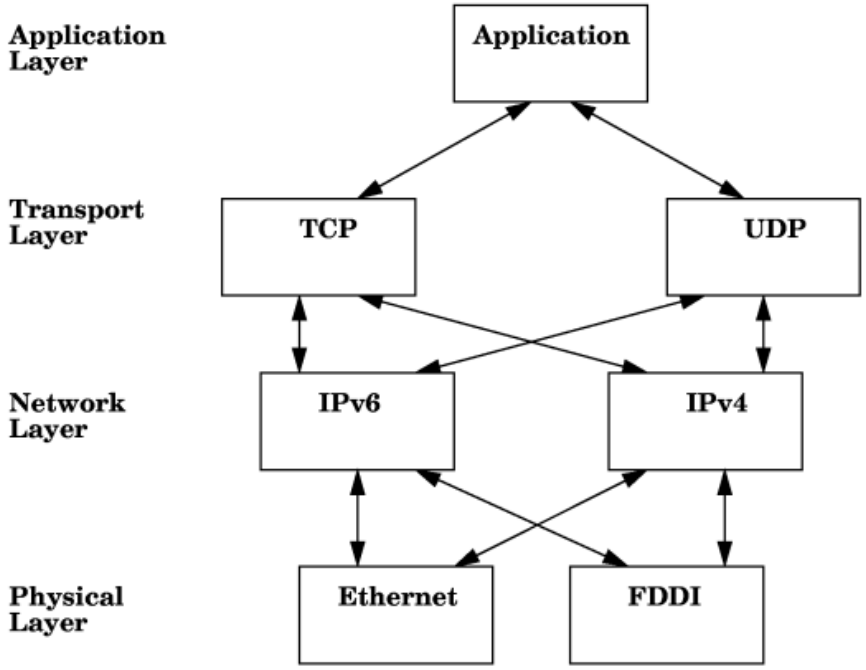


Figura 12. Dual Stack IPv4 e IPv6 [MUÑO2004]

El escenario de implementación ideal se inclina a la instalación de routers de stack duales, este escenario mostrado en la figura 12, se encarga de que todos los elementos de comunicaron tengan soporte de Ipv6, por lo general, cuando se desempeñan las actualizaciones y se efectúan las configuraciones adecuadas a los hots y routers, estos tiene la capacidad de manejar ambas versiones del protocolo IP. Logrando establecer comunicaciones en ambientes duales.

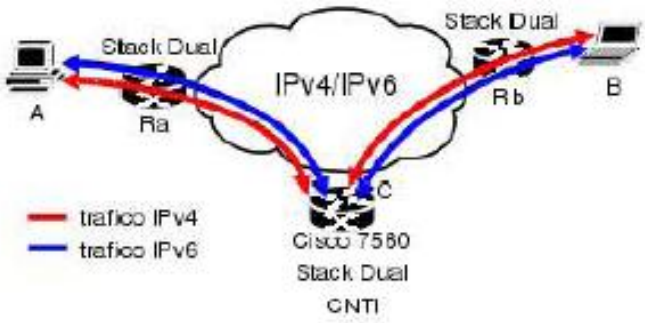


Figura 13. Escenario1 Dual Stack [MUÑO2004]

El escenario1 Dula Stack, mostrado en la figura 13, consta de dos máquinas A y B Ipv4/ IPv6, dos routers de borde R_A y R_B IPv4/IPv6 respectivamente y un sitio C con un router de borde Stack Dual (en este caso, el router frontera).

Se debe tener en cuenta que la maquinas A y B deben tener actualización del sistema operativo capaz de soportar IPv6. De igual manera los routers deben tener actualizaciones del software.

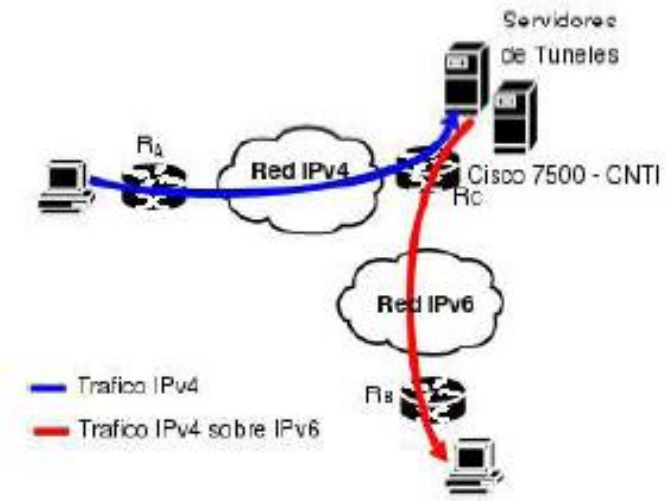


Figura 14. Escenario 2 Dual Stack [MUÑO2004]

Para el tipo de escenario de la figura 14, el extremo de la comunicación sin soporte IPv6 no necesitara realizar actualizaciones, pues el nodo central CNTI dispondrá servidores de túneles que realizarán el encapsulamiento y desencapsulamiento respectivo para paquetes IPv4 o paquetes IPv6, de acuerdo al caso.

Este escenario consta de una maquina (A) IPv4 y una máquina (B) con soporte IPv4/IPv6.un router de borde R_A IPv4, un router de borde R_B y R_C con soporte dual y capaces para manejar túneles.

4.2.5.2 Túneles [KAND2000]

La principal función de los túneles es llevar protocolos incompatibles o datos específicos sobre una red, por ejemplo, los túneles del Protocolo de Enrutamiento Multicast Vector Distancia (DVMRP) llevan datagramas multicast sobre redes unicast. IPSec en modo túnel lleva datos protegidos por un algoritmo de cifrado.

Para el desarrollo de IPv6 sobre una infraestructura existente IPv4 los túneles proveen una manera básica de comunicación entre hosts o islas de hosts IPv6 utilizando IPv4 como medio de transporte. En la figura 15 un túnel es creado para comunicar dos islas de hosts IPv6 sobre el Internet. Los enrutadores encargados de administrar el túnel deben tener configurado una dual stack para poder encapsular los paquetes IPv6 en datagramas IPv4 y viceversa.

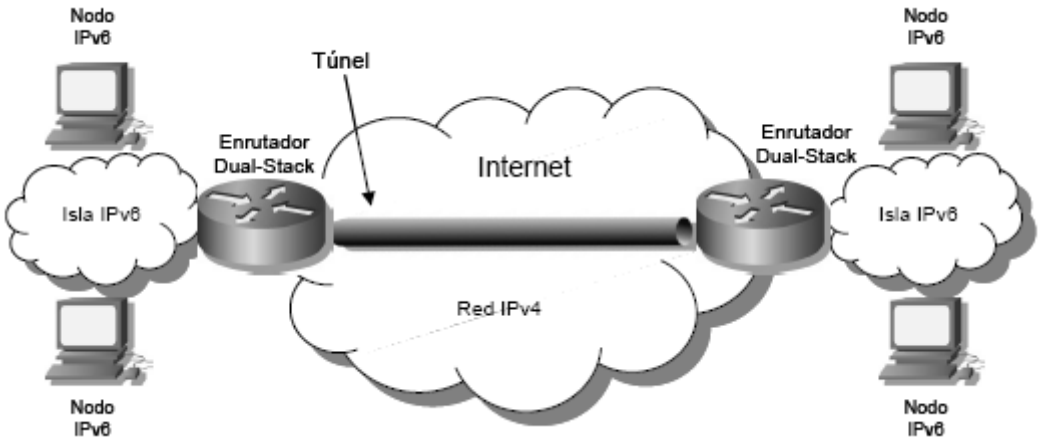


Figura 15. Túnel establecido entre dos islas IPv6 a través de la infraestructura IPv4 [KAND2000]

Para poder configurar un túnel primero es necesario tomar en cuenta los siguientes aspectos:

• Habilitar el protocolo 41: Si se tiene configurado un cortafuegos sobre IPv4, es necesario establecer una regla que permita el acceso y salida al protocolo 41. Como está descrito en el RFC 4213 "*IPv6* Transition Mechanisms" [21] el número de protocolo asignado a la encapsulación de paquetes IPv6 en IPv4 es el 41. Este valor es utilizado en el campo "Número de Protocolo" en el encabezado de IPv4 para especificar la encapsulación de un paquete IPv6 en un paquete IPv4.

• Manejo de mensajes de error (ICMPv4): Algunos viejos enrutadores en caso de error solo regresan ocho octetos de datos, sin embargo, los nodos emisores de los paquetes IPv6 necesitan conocer los campos de direcciones IPv6 en el error y cada uno de ellos ocupa 16 octetos.

• Traducción de Direcciones de Red (NAT): No es posible establecer túneles IPv6 en IPv4 a través de NAT cuando éste está habilitado en modo traducción dinámica de puerto y redirección de puerto. Por otra parte, es posible establecer dichos túneles si NAT es configurado en modo estático como lo muestra el RFC 4966 [22].

Una vez visto esto, es necesario definir un escenario en el cual se usará el túnel, existen tres posibles escenarios para la creación de un túnel:

• Host a Host: Esta arquitectura requiere que ambos hosts tengan un Dual Stack configurado y solo permite el establecimiento de sesiones IPv6 extremo a extremo entre ellos.

• Host a Enrutador: Hosts con un Dual Stack pueden establecer un túnel con un enrutador que también cuente con un Dual Stack. El enrutador puede tener conectividad IPv6 nativa sobre otra interfaz por lo que esta arquitectura permite el establecimiento de sesiones IPv6 extremo a extremo entre cualquier host de la isla IPv6 y el host aislado a través del enrutador.

• Enrutador a Enrutador: Enrutadores con un Dual Stack sobre una red IPv4 pueden establecer un túnel hacia otro enrutador con Dual Stack. Estos enrutadores pueden ser utilizados para interconectar islas de hosts IPv6, por lo que cualquier host puede establecer sesiones IPv6 extremo a extremo con otro host de la otra isla IPv6.

En la figura 16 se muestran los tres escenarios posibles para la creación de túneles, el caso (1) muestra la generación de un túnel host a host. El caso (2) presenta la generación de un túnel host a enrutador y por último, el caso (3) presenta la generación de un túnel enrutador a enrutador.

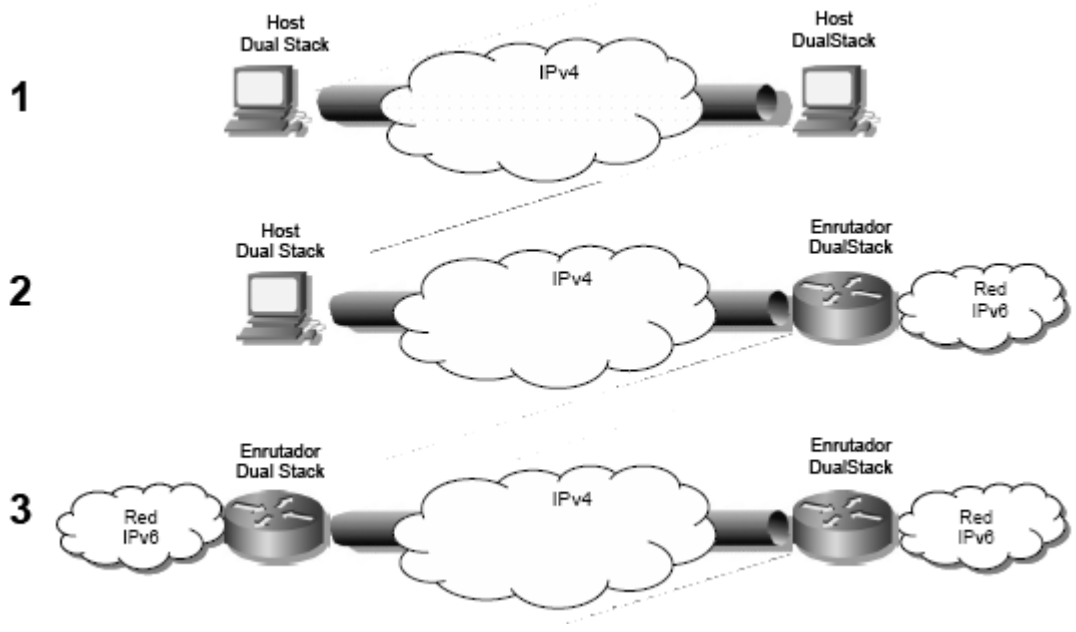


Figura 16. Escenarios para la creación del túnel. [KAND2000]

4.2.5.2.1 Técnicas para establecer Túneles [KAND2000]

El IETF definió protocolos y técnicas para establecer túneles entre nodos con dual-stack, entre estas técnicas se encuentran las siguientes:

• **Túneles 6to4**: En esta técnica los extremos del túnel están determinados por las direcciones globales IPv4 embebidas dentro de direcciones IPv6 *6to4*. Las direcciones IPv6 6to4 están formadas por la combinación de un prefijo de enrutamiento global 2002::/16 y una dirección IPv4 globalmente única. Los túneles 6to4 pueden ser configurados entre dos enrutadores en la orilla de sus respectivas redes, o entre un enrutador y un host. El único inconveniente de esta técnica para establecer túneles es que solo permiten enviar tráfico IPv6 entre hosts con prefijos de enrutamiento 2002. Para poder comunicarse con nodos con otros prefijos de enrutamiento tales como 2001::/16 y 3FFE::/16 es necesario utilizar un enrutador de reenvío (*relay router*) del 6bone el cual se encargará de proporcionar un servicio de enrutamiento global 6to4.

• **Intransite Automatic Tunnel Addressing Protocol (ISATAP):** Esta técnica permite crear túneles IPv6-IPv4 automáticamente dentro de un sitio IPv4. Cada *host* solicita a un enrutador dentro del sitio IPv4 una dirección IPv6 e información de enrutamiento, de esta manera, los paquetes enviados al Internet IPv6 son enrutados a través del enrutador ISATAP y los paquetes destinados hacia otros hosts dentro del mismo sitio son entregados directamente mediante túneles ISATAP. Las direcciones IPv6 se configuran automáticamente mediante el protocolo “descubrimiento de enrutador” ISATAP, aunque también pueden ser configuradas de manera manual. Una dirección ISATAP al igual que una dirección 6to4 está formada por la concatenación de un prefijo global de agregación unicast IPv6 y el identificador de interfaz. El prefijo utilizado por ISATAP para habilitar una dirección ISATAP en un host es FE80::/10 (dirección local). El identificador de interfaz es formado agregando los 32 bits de la dirección IPv4, después se concatena el valor 0000:5EFE (reservado por IANA para identificar direcciones ISATAP). Ejemplo: para una dirección IPv4 148.247.54.122 su dirección IPv6 ISATAP sería FE80::5EFE:94F7:367A. Las direcciones ISATAP también pueden utilizar prefijos unicast Globales de 64 bits, los cuales son asignados por los enrutadores. Cuando un nodo ISATAP desea comunicarse con otro nodo ISATAP sobre IPv6 el paquete IPv6 es encapsulado dentro de un datagrama IPv4 al igual que como sucede con el mecanismo 6to4.

• **Tunnel Broker**: El IETF definió este mecanismo para facilitar el desarrollo de túneles configurados sobre redes IPv4 ya que mediante esta técnica no se tiene que configurar manualmente cada extremo del túnel. Tal como está establecido en el RFC 3053 “IPv6 Tunnel Broker” [23] *el* tunnel broker es un sistema externo que actúa como un servidor sobre la red IPv4 y recibe peticiones de nodos con dual stack para configurar túneles automáticamente (modelo cliente-servidor). Estas peticiones son enviadas vía HTTP sobre IPv4 por el nodo que desea configurar

dicho túnel. El tunnel broker entonces envía de vuelta al cliente información tal como la dirección IPv4 del servidor del túnel, la dirección IPv6 del servidor del túnel, la nueva dirección IPv6 que será asignada a este host con dual stack y las rutas IPv6 default para la configuración del túnel. Algunos tunnel brokers ya proporcionan scripts de configuración para los hosts clientes. Finamente el tunnel broker aplica comandos de manera remota sobre un enrutador con dual stack y que está conectado a un dominio IPv6 para habilitar el túnel configurado. Para poder hacer uso de esta técnica es necesario utilizar los servicios de alguna entidad que ofrezca el servicio de tunnel broker tales como:

- Freenet6
- Dolphins tunnel broker
- British Telecom tunnel broker
- Hurricane Electric 21
- SixXS

La gran mayoría de los tunnel brokers ofrecen el servicio de manera gratuita, el único requisito es registrarse mediante el llenado de un pequeño formulario.

•**Generic Routing Encapsulation (GRE):** Esta técnica fue desarrollada originalmente por Cisco para transportar tráfico Multicast sobre redes *unicast* y protocolos como IPX y Appletalk sobre IP, pero también puede transportar tráfico IPv6 sobre redes IPv4. GRE no utiliza TCP o UDP, en su lugar trabaja directamente con la capa IP, utilizando el protocolo número 47. Este incluye sus propios mecanismos para verificar la entrega e integridad de los paquetes. La carga de un paquete GRE incluye un paquete de capa 3 completo con su encabezado y carga intactos. El enrutador en la entrada del túnel GRE toma los paquetes IP y los envuelve en un nuevo paquete con un encabezado GRE, después los envía por la red hasta que alcanzan el enrutador de la salida del túnel. Este extrae el paquete contenido dentro del paquete GRE y lo entrega al nodo destino

• **TEREDO:** La meta principal de esta técnica es entregar paquetes IPv6 a nodos con dual stack que se encuentran detrás de un dispositivo NAT sobre dominios IPv4. TEREDO fue diseñado por dos principales razones: la primera es que el buen funcionamiento de los túneles 6to4 recae en la configuración de una dirección pública IPv4 y la implementación de enrutamiento 6to4. Debido a que en muchas ocasiones se tienen configuraciones de NAT de varios niveles no sería posible asignar a cada uno de estos dispositivo NAT una dirección pública IPv4. La segunda razón por la que se creó TEREDO es debido a que los paquetes IPv6 encapsulados en paquetes IPv4 utilizan el valor 41 en el campo de protocolo en el encabezado del paquete IPv4 y la mayoría de los dispositivos NAT solamente son capaces de traducir TCP y UDP. Como el protocolo 41 no es común entre los dispositivos NAT este tipo de paquetes no podrían fluir a través de ellos para alcanzar a los nodos destino. TEREDO utiliza como medio de transporte a UDP

para la creación de túneles ya que los dispositivos NAT pueden manejar bien este protocolo a múltiples niveles de anidación. Utilizando una sola dirección IPv4 y mapeos UDP del dispositivo NAT es posible establecer túneles para diferentes hosts con dual stack detrás de un mismo dispositivo NAT, para ello este mecanismo consta de tres componentes principales:

- Servidor TEREDO: Este servidor está conectado al Internet y cuenta con una dirección global IPv4. Se encarga de administrar la señalización y tráfico con los clientes TEREDO.

- Cliente TEREDO: este se encuentra detrás de un dispositivo NAT y solicita conectividad IPv6 al servidor TEREDO mediante paquetes UDP IPv4.

- TEREDO de reenvío: Está conectado a Internet IPv6 y actúa como enrutador IPv6 para brindar conectividad a los clientes TEREDO mediante el uso de paquetes UDP.

Cada una de estas técnicas está desarrollada para un escenario distinto de aplicación túneles 6to4 está diseñado para interconectar islas IPv6, ISATAP está diseñado para interconectar hosts a enrutadores con dual-stack, tunnel-broker está diseñado para conseguir conectividad IPv6 sobre nodos aislados en redes IPv4, GRE permite no solo encapsular tráfico IPv6 sino también IPX y Appletalk y TEREDO está diseñado para conseguir conectividad IPv6 en hosts que están detrás de dispositivos NAT.

4.2.5.3 Hardware que soportan IPv6

Productos con soporte IPv6, se muestran en la tabla 5:

Casa de hardware	Productos	Versión de SO con soporte IPv6
Cisco	Todos.	A partir IOS 12.2(2)T.
Novell	Todos.	A partir de Netware 6
3Com	Routers NETBuilderII y PathBuilder S500	Software versión 11.0
Nortel.	Todos	A partir de BayRS versión 12.0
Hitachi	Familia de routers GR2000 Gigabit.	--
6Wind	Serie 6WINDGate 6200	--

Tabla 5. Hardware IPv6 [MUÑO2004]

4.2.5.4 Software que soportan IPv6

Sistema operativo con soporte IPv6 (ver tabla 6).

Han estructurado los stack para soportar eventualmente IPv6:

Casa de software	SO	Soporte/Parche	Fuente
Macintosh	Mac OS X 10.2 Jaguar	Sí	software licenciado
	Mac OS 9	No	---
Unix	AIX 4.3	Sí	software licenciado
	Tru64 UNIX 4.0D (de Compaq)	Sí	software licenciado
	Tru64 UNIX 5.1 (de Compaq)	Sí	software licenciado
	FreeBSD 4.0	Sí	www.freebsd.org
	Linux kernel 2.0 o más recientes	Sí	www.linux.org
	NetBSD1.5	Sí	www.netbsd.org
	OpenBSD 2.7 o más recientes	Sí	www.openbsd.org
	Solaris 8	Sí	wwws.sun.com/software/solaris/
	HP-UX 11i IPv6 (de Hewlett Packard)	Sí	software licenciado
Microsoft	Windows 95/98/NT	No	---
	Windows 2000	Preview technology	http://msdn.microsoft.com/downloads/sdks/platform/tpipv6.asp
	Windows XP	Sí	software licenciado

Tabla 6. Sistema operativo con soporte IPv6 [MUÑO2004]

4.2.6 Streaming

Se le llama streaming a la transmisión en tiempo real de un video o audio, es decir, en el caso de no ser utilizado el medio streaming, para mostrar un contenido multimedia en la red, se tendrá que descargar primero el archivo entero y luego ejecutarlo, para finalmente ver y escuchar lo que el archivo contenía. Por esta razón este servicio streaming tiene como función precipitar la descarga y por supuesto la ejecución, para que de esta manera se pueda visualizar el datagrama enviado mientras este se va descargando. [ALVA2004]

4.2.6.1Funcionamiento del video streaming [ALVA2004]

Imaginen una red LAN pequeña, donde solo se tiene un computador y un servidor, el proceso empieza cuando dicho servidor empieza a enviar el archivo y por lo tanto el cliente de igual manera comienza a recibir el archivo y construye un buffer en donde se almacena una pequeña parte de la información, que cuando se llena esta mínima cantidad de información enviada, el cliente empieza a observar el archivo y el proceso de descarga continua. Este sistema esta sincronizado para

que el archivo se pueda ver mientras se va realizando la descarga, de tal manera que cuando el archivo acaba de descargarse el fichero también haya acabado de visualizarse.

Puede haber inconvenientes de descensos de velocidad en el momento de la conexión pero es allí cuando se utiliza la información guardada por el buffer, de manera que se pueda aguantar un poco ese descenso.

Cuando se observa el funcionamiento del video streaming, se responde a la pregunta de que ventajas trae utilizar streaming, y la respuesta se intuye inmediatamente, pro que en un primer lugar no es necesaria la descarga del archivo, segundo no importa el tamaño del archivo, por mas grande que este sea se puede utilizar este medio y no deja copia en el disco duro.

4.2.6.2 Protocolos de Transmisión de Video Streaming [AUST2002]

Los dos tipos que existen de streaming, necesitan diferentes protocolos para llevarse a cabo:

- **Protocolos necesarios para realizar streaming en directo:** Los protocolos utilizados para transmitir este tipo de datos en tiempo real no pueden estar basados en TCP puesto que este protocolo está orientado a la conexión y en caso de que se produzca un error o se pierda un dato, éste se vuelve a retransmitir. Para vídeo y sonido en tiempo real esto no puede ocurrir por razones obvias. Por tanto, se necesitan protocolos basados en UDP: el protocolo más importante para realizar la transmisión de vídeo y sonido en tiempo real es RTP (Real-time Transport Protocol), el cual proporciona servicios de entrega en la red desde el origen hasta el destino para la transmisión de datos multimedia en tiempo real.

- **Protocolos necesarios para realizar streaming bajo demanda:** En cambio, cuando la transmisión de vídeo y sonido no se realiza en tiempo real y es el cliente el que controla la recepción de los datos, sí se pueden utilizar protocolos basados en el Protocolo de Control de Transmisión (TCP), como HTTP y FTP. HTTP y FTP son protocolos fiables, por ello se construyen en la capa más alta de TCP y así se aseguran de que los paquetes lleguen a su destino y en secuencia. De esta forma, si se pierden paquetes por el camino estos son retransmitidos, pero no hay problemas en la recepción porque es el cliente el que se encarga de todo.

4.2.6.3 Operaciones Soportadas por el protocolo: [ALVA2004]

Los modos de operación que utiliza el servidor para enviar el audio y/o video a la dirección de destino son:

- **Unicast:** La información (audio y video) es trasmitido a la fuente de la petición RTSP, con el número de puerto escogido por el usuario. Sucesivamente, la información es transmitida por es el mismo flujo confiable de RTSP.

- **Multicast, dirección escogida por el usuario:** El servidor de los medios escoge la dirección y el puerto del multicast. Este es un caso típico de la transmisión en vivo o por demanda.

- **Multicast**, **dirección escogida por el cliente:** Si el servidor está participando en un multicast conferencia, la dirección multicast, el puerto y la llave de codificación es dada en la descripción de la conferencia

4.2.6.4 Programas

Para poder desarrollar un video streaming en Internet se encuentran programas para realizar dicha tarea, tales como:

- Real Player
- Windows Media Player
- QuickTime
- VLC oVLANS

4.2.6.5 Flujo de streaming

Para poder crear un flujo de datos a partir de una señal de vídeo y/o audio, se requieren cuatro pasos:

1. Identificación del origen:

- Emisión en directo o tiempo real.
- Petición de archivos bajo demanda, en la que el material se procesa sin conexión (offline) antes de poder ser visualizado vía Internet.

2. Codificación del archivo: [AUST2002]

El material se digitaliza y se comprime. El vídeo y/o el audio se comprimen porque sino ocuparían mucho espacio. En la compresión se pierden datos pero no los suficientes como para que el vídeo no se vea con calidad. Este proceso

lo realizan los CODEC. Algunos formatos de compresión de vídeo son: MPEG (formato pionero), ASF (formato de Microsoft), rm (formato de Real Network), mov (QuickTime), etc. Estos formatos facilitan el streaming.

3. Transmitir los flujos de datos o almacenarlos en el servidor:

Si se trata de una difusión, los flujos de datos codificados se envían directamente. En caso contrario, los archivos codificados se guardan en un servidor de streaming o simplemente en un servidor Web. Los servidores de streaming ofrecen mayores prestaciones que los servidores Web, como por ejemplo, mandar un archivo con mayor o menor calidad dependiendo de la velocidad de la línea. No obstante, si no se desean altas prestaciones con un servidor Web es suficiente.

4. Reproductor (Player) para visualizar el flujo de datos:

Para poder recibir y ejecutar los archivos de streaming a través de Internet, el cliente solo tiene que disponer de un sencillo software: un CODEC y un Reproductor. Este Reproductor se encarga, en caso necesario, de realizar la petición del archivo al servidor. Posteriormente, se encargará de reproducir los flujos de streaming. El proceso es el siguiente: el Reproductor comienza a recibir el fichero y construye un buffer donde empieza a guardar la información. Cuando se ha llenado el buffer con una pequeña parte del archivo, el Reproductor lo empieza a mostrar y a la vez continúa con la descarga. El sistema está sincronizado para que el archivo se pueda ver mientras se va descargando, de modo que cuando ha terminado de descargarse también ha acabado de visualizarse. Si en algún momento la conexión sufre descensos de velocidad se utiliza la información que hay en el buffer, de modo que se puede soportar un poco ese descenso. Si la comunicación se corta demasiado tiempo, el buffer se vacía y la ejecución del archivo se cortaría también hasta que se restaurase la señal.

Existen actualmente en el mercado varios Reproductores multimedia, siendo los más importantes el RealPlayer de Real Networks y, sobre todo, el Media Player de Microsoft por su gran difusión. Destacar que también Java ofrece en su librería JMF para trabajar con contenido multimedia la posibilidad de implementar un Reproductor capaz que procesar flujos de streaming. [AUST2002]

4.3 ESTADO *DEL ARTE*

Debido al elevado crecimiento de usuarios en la red Internet, se vio en la necesidad de ampliar la capacidad de direccionamiento, por lo que en algunos países ya se esta implementado IPv6, que es el protocolo de internet de nueva generación.

Esta mejora en el protocolo ha permitido desarrollar nuevas redes de investigación, tales como APAN, CUDI, internet2, Geant, la red CLARA, RAAP, entre otras que hacen parte del los diferentes países del mundo.

El campo de las comunicaciones móviles esta en boom, e IPv6 con su nueva arquitectura y con mayor flexibilidad topológica, esta en la capacidad de afrontar el nuevo reto que estas traen.

Actualmente IPv6 la han adoptado países, como Estados Unidos, China, Corea, India, Europa y Perú. Estos países utilizan IPv6 en aeropuertos para mejorar su seguridad, de igual manera en los automóviles y en redes inalámbricas.

Es por esto que se hace vital la migración a IPv6, sin embargo para poder realizar dicha operación se hace necesario empezar por entender en pequeñas magnitudes los medios posibles que se pueden implementar para dicha migración. Entre ellos encontramos múltiples soluciones ya adoptadas como los nodos dual stack, los túneles, y a través de software.

5. DESARROLLO

El desarrollo del proyecto se divide en 6 etapas:

Etapa 1: Seleccionar el equipo de transmisión para llevar a cabo el desarrollo del proyecto.

Etapa 2: Diseñar y realizar una conexión que permita la interacción entre IPv6/ IPv4.

Etapa 3: Realizar la configuración apropiada, en el equipo de transmisión para comunicar IPv4 e IPv6.

Etapa 4: Definir el tipo de enrutamiento a utilizar.

Etapa 5: Implementar un nodo Dual Stack y/o un túnel que permitan enviar y recibir datagramas de IPv4 e IPv6.

Etapa 6: Realizar las pruebas correspondientes utilizando un Sniffer, para analizar las tramas de IPv4 e IPv6.

5.1 Delimitación del proyecto

En el desarrollo del proyecto, se presentaron diversos obstáculos y a su vez soluciones: en un principio se quiso realizar la transmisión de video usando Windows Vista, ya que es un sistema operativo que soporta IPv6, no obstante trae diversos permisos y defectos que impiden realizar una comunicación fácilmente, de igual manera los codificadores de video existentes para este sistema operativo, a la hora de utilizarlos no funcionan óptimamente como en otros sistemas operativos. En el sistema operativo MAC es posible trabajar con IPv6, sin embargo es de conocimiento de todos, que es algo costoso, los programas en la gran mayoría no son compatibles y no es común el uso de este acá en Colombia. Es por esta razón que en este proceso se toma la determinación de trabajar usando el sistema operativo Linux Ubuntu, ya que en primer lugar es un software libre y permite ser manipulado más fácilmente.

Es importante tener claro que la transmisión de IPv6/IPv4 se puede hacer de diversas maneras, tales como: por medio de software o bien por Routers, como se desarrollo este caso, sin embargo si se usan Routers también existen diversas alternativas, ya sea configurándolos con los diferentes tipos de tunnel, o por dual stack o bien por translación.

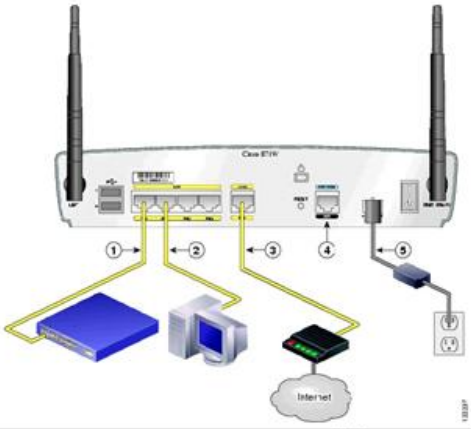
Sin embargo en el proyecto se llevo a cabo un tunnel ipv6ip, el cual permite encapsular los paquetes IPv6 en datagramas IPv4, haciendo uso de la infraestructura IPv4 existente y a su vez poder minimizar costos.

5.2 Seleccionar el equipo de transmisión para llevar a cabo el desarrollo del proyecto.

En esta etapa se debe tener en cuenta que el equipo, en este caso un Router cisco, permita instalar un IOS actual, el cual soporte IPv6.

En el proceso de selección de un equipo, se tuvo claro que se quería llevar a cabo con un router Cisco, no obstante no fue una tarea fácil , ya que cuando se inicio el proyecto no se encontraba mucha información sobre este tema, sin embargo enviando una solicitud a DESCA que es una empresa que maneja estos router y que los importa a Colombia, se hizo una reunión en Cisco México , concluyendo que un router no muy costoso que podía soportarlo era el router Cisco 801, no obstante este solo maneja un puerto con IPv6 que es el WAN y los cuatro Ethernet solo soportan IPv4, pero no consta de un puerto serial para comunicarse con otro, router, es por esto que después de realizar diversos intentos para realizar la comunicación, como hacer una translación de direcciones, se toma la determinación que no es posible dar una solución optima, debido a sus características y por ello se determina trabajar con dos router Cisco 1841.

5.2.1 Router Cisco 801 [CISCO2008]



1	Conexión Ethernet a un switch externo	4	Puerto de la consola
2	Conexión Ethernet a un PC	5	Adaptador de alimentación
3	Conexión WAN con módem de banda ancha para Internet		

Figura 17. Instalación típica del router Cisco 871[CISCO2008]

La figura 17. Muestra el panel posterior de un router Cisco 871 con dos puertos Bus serie universal (USB).

5.2.2 Características básicas del Router Cisco 801[CISCO2008]

Tipo de dispositivo:	Encaminador + conmutador de 4 puertos (integrado)
Factor de forma:	Externo
Dimensiones (Ancho x Profundidad x Altura):	26 cm x 21.6 cm x 5.1 cm
Peso:	1 kg
Memoria RAM:	128 MB (instalados) / 256 MB (máx.)
Memoria Flash:	24 MB (instalados) / 52 MB (máx.)
Protocolo de direccionamiento:	RIP-1, RIP-2
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Red / Protocolo de transporte:	PPTP, L2TP, IPSec, PPPoE, PPPoA
Protocolo de gestión remota:	SNMP, Telnet, HTTP
Características:	Protección firewall, soporte de DHCP, VPN, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), activable, soporte IPv6, Sistema de prevención de intrusiones (IPS)
Cumplimiento de normas:	IEEE 802.1x
Alimentación:	CA 120/230 V (50/60 Hz)

Tabla 7. Características básicas del router.

General

Factor de forma:	Externo
Anchura:	26 cm
Profundidad:	21.6 cm
Altura:	5.1 cm
Peso:	1 kg

Tabla 7. Características generales del Router.

Memoria

Memoria RAM:	128 MB (instalados) / 256 MB (máx.)
Memoria Flash:	24 MB (instalados) / 52 MB (máx.)
Conexión de redes	
Tecnología de conectividad:	Cableado
Conmutador integrado:	Conmutador de 4 puertos
Protocolo de interconexión de datos:	Ethernet, Fast Ethernet
Protocolo de conmutación:	Ethernet
Red / Protocolo de transporte:	PPTP, L2TP, IPSec, PPPoE, PPPoA
Protocolo de direccionamiento:	RIP-1, RIP-2
Protocolo de gestión remota:	SNMP, Telnet, HTTP

Tabla 8 . Memoria Router

Características

Cumplimiento de normas:	Protección firewall, soporte de DHCP, VPN, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), activable, soporte IPv6, Sistema de prevención de intrusiones (IPS)
Expansión / Conectividad	IEEE 802.1x
Interfaces:	4 x red - Ethernet 10Base-T/100Base-TX - RJ-45 ¦ 1 x red - Ethernet 10Base-T/100Base-TX - RJ-45 (WAN) ¦ 2 x Hi-Speed USB - 4 PIN USB tipo A ¦ 1 x gestión - consola - RJ-45
Diverso Algoritmo de cifrado:	Triple DES, AES
Método de autentificación:	RADIUS, TACACS+

Cumplimiento de normas:	EN 60950, IEC 61000-3-2, IEC 61000-4-11, IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, IEC 61000-4-8, IEC950, VCCI-II, EN55022 Class B, ICES-003 Class B, AS/NZ 3548 Class B, AS/NZS 3260, FCC Part 68, CS-03, UL 1950 Third Edition, EN 60555-2

Tabla 9. Características Router

Alimentación

Dispositivo de alimentación:	Adaptador de corriente - externa
Voltaje necesario:	CA 120/230 V (50/60 Hz)
Potencia suministrada:	26 vatios

Tabla 10. Alimentación del Router

Parámetros de entorno

Temperatura mínima de funcionamiento:	0 °C
Temperatura máxima de funcionamiento:	40 °C
Ámbito de humedad de funcionamiento:	10 - 85%

Tabla 11. Parámetros de entorno del Router

Configuración del Router Cisco 801[**CISCO2008]**

Como se dijo anteriormente en el desarrollo del proyecto, se platearon diversas soluciones, una de ellas, consiste en realizar una NAT, o realizar una dual stack, pese a esto no se obtuvo solución ya que se hace necesario otro Router para que se pueda tener una óptima comunicación. Ver la configuración de la NAT en Anexo 2.

5.2.3 Características básicas del Router Cisco 1841 **[CISCO2008]**

Los routers de la serie Cisco 1800 de servicios integrados incluye el router Cisco 1841, que es un router exclusivamente de datos. Los modelos de router Cisco 1841 admiten tarjetas de interfaz WAN (WIC), tarjetas de interfaz de voz/WAN (VWIC) en modo de sólo datos, tarjetas de interfaz WAN de ancho simple y alta velocidad (HWIC) y módulos de integración avanzada (AIM).

Figura 18. Router cisco 1841

En esta figura se muestra el hardware de la parte posterior del Router cisco 1841.

En el proceso del proyecto se utilizan dos Router Cisco 1841, con un IOS 12.4 (6). Cuyas características de ellos son las siguientes:

General

Tipo de dispositivo	Encaminador
Factor de forma	Externo - modular - 1U
Cantidad de módulos instalados (máx.)	0 (instalados) / 3 (máx.)
Anchura	34.3 cm
Profundidad	27.4 cm
Altura	4.8 cm
Peso	2.7 kg

Memoria

Memoria RAM	128 MB (instalados) / 384 MB (máx.) - SDRAM
Memoria Flash	32 MB (instalados) / 128 MB (máx.)

Conexión de redes

Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Red / Protocolo de transporte	IPSec

Protocolo de gestión remota	SNMP, HTTP
Características	Protección firewall, compresión del hardware, cifrado del hardware, asistencia técnica VPN, soporte VLAN, Sistema de prevención de intrusiones (IPS), montable en pared, Dynamic Multipoint VPN (DMVPN), Network Admissions Control (NAC)

Expansión / Conectividad

Total ranuras de expansión (libres)	1 (0) x Tarjeta CompactFlash ¦ Memoria ¦ 1 (1) x AIM ¦ 2 (2) x HWIC
Interfaces	2 x red - Ethernet 10Base-T/100Base-TX - RJ-45 ¦ 1 x USB - 4 PIN USB tipo A ¦ 1 x gestión - consola ¦ 1 x gestión - auxiliar

Diverso

Kit de montaje en bastidor	Opcional
Algoritmo de cifrado	DES, Triple DES, SSL, AES de 128 bits, AES de 192 bits, AES de 256 bits
Método de autentificación	Secure Shell v.2 (SSH2)
Cumplimiento de normas	CSA, CTR 21, CISPR 22 Class A, CISPR 24, EN 60950, EN 61000-3-2, IEC 61000-4-11, IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-6, EN 61000-3-3, EN55024, EN55022 Class A, EN50082-1, EN 61000-4-4, EN 61000-4-2, EN 61000-4-3, EN 61000-4-6, CS-03, EN 61000-4-5, UL 60950-1

Alimentación

Dispositivo de alimentación	Fuente de alimentación - interna
Voltaje necesario	CA 120/230 V (50/60 Hz)
Potencia suministrada	50 vatios

Software / Requisitos del sistema

OS proporcionado	Cisco IOS IP Base

Parámetros de entorno

Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	40 °C
Ámbito de humedad de funcionamiento	10 - 85%

Tabla 12. Características básicas Router cisco 1841

5.3 Diseñar y realizar una conexión que permita la interacción entre IPv6/IPv4 [CISCO2008]

En primera instancia se realiza el diseño, especificando las direcciones estáticas que se manejan en este caso son unicast como se muestra en la figura 19.

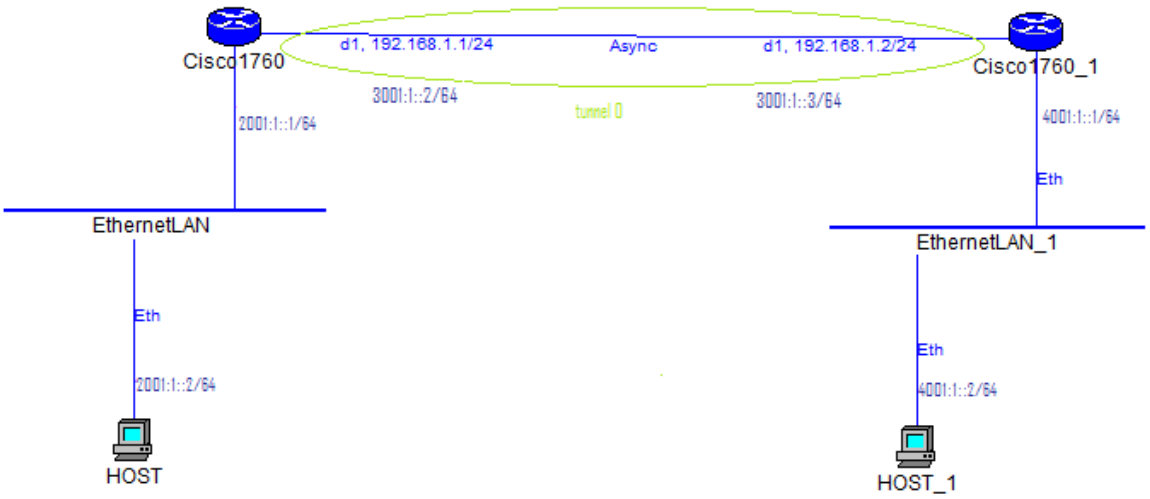


Figura 19. Diseño del tunnel IPv6IP

Después del diseño se hace la implementación del mismo como se observa en la figura 20.

Figura 20. Conexión física tunnel.

La infraestructura para llevar a cabo este proyecto, consta de dos Router Cisco 1841 conectados a través del puerto serial, y cada uno de ellos esta conectado a un equipo que soporte ipv6, en este caso específicamente se realizo sobre el sistema operativo Linux Ubuntu.

Los equipos están conectados a los Router por medio de cable UTP cruzados, y los Router están conectados entre si a atreves de un cable serial (figura 21).

Figura 21 Conexión Router Cisco 1841

En esta foto se observa la conexión de los dos routers, cada uno con su cable serial, el de consola y el cable UTP en la interface.

5.4 Realizar la configuración apropiada, en el quipo de transmisión para comunicar IPv4 e IPv6. [CISCO2008]

Como se ha nombrado anteriormente los Router a utilizar son cisco 1841 con un IOS 12.4 (15), los cuales al ser programados realizan un túnel, es decir este mecanismo permite que se envíen datagramas IPv6 encapsulados en paquetes IPv4.

La configuración de cada Router ya sea transmisor o receptor, se puede observar en los anexo 3 y 4 correspondientemente.

5.5 Definir el tipo de enrutamiento a utilizar [CISCO2008]

Existen dos protocolos de enrutamiento, ellos son:

PROTOCOLOS DE VECTOR DISTANCIA:

El enrutamiento por vector-distancia, también denominado algoritmo de enrutamiento Bellman-Ford, determina la dirección y la distancia (vector) hacia cualquier enlace en la red. La distancia puede ser el número de saltos hasta el enlace. Es decir el protocolo itera en el número de saltos en una ruta para hallar la más corta.

Los Routers que utilizan los algoritmos de vector-distancia envían su tabla de enrutamiento completa en cada actualización, pero solamente a sus vecinos. Los algoritmos de enrutamiento por vector distancia pueden ser propensos a los bucles de enrutamiento, pero desde el punto de vista informático son más simples que los algoritmos de enrutamiento de estado de enlace.

Entre los protocolos de enrutamiento vector-distancia se encuentran por ejemplo, los protocolos de información de enrutamiento (RIP), el cual es el IGP (Internal Gateway Protocol) más común de la red. RIP utiliza números de saltos como su única métrica de enrutamiento.

Protocolo de enrutamiento de Gateway interior (IGRP): es un IGP desarrollado por Cisco para resolver problemas relacionados con el enrutamiento en redes extensas y heterogéneas IGRP mejorado (EIGRP; E=Enhanced): este IGP propiedad de Cisco incluye varias de las características de un protocolo de enrutamiento de estado de enlace. Es por esto que se ha conocido como protocolo híbrido balanceado, pero en realidad es un protocolo de enrutamiento vector-distancia avanzado.

PROTOCOLOS DE ESTADO DEL ENLACE:

Los protocolos de enrutamiento de estado de enlace se diseñaron para superar las limitaciones de los protocolos de enrutamiento vector distancia. Los protocolos de enrutamiento de estado de enlace responden rápidamente a las modificaciones en la red, enviando actualizaciones sólo cuando se producen las modificaciones (triggered updates). También envían actualizaciones periódicas, conocidas como renovaciones de estado de enlace a rangos más prolongados; por ejemplo, 30 minutos. (RIP envía su tabla cada 30 segundos).

Cuando una ruta o enlace se modifica, el dispositivo que detectó el cambio crea una publicación de estado de enlace (LSA) en relación a ese enlace. Luego la LSA se transmite a todos los dispositivos vecinos. Cada dispositivo de enrutamiento hace una copia de la LSA, actualiza su base de datos de estado de enlace y envía la LSA a todos los dispositivos vecinos. Se necesita esta inundación de LAS para estar seguros de que todos los dispositivos de enrutamiento creen bases de datos que reflejen de forma precisa la topología de la red antes de actualizar sus tablas de enrutamiento.

Por lo general, los algoritmos de estado de enlace utilizan sus bases de datos para crear entradas de tablas de enrutamiento que prefieran la ruta más corta. Como pro ejemplo, la Ruta Libre Más Corta OSPG (Open Shortest Path First), Sistema Intermedio a Sistema Intermedio (IS-IS).

Los EGP enrutan datos entre sistemas autónomos. Un ejemplo de EGP es el protocolo de Gateway fronterizo (BGP).

5.5.1 Protocolo de enrutamiento EIGRP [CISCO2008]

En el proyecto específicamente se utiliza el protocolo EIGRP (extendido Protocolo de enrutamiento de gateway interior) que es una versión mejorada de IGRP (Protocolo de enrutamiento de gateway interior) desarrollada por Cisco, también conocido como protocolo de enrutamiento hibrido, utiliza el mismo algoritmo vector distancia, emplea el algoritmo de actualización de difunsión (DUAL), el cual garantiza el bucle libre de funcionamiento.

El EIGRP envía los paquetes, que son encapsulados en IPv4 o IPv6 y es responsable de la redistribución de rutas aprendidas de otros.

Ofrece propiedades de convergencia y eficacia operativa superiores, y combina las ventajas de los protocolos del estado de enlace con las de los protocolos por vector distancia.

Entre otras características se encuentra, que aumenta el ancho de la red hay que soporta de 15 hops a 224 hops, realiza actualizaciones parciales cuando el estado

de un destino cambia, eso reduce el ancho de banda para los paquetes EIGRP, de igual manera el neighbor discovery es utilizado para informar de los router vecinos, esto en el caso de IPv6.

Aunque no garantiza el uso de la mejor ruta, es bastante usado porque EIGRP es algo más fácil de configurar que OSPF. EIGRP mejora las propiedades de convergencia y opera con mayor eficiencia que IGRP. Esto permite que una red tenga una arquitectura mejorada y pueda mantener las inversiones actuales en IGRP.

Los routers EIGRP mantienen información de ruta y topología a disposición en la RAM, para que puedan reaccionar rápidamente ante los cambios. Al igual que OSPF, EIGRP guarda esta información en varias tablas y bases de datos.

EIGRP mantiene las siguientes tres tablas:

- **Tabla de vecinos**

  Cada router EIGRP mantiene una tabla de vecinos que enumera a los routers adyacentes. Esta tabla puede compararse con la base de datos de adyacencia utilizada por OSPF. Existe una tabla de vecinos por cada protocolo que admite EIGRP.

- **Tabla de topología**

  La tabla de topología se compone de todas las tablas de encaminamiento EIGRP recibidas de los vecinos. EIGRP toma la información proporcionada en la tabla de vecinos y la tabla de topología y calcula las rutas de menor costo hacia cada destino. EIGRP rastrea esta información para que los routers EIGRP puedan identificar y conmutar a rutas alternativas rápidamente. La información que el router recibe de los vecinos se utiliza para determinar la ruta del sucesor, que es el término utilizado para identificar la ruta principal o la mejor. Esta información también se introduce a la tabla de topología. Los routers EIGRP mantienen una tabla de topología por cada protocolo configurado de red (como IP, IPv6 o IPX). La tabla de enrutamiento mantiene las rutas que se aprenden de forma dinámica.

- **Tabla de encaminamiento**

  La tabla de encaminamiento EIGRP contiene las mejores rutas hacia un destino. Esta información se recupera de la tabla de topología. Los routers EIGRP mantienen una tabla de encaminamiento por cada protocolo de red.

5.6 Implementar un nodo Dual Stack y/o un túnel que permita enviar y recibir datagramas de IPv4 e IPv6 *[IETF2008].*

En este proyecto como se observa en la segunda etapa, se diseña e implementa un tunnel usando dos routers y dos computadores.

Una Dual Stack permite recibir datagramas de IPv4 o IPv6, no obstante el equipo debe soportarlo igualmente, aunque el enfoque sea *dual stack*, éste puede variar en función de qué partes de la pila de protocolos son compartidas y cuáles son independientes para cada versión de IP. Lo ideal sería que sólo la capa de red estuviese duplicada y que las demás capas fuesen compartidas (arquitectura de capa IP dual). Esto es lo que ocurre en Windows Vista, el nuevo sistema operativo de Microsoft, en contraste con Windows XP que dualiza la capa de red y la de transporte (arquitectura de pila dual generalizada), por lo que en algunos casos los administradores han de aplicar configuración redundante para cada pila. En términos generales, la aproximación *dual stack* no requiere necesariamente la creación de túneles, mientras que para crear túneles es imprescindible una aproximación *dual stack*. Aunque lo normal es que un nodo IPv6/IPv4 implemente ambas tecnologías. No obstante en el proyecto no se lleva a cabo un dual stack como tal ya que no se tiene una red ipv6 en cada extremo.

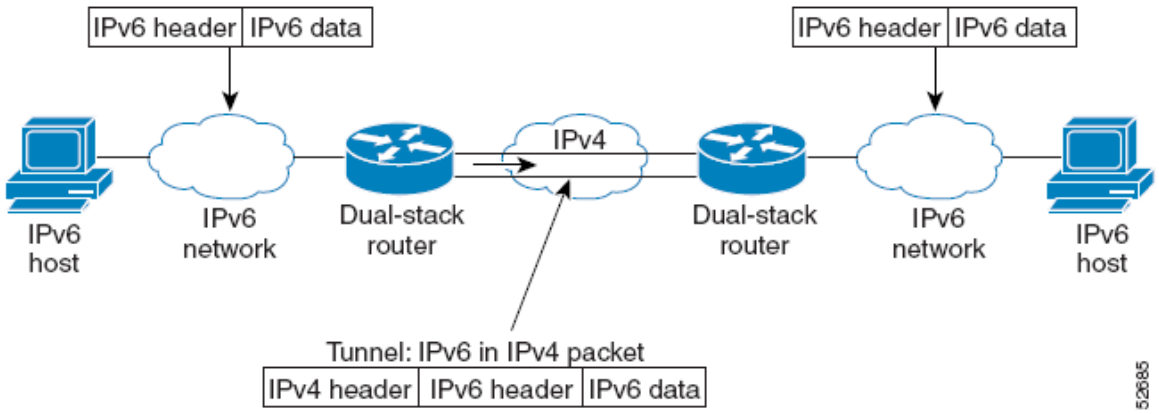


Figura 22. Nodo Dual Stack y Tunneling. [CISCO2008]

La importancia de implementar el tunnel es que nos permite implementar IPv6 en redes IPv4, es decir por medio de la unión de dos o mas routers es posible que se encapsulen los datagramas de IPv6 en paquetes de IPv4, lo que favorece la emigración al nuevo protocolo de internet, ya que se puede utilizar la infraestructura actual, no obstante existe otro tipos de túnel, que hacen lo contrario, o también se puede lograr la comunicación a través de una translación, como se explica teóricamente en el marco referencial.

5.7 Realizar las pruebas correspondientes utilizando un Sniffer, para analizar las tramas de IPv4 e IPv6.

En la siguiente figura se observa la trama de IPv6 cuando se hace la comunicación entre un equipo 1 con IPV6, pasando por el tunnel el cual encapsula los paquetes de IPv6 en datagramas en IPv4, y luego los desencápasela para que lleguen al equipo 2 que también maneja un direccionamiento IPv6 y se puede divisar la trama en la figura 23 y 24.

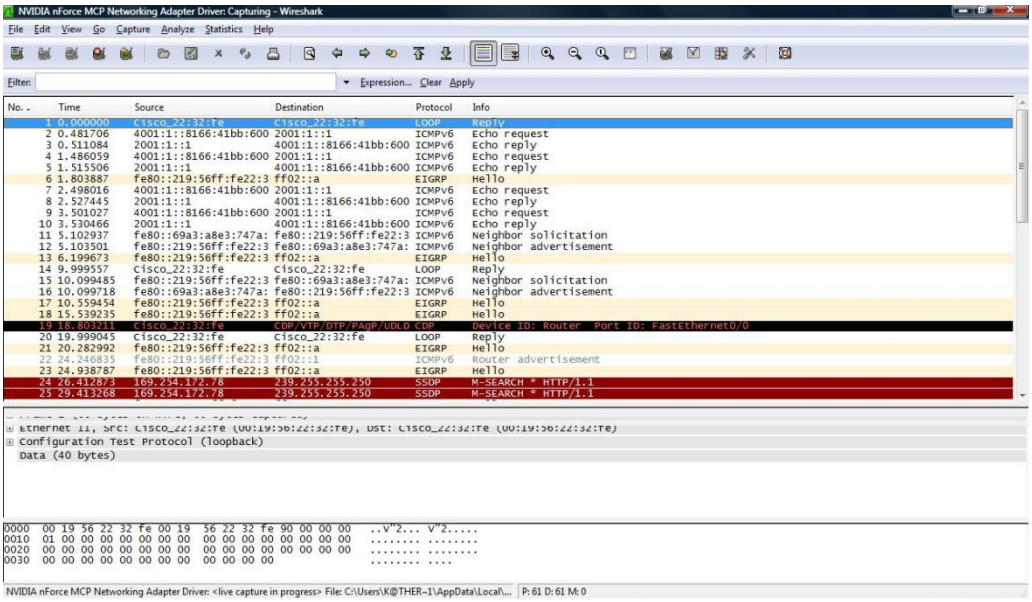


Figura 23. Equipo transmisor

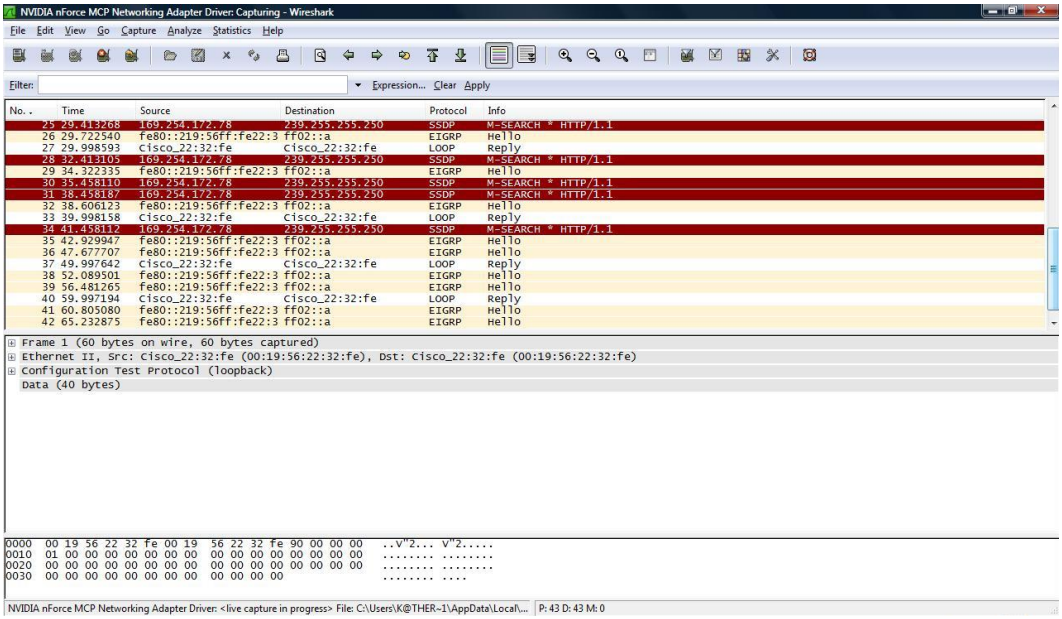


Figura 24. Equipo Receptor

6. PRUEBAS Y RESULTADOS

En esta etapa de la monografía, cabe anotar todas las pruebas realizadas para llegar a un optimo resultado, sin embargo dichas pruebas actualmente en el nuevo planteamiento del proyecto no son las mas adecuadas, ya que no son los requerimientos sugeridos, pero estas hacen parte del proceso de desarrollo del mismo.

6.1 Prueba 1.

Durante la realización del proyecto se plantearon diversas soluciones para el mismo entre ellas realizar un solo nodo Dual Stack, conectado dos host con Windows vista los cuales soportan IPv4 e IP v6.

6.1.1 VLC [VLC2003]

Es un reproductor multimedia (VideoLAN Client), soporta diferentes tipos de códecs de audio y video, de igual manera soporta varios formatos de los mismos. Este también puede ser usado como servidor en IPv4 o IPv6.

VLC es un software libre (freeware) y se puede descargar de la página www.videolan.org.

VLC es la solución de software completa para la trasmisión de video, desarrollada por estudiantes de Ecole Centrale Paris y desarrolladores de todo el mundo, dentro de GNU General Public License (GPL). VideoLAN está diseñado para transmitir vídeo MPEG en redes con gran capacidad de ancho de banda.

La solución VideoLAN incluye:

- VLS (Servidor VideoLAN), el cual puede transmitir archivos MPEG-1, MPEG-2 y MPEG-4, DVDs, canales digitales de satélite, canales digitales de televisión terrestre y vídeo en vivo sobre la red en unicast o multicast,
- VLC (inicialmente cliente VideoLAN), el cual puede ser usado como servidor para transmitir archivos MPEG-1, MPEG-2 y MPEG-4, DVDs y vídeo en vivo sobre la red en unicast o multicast; o usado como cliente para recibir, decodificar y visualizar flujos MPEG sobre varios sistemas operativos.

VLC trabaja sobre muchas plataformas: Linux, Windows, Mac OS X, BeOS, *BSD, Solaris, Familiar Linux, Yopy/Linupy y QNX. Puede leer archivos MPEG-1, MPEG-2 y MPEG-4 / DivX desde un disco duro, un CD-ROM, DVDs y VCDs, desde un

tarjeta receptora de satélite (DVB-S), Flujos MPEG-1, MPEG-2 y MPEG-4 desde la red enviados por la salida de VLS o VLC's.

VLC también puede ser usado como servidor para transmitir archivos MPEG-1, MPEG-2 y MPEG-4 / DivX, DVDs, desde una tarjeta codificadora MPEG.

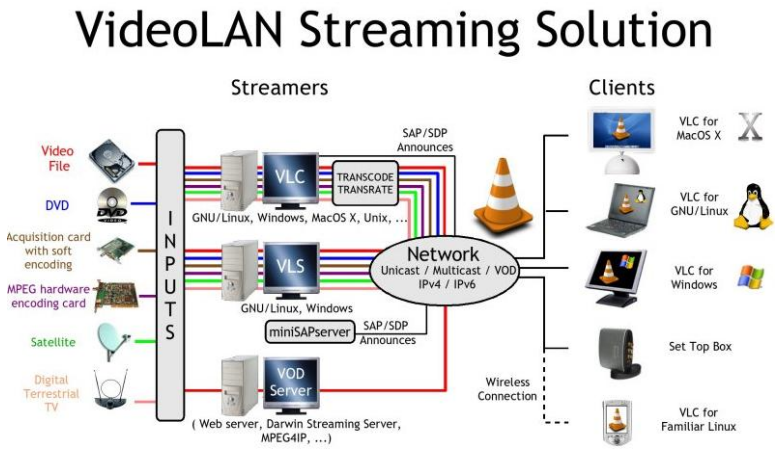


Figura 25. La solución VideoLAN global [VLC2003]

Se utiliza VLC para la codificación, los pasos a seguir son los siguientes:

1. Al ingresar a VLC se va archivo y se selecciona la opción de abrir archivo, obteniendo la siguiente pantalla, en donde se selecciona el botón de explorar y se carga el archivo que se quiere codificar, de igual manera se elige el botón de volcado/salvar y caché. Ver figura 26.

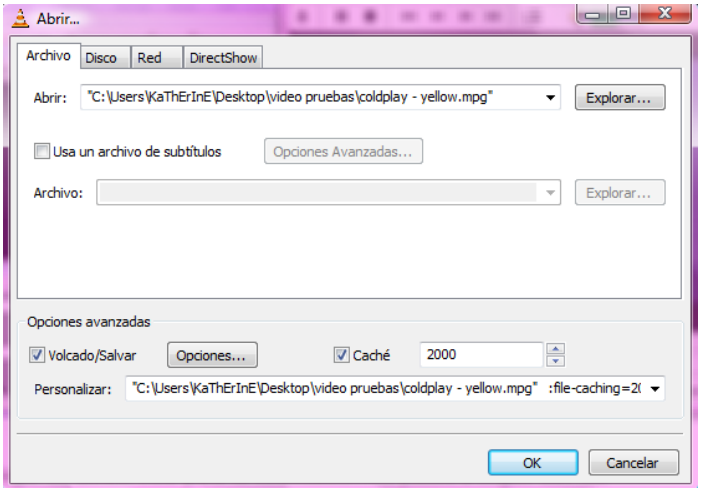


Figura 26. Pantalla abrir archivo.

2. Después de elegir volcado/salvar, se selecciona el botón opciones en donde se abre una nueva ventana, en la cual se escoge la opción reproducir localmente, luego se elige el protocolo de transmisión a utilizar, allí se ingresa la dirección IP y el puerto, de igual manera se debe selecciona el códec de video y audio, la tasa de bits de cada uno y por ultimo se escoge la opción de elige todo volcado elemental y tiempo de vida. Ver figura 27.

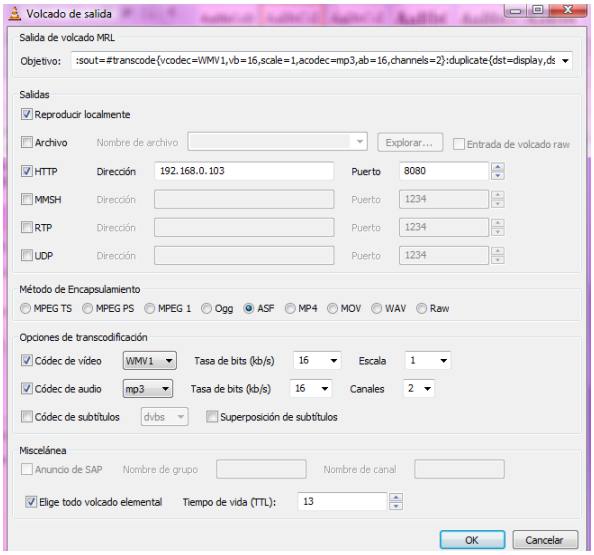


Figura 27. Pantalla volcado de salida.

3. Por ultimo se da ok y aparece la siguiente ventana de la figura 28. con el video que se esta transmitiendo.

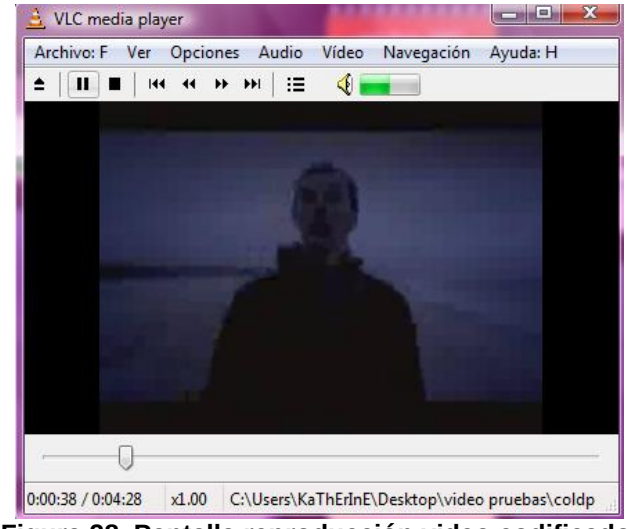


Figura 28. Pantalla reproducción video codificado.

4. Para recepción del video trasmitido a otro computador, es necesario en este abrir un Explorer y le dar el comando [mms:///(dirección IP) :(puerto)] el cual se señala en rojo en la siguiente pantalla. El comando mms (Microsoft media services) es un protocolo para hacer Streaming de contenido multimedia. (Figura 29).

Figura 29. Pantalla recepción del video transmitido.

5. El comando dado en el paso anterior permite que de inmediato se cargue el archivo transmitido, este lo hace atreves del reproductor de Windows media en primer lugar sale conectado con el medio, luego almacenando en buffer, para luego mostrar el video. Como se observa en la parte inferior de las pantallas mostradas en las figuras 30, 31 y 32.

Figura 30. Pantalla conectando con medio

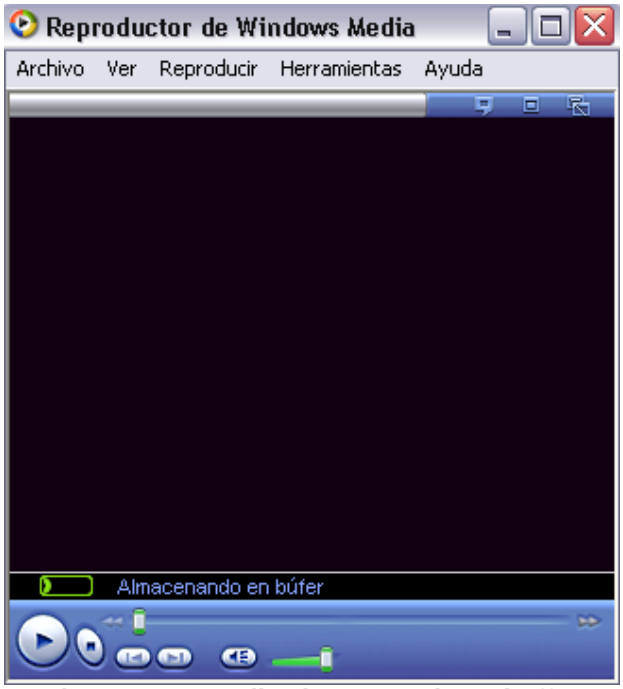


Figura 31. Pantalla almacenando en buffer

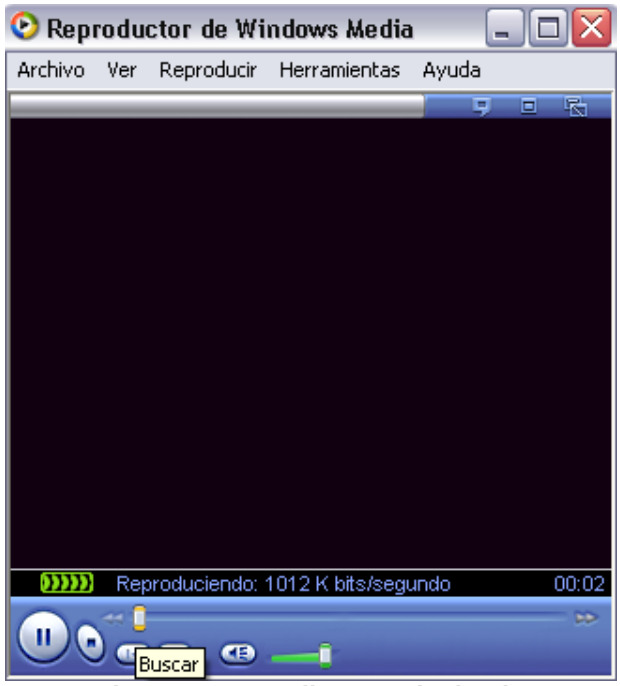


Figura 32. Pantalla reproduciendo

6.1.2 WINDOWS MEDIA ENCODER

A través de Windows media Encoder, se realiza la misma transmisión de video streaming como en la prueba anterior, usando IPv4.
Los pasos a seguir para un óptimo resultado son:

1. Se debe escoger el tipo de captura que se desee, en este caso se va a difundir un video existente en el PC. (Figura 33).

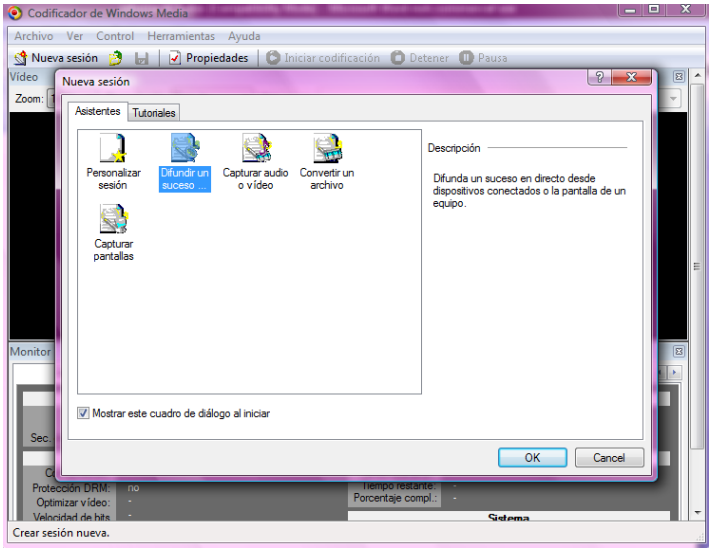


Figura 33. Pantalla tipo de captura.

2. En esta ventana se da la opción de escoger el dispositivo que se desee, ya sea por capturadora de video y audio, por la cámara y micrófono del equipo o por defecto si se quiere capturar un archivo desde tu PC. (Figura 34).

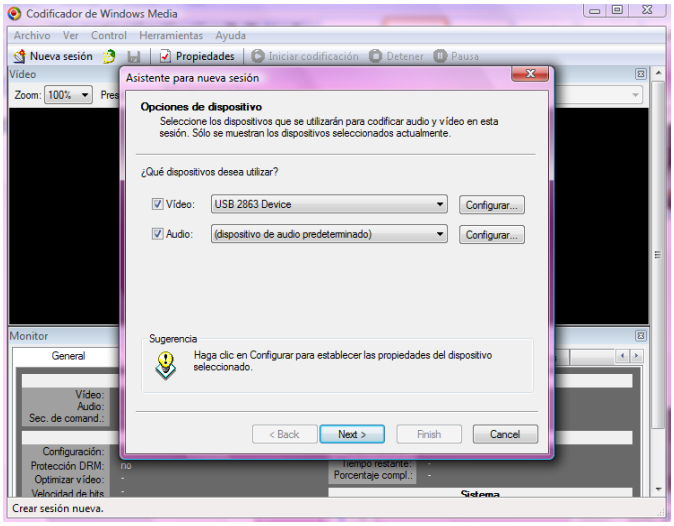


Figura 34. Pantalla selección dispositivo.

3. En este caso se va a utilizar la tarjeta de video USB 2863, por lo tanto es necesario realizar su configuración teniendo en cuenta el canal y el tipo de entrada. (Figura 35).

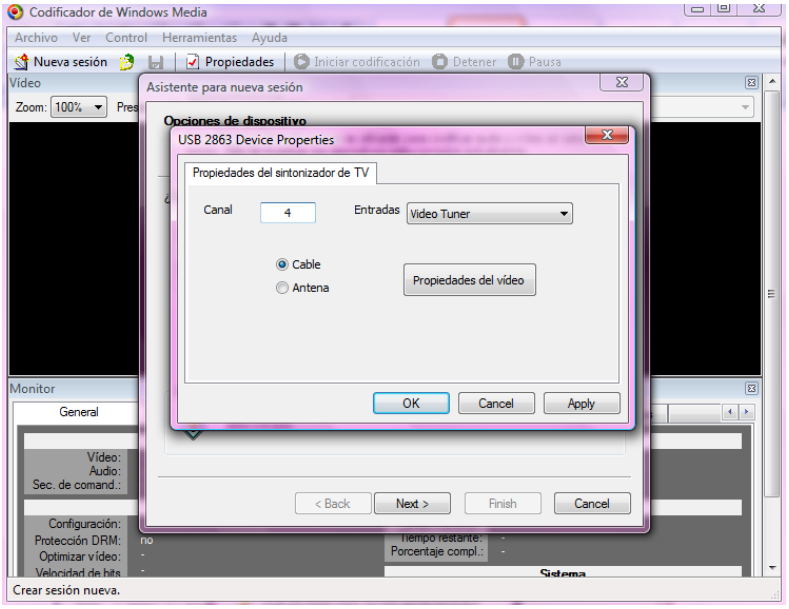


Figura 35. Pantalla configuracion dispositivo.

4. El siguiente paso da la opción de escoger el método de difusión. (Figura 36).

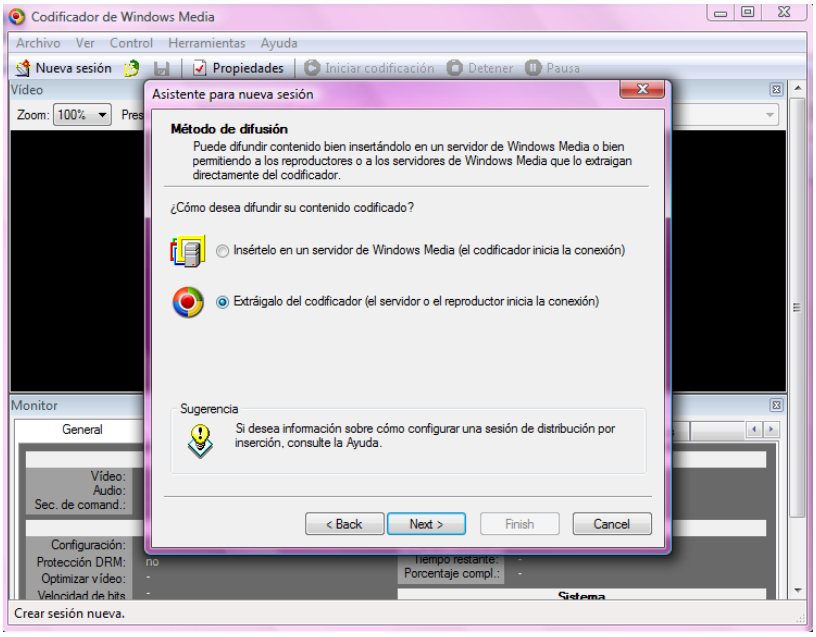


Figura 36. Pantalla método de difusión.

5. En esta ventana se selecciona el puerto y Windows media encoder da la dirección IP por defecto (Figura 37).

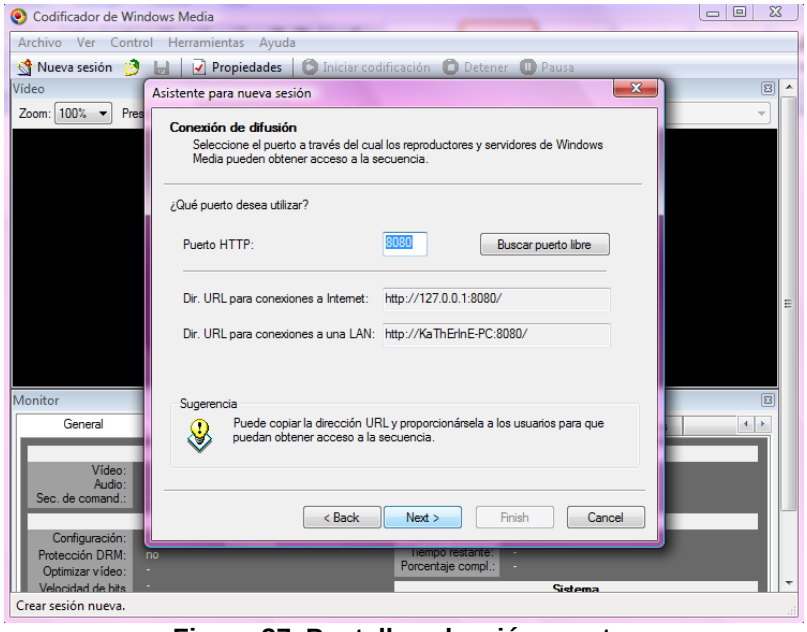


Figura 37. Pantalla selección puerto.

6. Esta es la opción de codificación, es decir a que tasa de bits desea transmitir. (Figura 38).

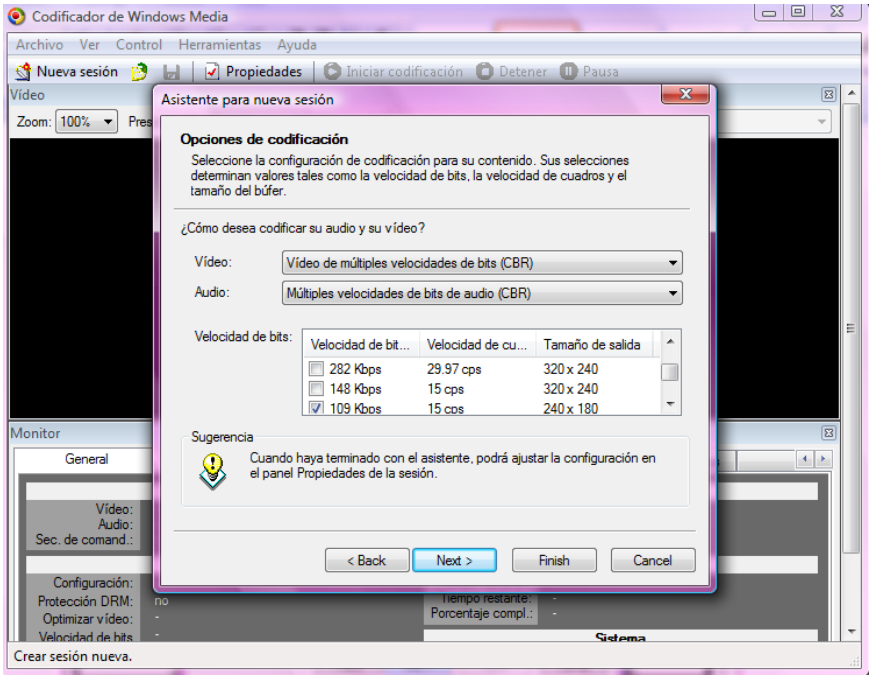


Figura 38. Pantalla tasa de bits

7. Se puede guardar el archivo a transmitir. (Figura 39).

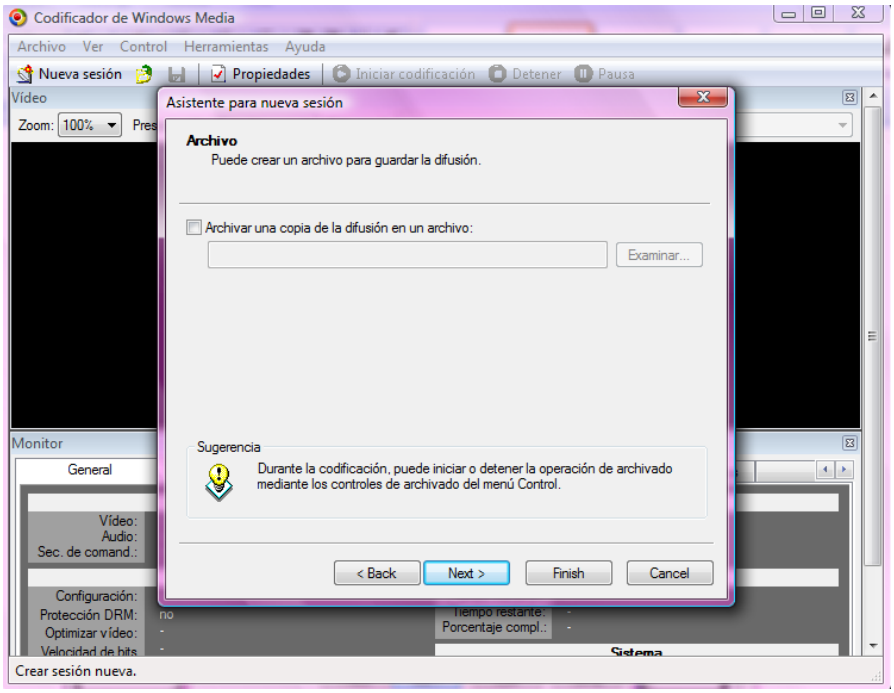


Figura 39. Pantalla guardar archivo.

8. Esta ventana muestra la opción de agregar archivos de video. (Figura 40).

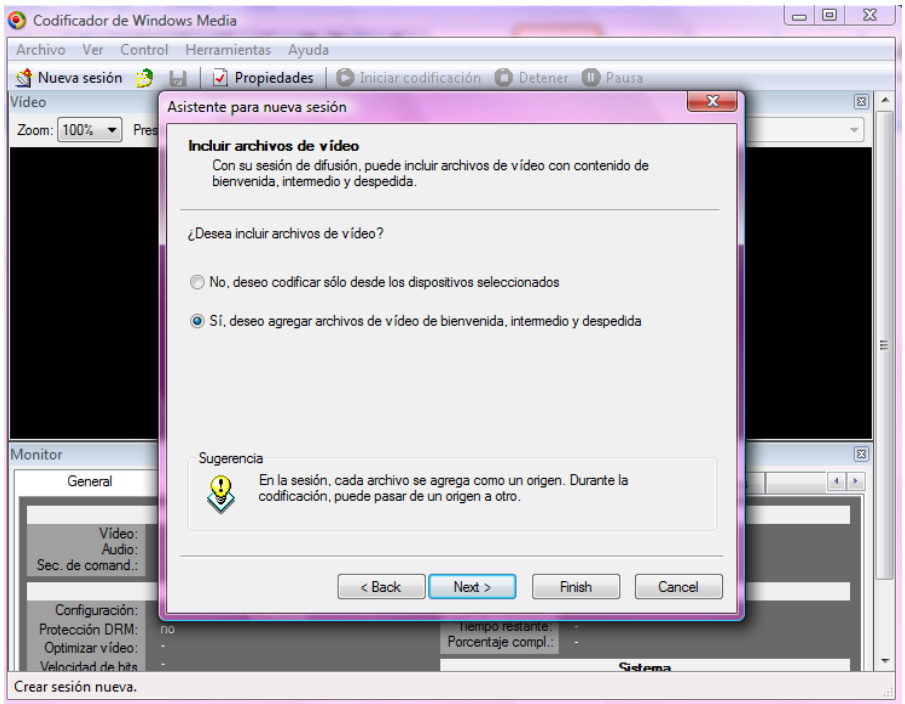


Figura 40. Pantalla agregar archivo de video

9. Se escoge el archivo a codificar. (Figura 41).

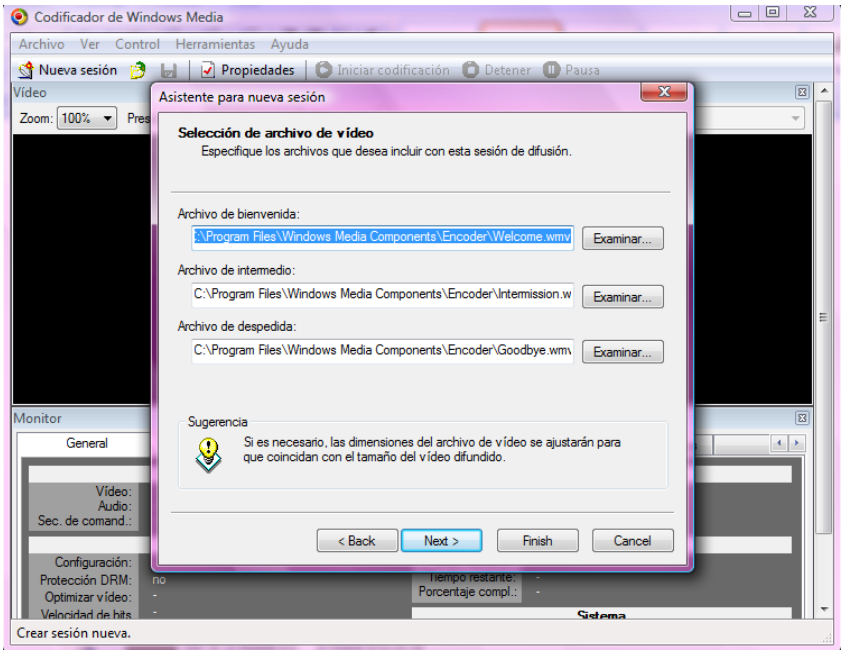


Figura 41. Pantalla archivo a codificar.

10. Si se desea se puede añadir información del archivo. (Figura 42).

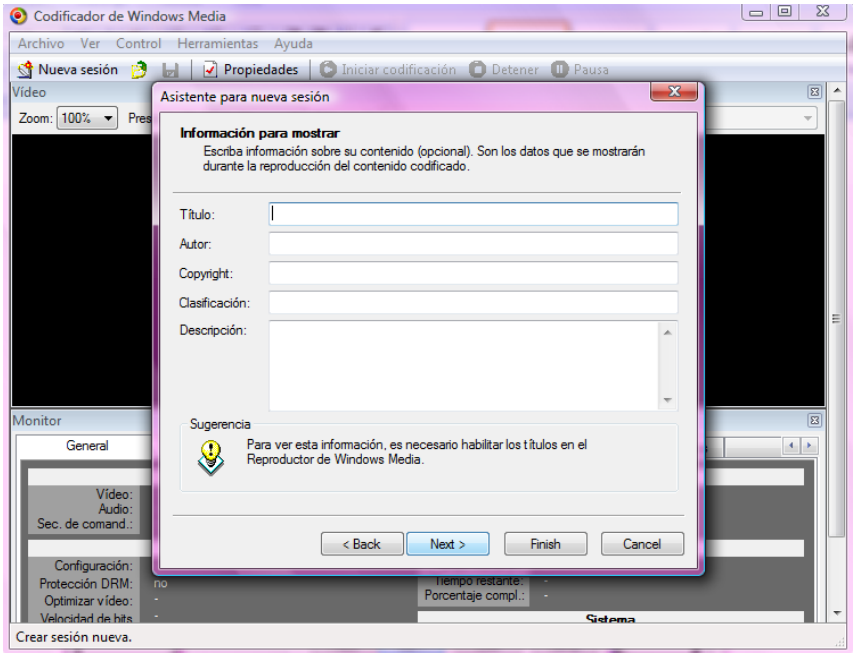


Figura 42. Pantalla información archivo.

11. Esta ventana muestra la configuración hecha anteriormente. Y después de revisar que todo este correcto, se da finalizar. (Figura 43).

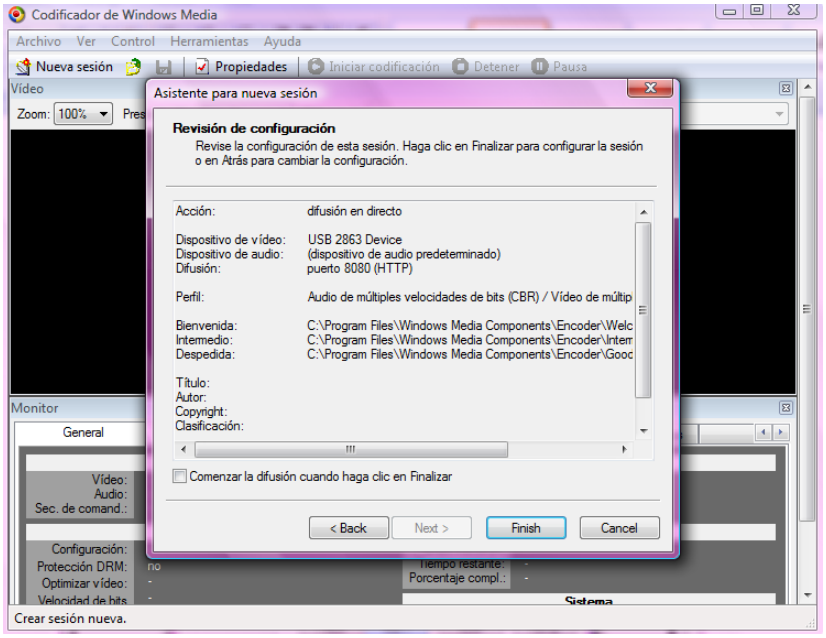


Figura 43. Pantalla visor configuración.

12. En esta pantalla se muestra el video a codificar y su codificación. No obstante desde otro equipo se abre una pagina de Explorer y se le da el comando mms://(dirección IP):(Puerto). (Figura 44).

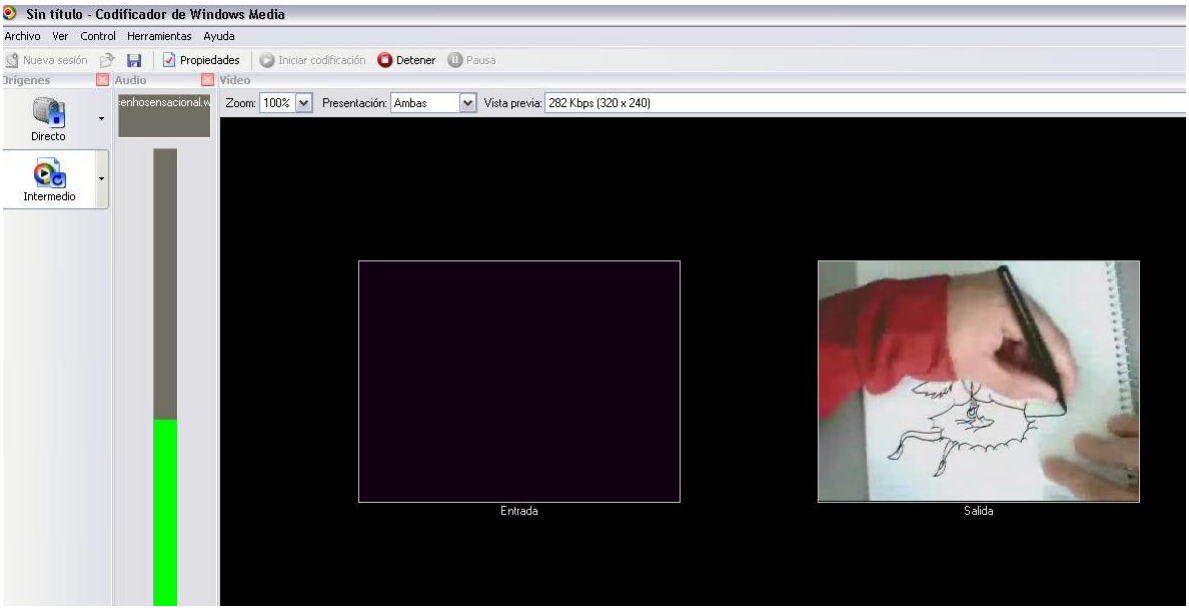


Figura 44. Pantalla recepción de video.

Durante la transmisión del video streaming bajo el protocolo IPv4, por medio de un software espía o analizador de tráfico, llamado Wireshark se hace la captura de los paquetes envidos, como se muestra en la figura 45.

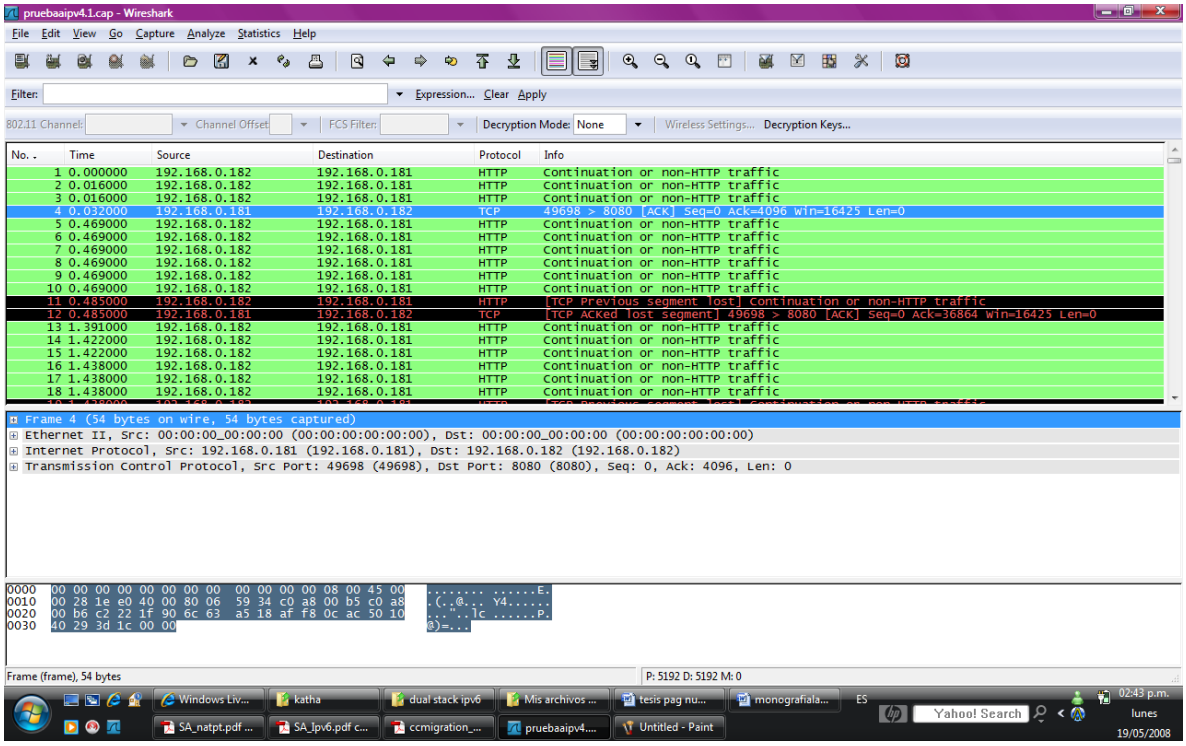


Figura 45. Análisis transmisión 1pv4

Vale aclarar que la transmisión de video streaming usando los dos codec's, se hizo a través del Router, es decir, cada computador esta conectado a un puerto Ethernet, formando así, la red IPv4

6.2 Prueba 2

Como se ha explicado anteriormente el Router cisco 801, solo consta de un puerto WAN, que soporta IPv6 por lo tanto no fue posible realizar la misma prueba que se hizo con IPv4, sin embargo usando vlc, se hizo la codificación y decodificación del video en el mismo equipo dando como resultado lo siguiente:

1. Al igual que con IPv4 se da la opción de abrir un archivo, se carga el archivo a transmitir y se selecciona volcado y el cache. (Figura 46).

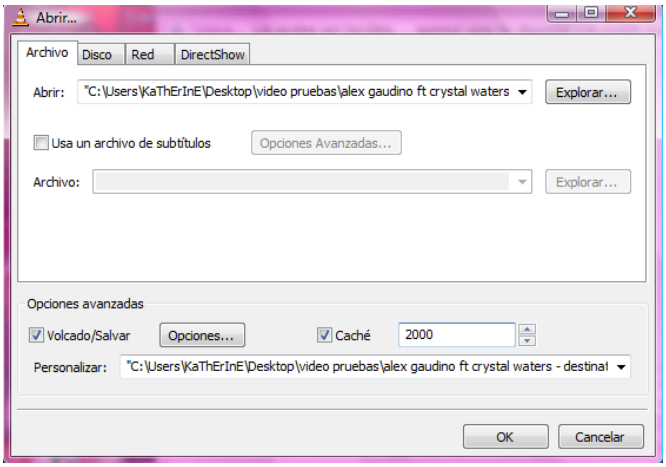


Figura 46. Pantalla abrir archivo.

2. En opciones de volcado se selecciona lo mismo que en IPv4 pero en este caso al dirección IP cambia, por una de versión 6, como se muestra subrayado en la siguiente imagen. (Figura 47).

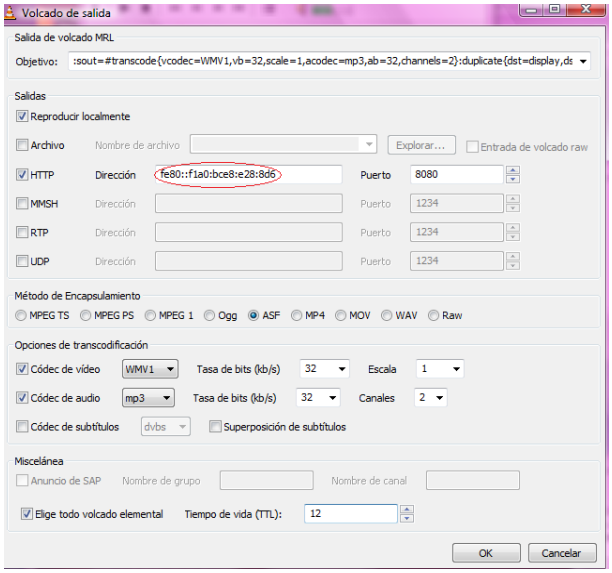


Figura 47. Pantalla volcado de video.

3. En esta pantalla se muestra el video a transmitir. (Figura 48).

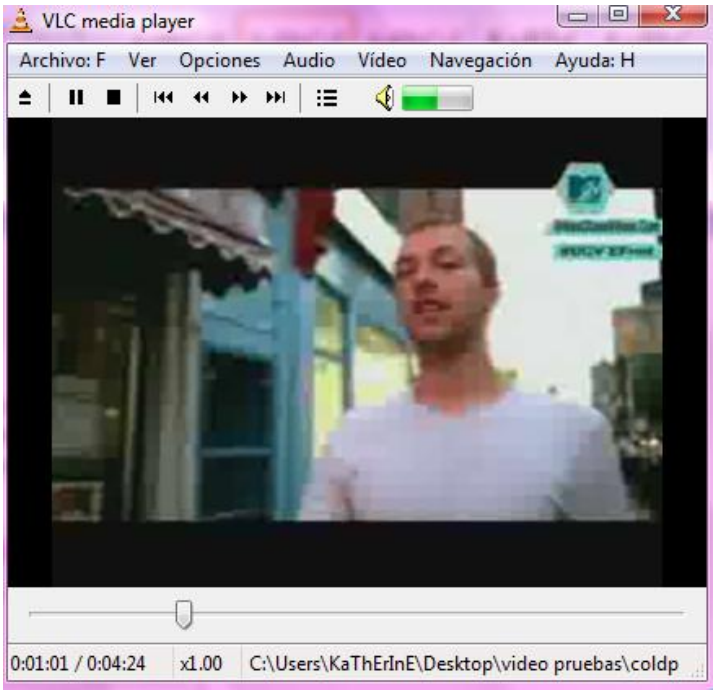


Figura 48. Pantalla video a transmitir.

4. Para comprobar que si se esta llevando a cabo dicha codificación desde otra ventana de VLC se da la opción de abrir volcado de red. (Figura 49).

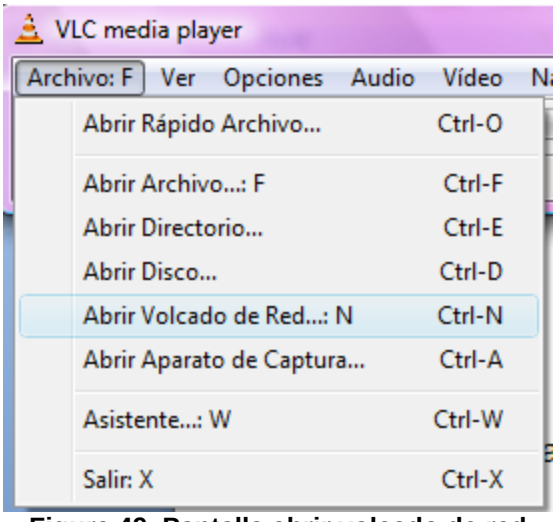


Figura 49. Pantalla abrir volcado de red

5. Posteriormente abre la siguiente ventana donde se da la dirección IPv6 y el tipo de protocolo en el que se esta codificando. (Figura 50).

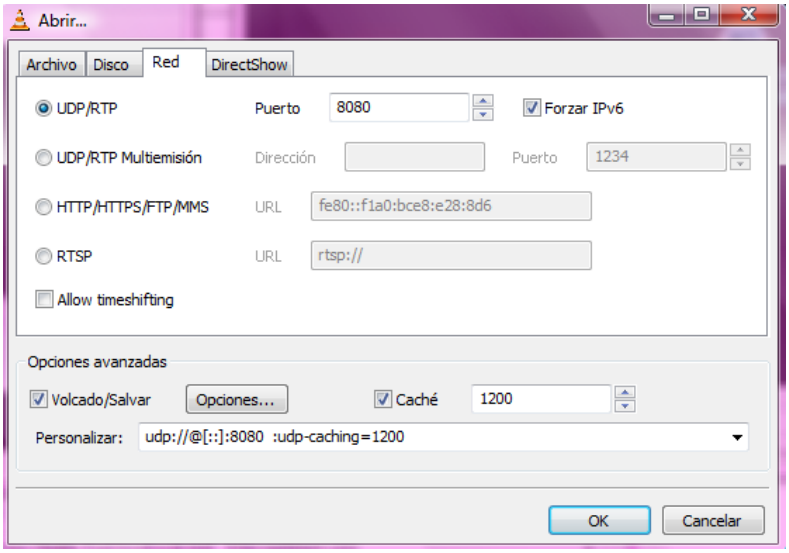


Figura 50. Pantalla red.

6. En la siguiente imagen se observa la dirección subrayada en rojo, los dos puntos encerrados en corchetes indica que es de versión 6, y al lado el puerto en el que se esta transmitiendo, la imagen de la izquierda es el video codificado, y el de la derecha, el archivo a codificar, si embargo existe un retardo, pero es un retardo normal. (Figura 51).

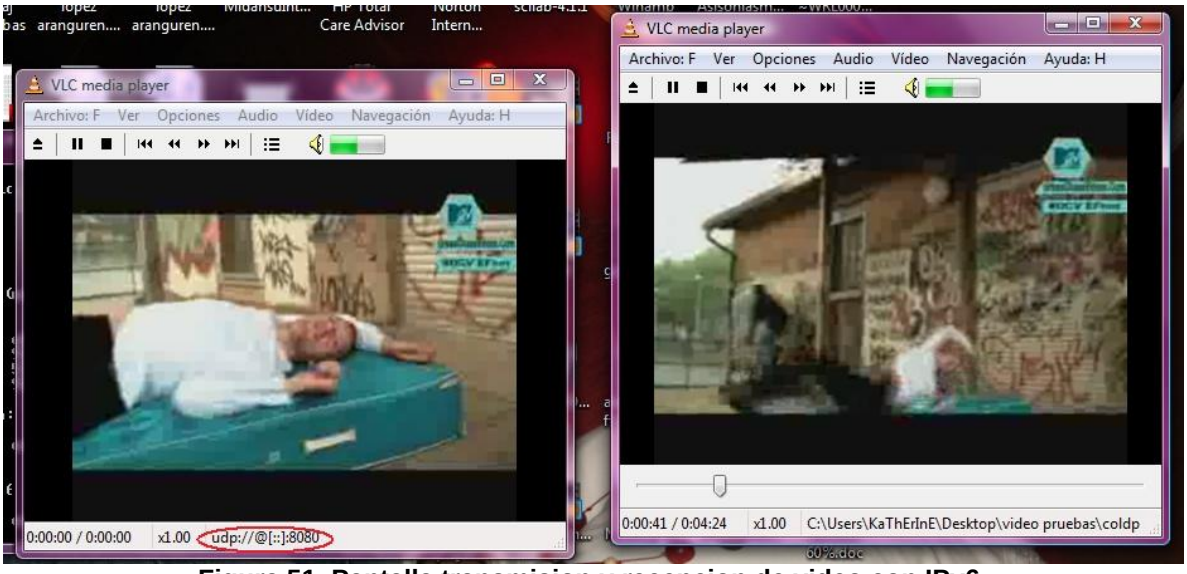


Figura 51. Pantalla transmision y recepcion de video con IPv6.

6.3 Prueba 3

Después de los diferentes experimentos con Windows vista para transmitir video streaming, se realiza la misma prueba con el sistema operativo Linux, ya que en primera instancia es un software libre y segundo permite ser manipularlo mas fácilmente, no obstante en Windows vista aunque es un sistema operativo que soporta trafico IPv6, como es nuevo presenta muchos errores y diversos permisos obstruidos, los cuales no son simples de habilitar y mas por la falta de información

1. En la siguiente pantalla se muestra la configuración desde el terminal en el sistema operativo Linux Ubuntu, en este código se indica la dirección de donde se encuentra el archivo y su extensión, de igual manera la dirección del equipo a transmitir y la interface de salida, seguida por el tiempo de vida. (Figura 52).

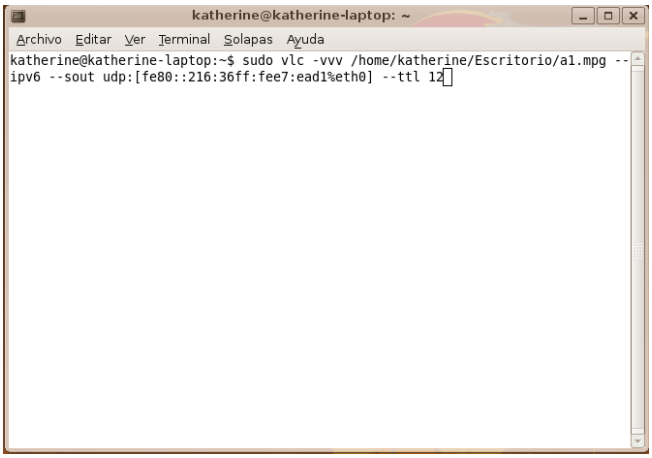


Figura 52. Equipo transmisión de video

2. En la siguiente pantallazo se muestra el terminal de Linux Ubuntu desde el equipo receptor con su código correspondiente. (Figura 53).

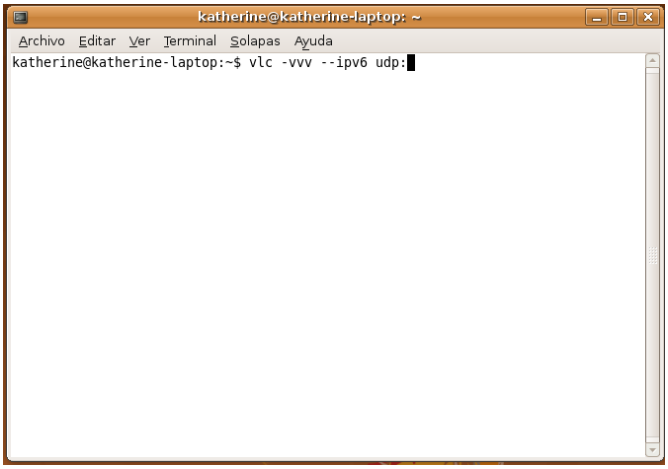


Figura 53. Configuración de quipo recetor

3. En este pantallazo se muestra cuando el video ya esta transmitiendo y espera respuesta del receptor. (Figura 54).

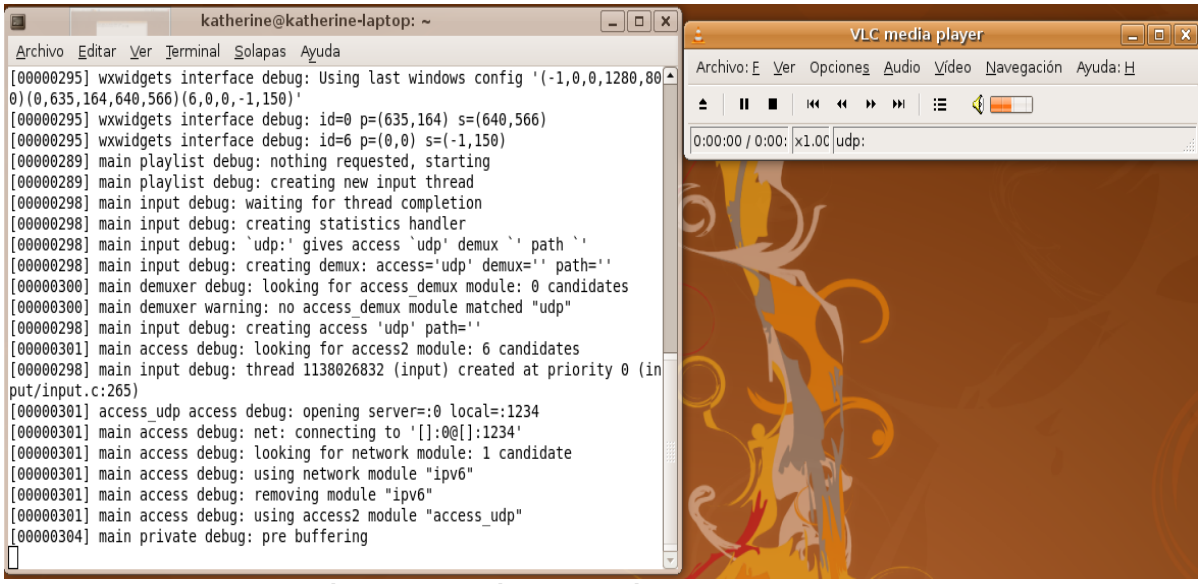


Figura 54. Equipo transmisor

4. el video transmitido en el equipo receptor. (Figura 55).

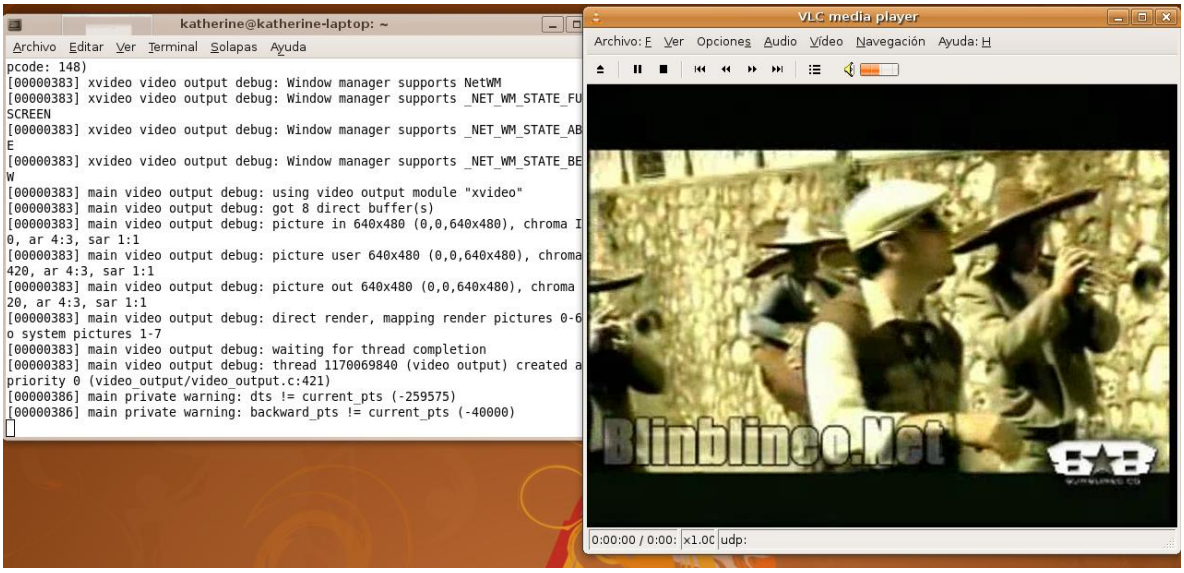


Figura 55. Video transmitido en el equipo receptor

5. en los siguientes pantallazos se puede observar los datagramas IPv6, en el equipo transmisor y en el receptor. (Figura 56 y 57).

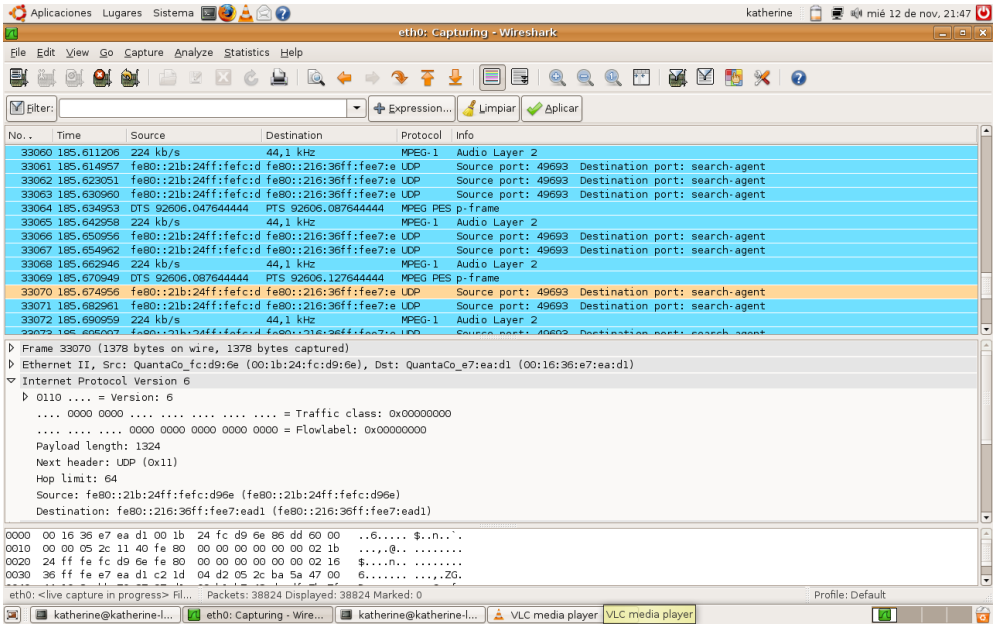


Figura 56. Análisis trama IPv6 en el equipo transmisor

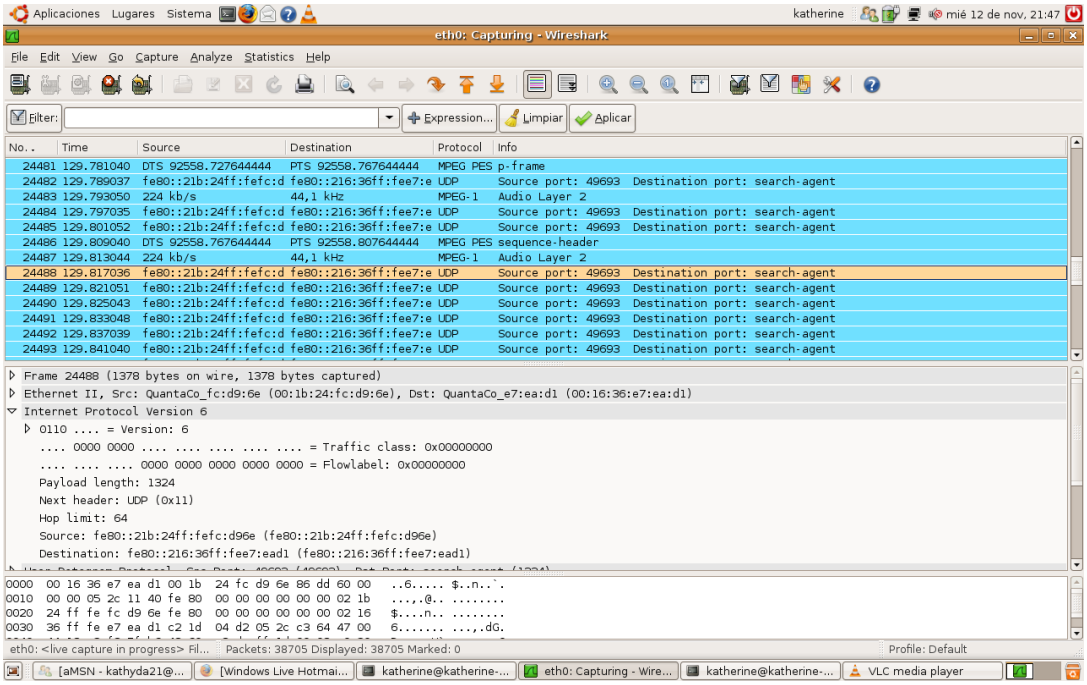


Figura 57. Análisis trama IPv6 en el equipo receptor

7. CONCLUSIONES

- Existen diversos programas que permiten la decodificación de video, sin embargo en este proyecto en primer lugar se quiso usar el Windows media Encoder el cual era útil para realizar la trasmisión de video streaming bajo el protocolo ipv4, no obstante, este no permite realizar la transferencia con el protocolo ipv6, ya que como se dijo anteriormente solo maneja direcciones de 32 bits.

- La dificultad de este proyecto se ve reflejada en la búsqueda del dispositivo a utilizar ya que actualmente cisco maneja diversos router que soportan IPv6 dependiendo del IOS que puedan soportar, no obstante estos equipos tiene un costo elevado y son difíciles de adquirir.

- Algunas de las implementaciones actuales de IPv6, tales como las que hay en el sistema operativo IOS de CISCO son muy limitadas, ya que no cuentan con una implementación de IPSec nativa IPv6, en su lugar utilizan la implementación de IPSec sobre IPv4 y la aplican sobre túneles 6to4, debido a esto se pierde el potencial real de los servicios de seguridad ofrecidos por IPv6.

- La versión 12.2(11)T3 de IOS además no cuenta con soporte para manejo de QoS, ni soporte para tráfico multicast sobre IPv6, por lo tanto fue necesario utilizar un IOS mas actualizado como es el IOS 12.4 (6) o 12.4(15).

- Realizar una red de IPv6 punto a punto no fue posible por la incompatibilidad de versión del sistema operativo Windows vista, deben ser la misma edición.

- Para realizar una comunicación optima entre redes con IPv4 e IPv6, no basta con un solo Router ya que este no se va a entender con un host sino con otro Router, siendo este el problema principal, presentado en el desarrollo del proyecto, sin embargo es posible usar solo una dual stack cuando en el equipo se ha realizado una configuración oportuna, para que se puedan entender.

- El túnel permite con mayor facilidad, la emigración a IPv6, ya que es un método sencillo, y lo más importante es que minimiza costos porque es posible utilizar las redes actuales.

- Para realizar la transmisión de video Streaming usando el servidor vlc, fue necesario realizarla en el sistema operativo Linux, en este caso Ubuntu, ya que es fácil de manipular las direcciones y vlc tiene un mejor comportamiento en este.

- Se debe tener en cuenta que no basta con realizar el tunnel si no se tiene definido un protocolo de enrutamiento y realizar una correcta asignación de direcciones IP.

- Aunque existen diversos software o decodificadores de videos, actualmente son pocos los que permiten transmitir tramas IPv6, ya que permiten transmitir solo usando la dirección IPv6 que viene por defecto la cual es basada en la MAC del esquipo.

- El sistema operativo Linux Ubuntu permite realizar una red IPv6, y transmitir el video streaming, sin inconvenientes y fácilmente.

8. RECOMENDACIONES

Cabe anotar que para el manejo de direccionamiento IPv6, se debe manejar un sistema operativo que lo soporte. Actualmente Microsoft cuenta con Windows vista que este por defecto lo trae, sin embargo en Windows anteriores se puede utilizar un service pack 2, igualmente con Linux, Mac, entre otros que ya facilitan realizar aplicaciones que soporten IPv6.

Una recomendación es tener clara la aplicación a utilizar con IPv6, ya que recientemente no todas las aplicaciones lo soportan.

A la hora de escoger el equipo, es importante tener en cuenta sus características físicas, y si es posible actualizar el IOS para que permita implementar IPv6 y sus protocolos de enrutamiento.

9. TRABAJO FUTURO

La realización de un nodo dual stack o de un túnel que permita la transferencia de datos, audio y video de ipv4 a ipv6 se puede realizar mediante un software, o bien usando las diversas series de routers Cisco, tales como las 2811, 7200.

Construir un sistema que provea servicio de videoconferencia sobre IPv6/IPv4 a partir de la implementación VideoLAN, en la cual las transmisiones puedan iniciarse a partir de peticiones de los clientes.

Realizar este proyecto usando el mecanismo de trasmisión de traducción de protocolos.

Realizar un túnel, usando dirección dinámica, es decir usando un mayor número de equipos.

10. GLOSARIO

- **VIDEO STREAMING:** Es la transmisión de video o audio en tiempo real. No es necesario descargar el archivo para verlo sino que se pude mirar al mismo tiempo en el que este se descarga. [ALVA2004]

- **DUAL STACK:** Plataforma que permite introducir nodos de IPv4/IPv6. tiene la capacidad de enviar y recibir tanto datagramas de IPv4 como IPv6. [MUÑO2004]

- **PROTOCOLO DE INTERNET (IP):** Protocolo Internet, proporciona los medios necesarios para la transmisión de bloques de datos llamados datagramas desde el origen al destino, donde origen y destino son hosts identificados por direcciones de longitud fija [REQU1981].

- **IPV4:** Protocolo de Internet versión 4 [REQU1981].

- **IPv6:** Protocolo de Internet versión 6 [REQU1981].

- **PROTOCOLO:** Se define como protocolo al conjunto de reglas que controlan la secuencia de un mensaje que ocurre en la comunicación de un equipo a otro en una red. [WIKI]

- **UDP:** User Datagram Protocol. Es un protocolo del nivel de transporte basado en el intercambio de datagramas. [WIKI].

- **TCP:** Es el Protocolo de Control de Transmisión [WIKI].

- **SSH:** Secure SHell. Protocolo de seguridad. [WIKI].

- **SSL:** Secure Socket Layer. Protocolo de seguridad. [WIKI].

- **FTP:** File Transfer Protocol. Protocolo de transferencia de archivos. [WIKI].

- **ICMP:** Internet Control Message Protocol. Protocolo de Control de Mensajes de Internet. [WIKI].

- **IEEE:** Institute of electrical and electronics engineers, organización en los estados unidos de ingenieros eléctricos y electrónicos. [IEEE2008].

- **DATAGRAMA:** es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente encaminar

el fragmento hacia el equipo terminal de datos receptor, de manera independiente a los fragmentos restantes. [WIKI].

- **MMS:** Microsoft Media Services, un protocolo para hacer Streaming de contenido multimedia. [WIKI].

- **ASF:** Advanced Streaming Format (o ASF, posteriormente renombrado a Advanced Systems Format) es un contenedor multimedia de audio y video digital propiedad de Microsoft, diseñado especialmente para el streaming. [WIKI].

- **CODEC:** es un algoritmo de comprensión utilizado para reducir el tamaño de un flujo. [WIKI].

- **MPEG:** es un códec. Existen versiones MPEG1, MPEG2. [WIKI].

- **WMV:** es un nombre genérico que se da al conjunto de algoritmos de compresión ubicados en el set propietario de tecnologías de video desarrolladas por Microsoft, que forma parte del framework Windows Media. [WIKI].

- **MP3: MPEG-1 Audio Layer 3**, más conocido como **MP3**, es un formato de audio digital comprimido con pérdida desarrollado por el Moving Picture Experts Group (MPEG) para formar parte de la versión 1 (y posteriormente ampliado en la versión 2) del formato de vídeo MPEG. Su nombre es el acrónimo de MPEG-1 Audio Layer 3. [WIKI].

- **NAT:** Network Address Translation. Traducción de dirección. [WIKI].

- **DNS:** Protocolo de resolución de nombres de dominio. [WIKI].

- **ARP:** Protocolo de resolución de direcciones. Permite determinar los dispositivos de la capa 2 y las direcciones capa 3. [WIKI].

- **DCHP:** (Dynamic Host Configuration protocol) es un protocolo de red que permite a los nodos de una red IP obtener parámetros de configuración automáticamente. Protocolo tipo cliente-servidor, donde un servidor posee una lista de direcciones y las va asignando a los clientes, sabiendo a quien, el tiempo y quien ha estado en la posición de esta. [WIKI].

- **OSPF**: (Open Shortest Path First) protocol de enrutamiento jerárquico de pasarela interior. [WIKI].

- **EIGRP** extendido (Protocolo de enrutamiento de gateway interior extendido**):** Versión avanzada de IGRP desarrollada por Cisco. Ofrece

propiedades de convergencia y eficacia operativa superiores, y combina las ventajas de los protocolos del estado de enlace con las de los protocolos por vector distancia. Comparar con IGRP. Ver también OSPF y RIP. [CISCO2008].

11. BIBLIOGRAFÍA

11.1 Referencias Bibliográficas

- [SATL2000] Stalling William. Comunicaciones y Redes de Computadores. Sexta edición. Editorial Prentice Hall.2000
- [AUST2002] Austerberry David. La Tecnología del Streaming de Video y Audio. Editorial Focal Press.2002.
- [DAVI2003] Davies Joseph. Understanding IPv6.2003
- [HUNT1997] Hunt Craig. TCP/IP Network Administration. Segunda edicion.1997.
- [MILLA2003]Ramón Jesús Millán Tejedor. El Protocolo de Internet IPv6.
- [VERD2000] Gabriel Verdejo Álvarez. El protocolo IPv6 y sus extensiones de seguridad IPSec. Universidad Autónoma de Barcelona. 2000

11.2 Referencias de Internet

- [ALVA2004] Miguel, Álvarez. ¿Que es Streaming? Desarrollo web. www.desarrolloweb.com/manuales/queesstreaming.htm, Visitada el 18 de septiembre de 2006.
- [MUÑO2004] Muñoz Lucavechi Joaquín. Centro de tecnología de información, CNTI.2004
- [REQS1981] Request For Vommrnts. www3.reft.org/rfc.html
- [VLC2003] VLC Media Player. www.videolan.org
- [KAND2000] Ettikan Kandasamy Karuppiah, Gopi Kurup, Takefumi amazaki,"Application Performance Analysis In Transition Mechanism From Ipv4 to IPv6", *Proceedings APAN Conf. 2000*, Tsukuba, Japan, Feb. 14-18, 2000. http://www.my.apan.net/ipv6/Papers/ettikan.PDF
- [WIRE2008] Wireshark. www.wireshark.org
- [WIKI] http://es.wikipedia.org/wiki
- [IEEE2008] http://www.ieee.org/portal/site
- [CISCO2008] www.cisco.com
- [IETF2008] www.ietf.org

12. ANEXOS

Anexo 1. RFC relacionados con IPV6

Documento	Título	
Especificaciones Básicas	RFC2460	Especificaciones del Protocolo Internet Versión 6 (IPv6)
	RFC2461	Descubrimiento del Vecindario para IPv6 (ND)
	RFC2462	Autoconfiguración de Direcciones "stateless" IPv6
	RFC2463	Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6)
	RFC1981	Descubrimiento del MTU de la ruta para IPv6
	RFC1809	Uso del campo "Etiqueta de Flujo" en IPv6
Direccionamiento	RFC2373	Arquitectura de Direccionamiento en IPv6
	RFC1887	Arquitectura para la Asignación de Direcciones Unicast IPv6
	RFC2374	Formato de Direcciones Unicast Agregables Globales
	RFC2450	Propuesta de normas de asignación de TLA y NLA
Routing	RFC2080	RIP para IPv6
	RFC2081	Aplicabilidad de RIPng para IPv6
	RFC2283	Extensiones Multiprotocolo para BGP-4
	RFC2545	Uso de las Extensiones Multiprotocolo de BGP-4 para Routing entre dominios para IPv6
	RFC2740	OSPF para IPv6
DNS	RFC1886	Extensiones DNS para soportar IPv6
IPv6 sobre ...	RFC2464	Transmisión de paquetes IPv6 sobre redes Ethernet
	RFC2467	Transmisión de paquetes IPv6 sobre redes FDDI
	RFC2470	Transmisión de paquetes IPv6 sobre redes Token Ring
	RFC2472	IPv6 sobre PPP
	RFC2491	IPv6 sobre redes de Acceso Múltiple Sin Broadcast

	RFC2492	IPv6 sobre redes ATM
Seguridad	RFC2401	Arquitectura de Seguridad para IP
	RFC2402	Cabecera de Autenticación IP
	RFC2406	Encriptación de datos en IP (ESP)
	RFC2408	Asociaciones de Seguridad y Protocolo de Gestión de Claves en Internet (ISAKMP)
Multicast	RFC2375	Asignación de Direcciones Multicast
	RFC2710	Descubrimiento de nodos que desean recibir Multicast para IPv6
	RFC2776	Protocolo de Anunciación de Zonas de Ambito Multicast (MZAP)
Anycast	RFC2526	Direcciones de Subredes para Anycast en IPv6
Multi-Homing	RFC2260	Soporte Escalable de Multi-homing para Conectividad Multi-Proveedor
	RFC2497	Transmisión de paquetes IPv6 sobre redes ARCnet
Transición	RFC1933	Mecanismos de Transición para Routers y Hosts IPv6
	RFC2185	Aspectos de Routing de la Transición IPv6
	RFC2473	Especificaciones Genéricas de Tunelización de Paquetes en IPv6
	RFC2529	Transmisión de IPv6 sobre Dominios IPv4 sin Túneles Explícitos
	RFC2765	Algoritmo de Traslación Stateless IP/ICMP (SIIT)
	RFC2766	Protocolo de Traslación - Traslación de Dirección de Red
	RFC2767	Doble Pila en Hosts usando la Técnica "Bump-In-the-Stack" (BIS)
API	RFC2292/bis	Advanced Sockets API para IPv6
	RFC2553/bis	Basic Socket API para IPv6
MIB	RFC2452	Base de Información de Gestión para IPv6: TCP
	RFC2454	Base de Información de Gestión para IPv6: UDP
	RFC2465	Base de Información de Gestión para IPv6: Convenciones Textuales y Grupo General
	RFC2466	Base de Información de Gestión para IPv6: ICMPv6

Otros	RFC1881	Gestión de la Asignación de Direcciones IPv6
	RFC1924	Representación Compacta de Direcciones IPv6
	RFC2147	TCP y UDP sobre Jumbogramas IPv6
	RFC2428	Extensiones FTP para IPv6 y NAT
	RFC2471	Plan de Asignación de direcciones IPv6 para Pruebas
	RFC2474	Definición del Campo de Servicios Diferenciados (DS) en Cabeceras IPv4 e IPv6
	RFC2546	Prácticas de Routing en 6Bone
	RFC2663	Consideraciones y Terminología de IP NAT
	RFC2732	Formato para la representación literal de direcciones IPv6 en URL's
	RFC2772	Guías de Routing en el troncal 6Bone
	RFC2775	Transparencia de Internet

Anexo 2. Configuración NAT Router cisco 801

```
Current configuration : 1048 bytes
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no new-model
!
!
ip cef
!
!
ipv6 unicast-routing
multilink bundle-name authenticated
!
!
archive
 log config
  hidekeys
!
!
!
interface FastEthernet0
!
interface FastEthernet1
!
interface FastEthernet2
 switchport access vlan 2
!
interface FastEthernet3
!
interface FastEthernet4
 no ip address
 speed 10
 half-duplex
 ipv6 address 2001:2::10/64
 ipv6 enable
 ipv6 nat
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
```

```
 ipv6 nat prefix 2010::/96
 ipv6 nat
!
interface Vlan2
 no ip address
 shutdown
!
interface Vlan3
 ip address 192.168.3.1 255.255.255.0
!
!
no ip http server
no ip http secure-server
!
!
ipv6 nat v4v6 source 192.168.1.200 2010::60
ipv6 nat v6v4 source 2001:2::1 192.168.1.2
!
!
control-plane
!
!
line con 0
 no modem enable
line aux 0
line vty 0 4
 login
!
scheduler max-task-time 5000

!
webvpn cef
end
```

Anexo 3. Configuración Router 1841 transmisor

```
Router#sh run
Building configuration...

Current configuration : 1100 bytes
!
! No configuration change since last restart
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
memory-size iomem 25
ip cef
!
!
!
!
!
ipv6 unicast-routing
!
!
!
!
!
!
!
!
!
!
interface Tunnel0
 no ip address
 ipv6 address 3001:1::2/64
 ipv6 enable
```

```
 ipv6 eigrp 1
 tunnel source Serial0/0/0
 tunnel destination 192.168.1.2
 tunnel mode ipv6ip
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 4001:1::2/64
 ipv6 enable
 ipv6 eigrp 1
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
ip address 192.168.1.1 255.255.255.0
no ip address
 shutdown
 no fair-queue
 clock rate 64000
!
interface Serial0/0/1
no ip address
 shutdown
 no fair-queue
 clock rate 64000
 !
router eigrp 1
 network 192.168.1.0
 auto-summary
!
!
!
ip http server
no ip http secure-server
!
!
!
ipv6 router eigrp 1
 no shutdown
!
```

```
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end

Router#
```

Anexo 4. Configuración router 1841 receptor

```
Router>enable
Router#sh run
Building configuration...

Current configuration : 1133 bytes
!
! No configuration change since last restart
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip cef
!
!
!
!
!
ipv6 unicast-routing
!
!
!
!
!
!
!
!
!
!
!
interface Tunnel0
 no ip address
 ipv6 address 3001:1::3/64
```

```
 ipv6 enable
 ipv6 eigrp 1
 tunnel source Serial0/0/0
 tunnel destination 192.168.1.1
 tunnel mode ipv6ip
!
interface Tunnel1
 no ip address
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:1::1/64
 ipv6 enable
 ipv6 eigrp 1
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
ip address 192.168.1.2
 clock rate 64000

!
interface Serial0/0/1
 no ip address
 shutdown
 no fair-queue
 clock rate 125000
!
router eigrp 1
 network 192.168.1.0
 auto-summary
!
!
!
ip http server
no ip http secure-server
!
!
!
ipv6 router eigrp 1
```

```
 no shutdown
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end

Router#
```