Universidad Nacional de La Matanza
Departamento de Ingeniería e Investigaciones Tecnológicas

Código: C145

Título del Proyecto: Implementación y Desarrollo de Aplicaciones Nativas para IPv6

Programa de Investigación: PROINCE

Director del Proyecto: Daniel Alberto Giulianelli (DAG)

Co-Director del Proyecto: Rocío Andrea Rodríguez (RAR)

Integrantes del Proyecto (en orden alfabético):

Docentes Investigadores:
Binker Carlos (CB), Blanco Gabriel Esteban (GEB), Caiafa Marcelo (CM), Cruzado Graciela Susana (GSC), Fernández Víctor Manuel (VMF), Marko Isabel Beatriz (IBM), Moreno Edgardo Javier (EJM), Trigueros Artemisa (AT), Vera Pablo Martín (PMV)

Alumnos en Formación:
Cammarano Pablo (PC), Cornejo María Antonella (MAC), Dogliotti Mariano Gastón (MGD), Valles Gabriela Yanina (GYV)

Fecha de inicio: 2013/01/01 - Fecha de finalización: 2014/12/31

Resumen: Este proyecto está asociado al programa “Conectividad IPv6”. En el marco de la presente propuesta se espera implementar aplicaciones ya existentes con soporte a IPv6, ofrecer asesoramiento sobre las diversas aplicaciones para las distintas necesidades, encontrar necesidades no solucionadas con las aplicaciones existentes y desarrollar una aplicación concreta que permita satisfacer una necesidad puntual que contribuya al ámbito de I+D (Investigación y Desarrollo). Se analizarán diversos frameworks para IPv6, eligiendo uno con el cual se realizará el desarrollo de una aplicación nativa. La cual será utilizada para fines académicos en el marco de la universidad y además será ofrecida gratuitamente para su uso en otras instituciones académicas. Este proyecto no sólo permitirá formar investigadores y alumnos en las características del protocolo sino trabajar a nivel de aplicación con él. El impacto será importante para el grupo de investigación y también para la universidad pudiendo hacer uso de IPv6 masivamente extendiendo el alcance actual de la conectividad.

Palabras claves: IPv6, Protocolo, Aplicaciones, Socket

Área de conocimiento: Ingeniería de Comunicaciones, Electrónica y Control
Código de Área de Conocimiento: 1800
Disciplina: Computación
Código de Disciplina: 1802
Campo de Aplicación: Computación
Código de Campo de Aplicación: 1802

Implementación y Desarrollo de Aplicaciones Nativas para IPv6

Resumen

Este proyecto está asociado al programa “Conectividad IPv6”. En el marco de la presente propuesta se espera implementar aplicaciones ya existentes con soporte a IPv6, ofrecer asesoramiento sobre las diversas aplicaciones para las distintas necesidades, encontrar necesidades no solucionadas con las aplicaciones existentes y desarrollar una aplicación concreta que permita satisfacer una necesidad puntual que contribuya al ámbito de I+D (Investigación y Desarrollo). Se analizarán diversos frameworks para IPv6, eligiendo uno con el cual se realizará el desarrollo de una aplicación nativa. La cual será utilizada para fines académicos en el marco de la universidad y además será ofrecida gratuitamente para su uso en otras instituciones académicas. Este proyecto no sólo permitirá formar investigadores y alumnos en las características del protocolo sino trabajar a nivel de aplicación con él. El impacto será importante para el grupo de investigación y también para la universidad pudiendo hacer uso de IPv6 masivamente extendiendo el alcance actual de la conectividad.

Palabras claves: IPv6, Protocolo, Aplicaciones, Socket

1. Estructura

En este apartado se presenta la estructura del presente informe la cual toma como base la propuesta en forma general de la guía de informes de avance/finales, realizando agregados (indicándose con una –A– después del título) o quitando aquellos títulos que no aplican en la presente temática (indicándose con una –NA– después del título).

1. Estructura **– A –**
2. Introducción
   - 2.1 Selección del Tema
   - 2.2 Definición del Problema
   - 2.3 Justificación del Estudio
   - Limitaciones **– NA –**
   - 2.4 Alcances del Trabajo
   - 2.5 Objetivos
   - 2.6 Hipótesis
3. Desarrollo:
   - Material y Métodos **– NA –**
   - 3.1. Lugar y Tiempo de la Investigación
   - Descripción del Objeto de Estudio **– NA –**
   - Descripción de Población y Muestra **– NA –**
   - 3.2. Diseño de la Investigación
   - Instrumentos de Recolección y Medición de Datos **– NA –**
   - Confiabilidad y Validez de la Medición **– NA –**
   - Métodos de Análisis Estadísticos **– NA –**
   - 3.3. Etapas Ejecutadas **– A–**
     - 3.3.1 ETAPA 1: Relevamiento **–A–**
       - 3.3.1.1 Tarea 1: Estado del Arte **–A–**
       - 3.3.1.2 Tareas 2 y 3: Aplicaciones Existentes Clasificadas según su uso **–A–**
       - 3.3.1.3 Tarea 4: Seleccionar de Aplicaciones de Utilidad para el Laboratorio de I+D **–A –**
     - 3.3.2 ETAPA 2: Conectividad IPv6 **–A –**
       - 3.3.2.1 Tarea 5: Crear LAN IPv6 **–A–**
       - 3.3.2.2 Tarea 6: Conectividad a Internet mediante IPv6 **–A–**
       - 3.3.2.3 Tarea 7: Configuración de Equipos **–A–**
       - 3.3.2.4 Tarea 8: Pruebas de Conectividad **–A–**

[1] La tarea 9 corresponde a la elaboración y entrega del informe de avance por ello no se consigna en esta estructuración para el presente informe final

2. Introducción

2.1. Selección del Tema

Si bien desde su creación se anuncio que IPv6 no reemplazaría a IPv4, todo parece indicar que esto pueda ocurrir para solucionar el problema del agotamiento de las direcciones IP. Algunas predicciones indicaban que antes del 2010 IPv4 debía estar sustituido previo al agotamiento de direcciones. En el 2007 la LACNIC mencionaba al "2011 como el año en el que se recomienda a todos los proveedores de Internet de la región a tener bloques de direcciones IPv6, ya en uso, para servicios de producción" [AZA07]. Sin embargo en la actualidad aún muchos usuarios y proveedores de servicios trabajan bajo IPv4, otros están implementando mecanismos de transición: Doble Pila, Entubamiento (Tunneling) ó Traducción de Encabezados. Para poder trabajar internamente con IPv4 y salir al exterior con una IPv6.

IANA es la autoridad encargada de distribuir los bloques de las direcciones IP a lo largo del mundo. Para conseguir este objetivo entrega bloques a 5 entidades (AFRINIC, ARIN, APNIC, LACNIC, RIPE) quienes a su vez las entregan a las entidades gubernamentales y a los proveedores de internet (ISP). IANA ya no posee bloques para distribuir esto conlleva a que las entidades agoten las que les quedaban aún disponibles. En la figura 1 se muestra entidades sin direcciones IP con una estimación proyectada.

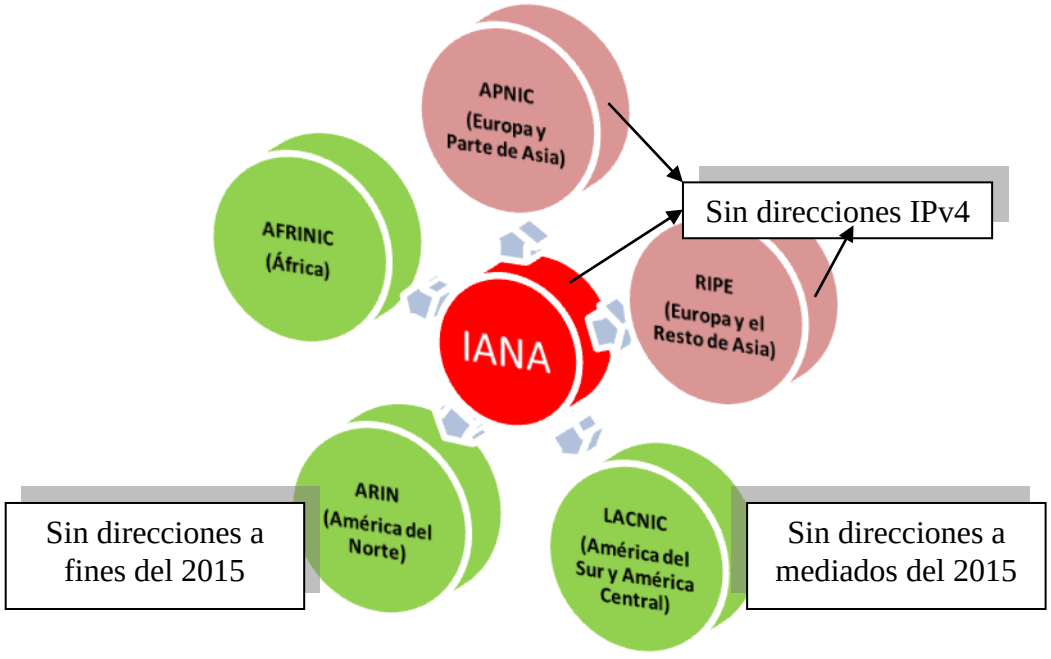


Figura 1. Agotamiento de las direcciones IPv4

El agotamiento de direcciones fue el motivo para construir un nuevo protocolo (con 128 bits). Esto permite una cantidad hipotética de direcciones de 2^{128} = 340 sextillones de direcciones IPv6.

IPv6 tiene principalmente las siguientes ventajas:

- Mayor cantidad de direcciones: Mientras IPv4 tenía 2^{32} direcciones IPv6 cuenta con 2^{128}. “Se estima que si se repartiesen en toda la superficie de la Tierra habría 6,67x1023 IPs por m²” [INN12].
- Flexibilidad: Formato de cabecera más flexible que en IPv4 para agilizar el encaminamiento.
- Extensibilidad: IPv6 ha sido diseñado para ser extensible y ofrece soporte optimizado para nuevas opciones y agregados, permitiendo introducir mejoras en el futuro.
- Identificación de Flujo de Paquetes: Nueva etiqueta de flujo para identificar paquetes de un mismo flujo.
- Fragmentación en nodos: La fragmentación se realiza en el nodo origen y el reensamblado se realiza en los nodos finales, y no en los routers como en IPv4.
- Movilidad: incluida en el estándar, que permitirá cambiar de red sin perder la conectividad. IPv6 incluye mecanismos de movilidad más eficientes y robustos lo cual beneficiará no sólo a los usuarios de telefonía y dispositivos móviles, sino también (por ejemplo) tener buenas conexiones a internet durante los vuelos de avión.
- Multicast: Además de Unicast, Anycast y Broadcast. IPv6 incorpora Multicast (posibilidad de envió a un grupo de receptores interesados).
- Auto-configuración de los nodos finales, que permite a un equipo aprender automáticamente una dirección IPv6 al conectarse a la red.
- Aplicaciones: IPv6 permite el uso de jumbogramas (paquetes de datos de mayor tamaño 64K). Para dar mejor soporte a tráfico en tiempo real (ej. videoconferencia), IPv6 incluye etiquetado de flujos en sus especificaciones. Con este mecanismo los encaminadores o routers pueden reconocer a qué flujo extremo a extremo pertenecen los paquetes que se transmiten.
- Plug and Play: IPv6 incluye en su estándar el mecanismo "plug and play", lo cual facilita a los usuarios la conexión de sus equipos a la red. La configuración se

realiza automáticamente. Esto permite que al conectar una máquina a una red IPv6, se le asigne automáticamente una (ó varias) direcciones IPv6.

- VOIP: Dos de los problemas actuales de los servicios de Voz sobre IP (VoIP) son QoS y NAT. Las comunicaciones pueden resultar en baja calidad de voz (QoS), y presentar dificultad para atravesar firewalls (NAT). Al incorporar IPv6 una gran cantidad de direcciones, no será necesario utilizar NAT, y sus nuevas capacidades de Plug and Play, seguridad, y QoS implicarán mejores conexiones de voz.

LACNIC (Latin American and Caribbean Internet Addresses Registry) indica que “la adopción temprana de IPv6 por la comunidad académica ha tenido como fin, por un lado la experimentación e investigación y por otro la formación de recursos humanos en el tema. A su vez, algunas necesidades propias de este sector se ven beneficiadas con características disponibles en este protocolo” [LACne]. Este organismo señala algunos ejemplos a nivel aplicación:

- La necesidad de contar con direcciones públicamente alcanzables, que permitan la interacción entre pares (en aplicaciones "peer to peer" como videoconferencia, operación remota de instrumentos, GRIDs, etc.).
- Características como multicast, necesario en aplicaciones como access grid y otras que requieren optimizar el uso del ancho de banda.
- Disponibilidad de IPSec como parte del stack, lo que facilita el despliegue de aplicaciones que requieren seguridad de extremo a extremo, como disponibilidad de recursos en malla (grids).
- Las nuevas posibilidades que brindan las características de QoS (Calidad de Servicio) incorporadas al protocolo.

2.2. Definición del Problema

El proyecto surge con vinculación con el programa “Conectividad IPv6” que iniciará en el 2013, mediante un interés concreto del DIIT (Departamento de Ingeniería e Investigaciones Tecnológicas) de UNLaM para que se pueda sacar provecho de la conectividad la cual actualmente se encuentra en un único laboratorio. Dentro del marco de este proyecto se construirá una LAN IPv6 en el laboratorio del GIDFIS (Grupo de Investigación, Desarrollo y Formación en Innovación de Software) pero además se realizará una conexión con el nodo que tiene conectividad IPv6 esta conexión permitirá no solo proveer internet por IPv6 a ese laboratorio sino a toda la

zona aledaña compuesta por otros laboratorios de I+D tanto de Ingeniería como de Ciencias Sociales (ver figura 2). Si bien no es el objetivo principal proveer conectividad a los laboratorios de I+D, este será un impacto favorable asociado al proyecto.

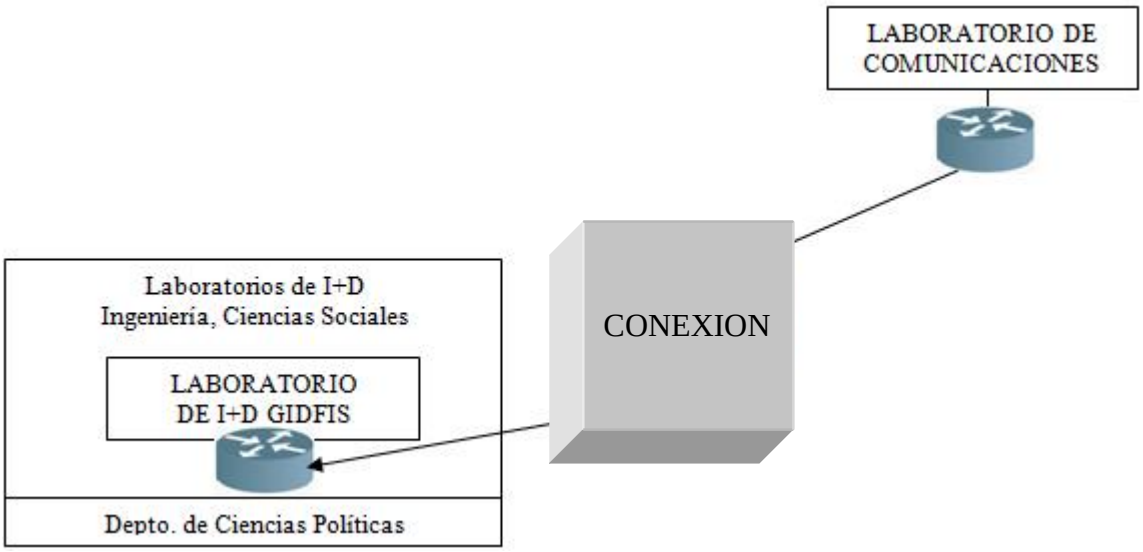


Figura 2. Conexión a IPv6 prevista

Además de la propuesta de solución en cuanto a hardware, en estos momentos la principal atención está puesta en cómo aprovechar este protocolo a nivel software. Por ello se plantea la necesidad de construir y ofrecer aplicaciones nativas para IPv6. Distintas aplicaciones con determinadas características se benefician con IPv6 (ver figura 3).

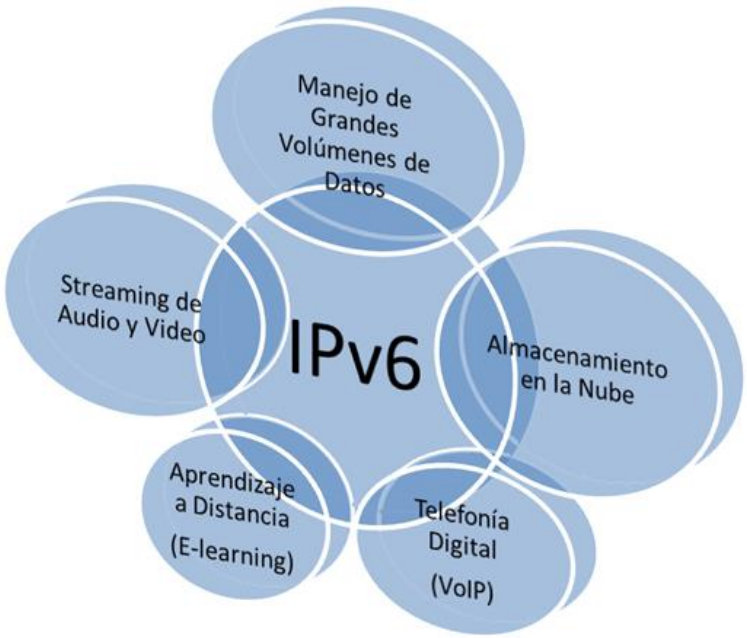


Figura 3. Aplicaciones que se pueden beneficiar con IPv6

El tener una conectividad a IPv6 permitirá poder probar servicios, construir aplicaciones nativa, etc.

2.3. Justificación del Estudio

Gradualmente IPv6 irá reemplazando la conectividad con el protocolo IPv4, la dificultad básica reside en poder actualizar todo el hardware que sólo puede funcionar con el protocolo anterior. Esta actualización lógicamente se va produciendo en forma paulatina (tomándose mayor tiempo que el planificado, lo que provoca que haya áreas en las que se han agotado las direcciones IPv4 asignadas [AZA07]). Cuando efectivamente IPv6 sea el protocolo de uso tradicional, surgirá un siguiente interrogante que es cómo desde las aplicaciones se pueden aprovechar las ventajas que este protocolo ofrece.

La importancia del proyecto reside en el conocimiento que se profundizará sobre IPv6 con un alto interés en la transferencia del mismo tanto en el área docente como con otros equipos externos de investigación. En particular para la UNLaM, será posible a través del presente proyecto sentar bases de aplicaciones gratuitas para ser utilizadas en IPv6, desarrollo de nuevas aplicaciones y por supuesto como punto importante que el laboratorio de I+D asignado al grupo de trabajo GIDFIS cuente con una LAN IPv6 y pueda tomar la conectividad que actualmente se cuenta en un nodo lejano al mismo para conectarse con el exterior. Se espera poder transferir el conocimiento tanto internamente a docentes y alumnos; como a pares fuera del ámbito de la UNLaM.

2.4. Objetivos

- Formar un grupo especializado sobre IPv6 a nivel de aplicaciones que pueda asesorar al resto de los pares en esta área.
- Analizar frameworks para desarrollo nativo en IPV6.
- Desarrollar una aplicación nativa para IPv6 para el ámbito académico.

2.5. Alcances del Trabajo

En este proyecto se atienden principalmente tres cuestiones: (1) revisión del estado del arte, análisis de software existente; (2) instalación y configuración de equipamiento; (3) desarrollo nativo. Para lo cual el tiempo del proyecto ha sido dividido en 5 etapas con tareas asociadas, las cuales fueron planteadas en el protocolo inicial del proyecto. Se ha respetado dicho cronograma (el cual se vuelca nuevamente en el ítem 3.1).

2.6. Hipótesis

Muchas aplicaciones proveen soporte a IPv6, aunque no fueron realizadas nativamente para este protocolo. Existen diversas áreas en las cuales no se cuentan con aplicaciones que aprovechen las ventajas de IPv6, que, sin duda sería de gran utilidad para determinados dominios.

3. Desarrollo

3.1. Lugar y Tiempo de la Investigación

Las tareas se realizan dentro del laboratorio designado para este proyecto. El DIIT cuenta con un laboratorio de investigación en el cual se encuentra el grupo GIDFIS (Grupo de Investigación Desarrollo y Formación en Innovación de Software).

Los tiempos de las tareas se llevaron a cabo en base al GANTT (ver tabla 1 y 2) diseñado previamente en el momento de la presentación del protocolo del presente proyecto. La tabla 1 se corresponde con el primer año de la investigación, hasta la actividad 9 inclusive. En la tabla 2 están contenidas las actividades del segundo año, actividades numeradas desde 10 a 16. Todas las actividades serán desarrolladas sintéticamente a modo de resumen en el presente informe final.

Tabla 1. Gantt de Tareas Previstas para el Primer Año - 2013

Actividades 1er Año	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
ETAPA 1 – Relevamiento	**X**	**X**	**X**	**X**	**X**	**X**						
1- Estado del Arte a) Síntesis de Material generalidades de IPv6 b) Síntesis publicaciones científicas en el área c) Resumen de investigación académicas de otras universidades	X	X	X	X								
2- Aplicaciones Existentes a) Listado de aplicaciones que cuentan con soporte IPv6 b) Clasificación de las aplicaciones por sus usos				X	X							
3- Clasificación de las Aplicaciones por sus Usos				X	X							
4- Seleccionar las aplicaciones que son de utilidad para el entorno del laboratorio de I+D					X	X						
ETAPA 2- Conectividad IPv6							**X**	**X**	**X**	**X**	**X**	**X**
5- Crear una LAN IPv6 dentro del laboratorio de Investigación (para tener conectividad en forma local)							X					
6- Extender el alcance de IPv6 para tener conexión en el laboratorio de I+D a) Analizar las distancias desde el actual punto de conectividad de UNLaM para instalar hardware que permita proporcionar conectividad al laboratorio de I+D b) Instalar un router con alcance suficiente para conectar ambos puntos								X	X	X		
7- Configuración de Equipos del Laboratorio											X	
8- Pruebas de Conectividad y Alcance de la señal												X
9- Informe de Avance												**X**

Tabla 2. Gantt de Tareas Previstas para el Segundo Año - 2014

Actividades 2do Año	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
ETAPA 3 - Instalación	**X**	**X**										
10- Instalación aplicaciones seleccionadas en la etapa 1 (tarea 4) a) Instalación b) Prueba de aplicaciones en el laboratorio I+D c) Prueba de las aplicaciones entre nodos con conectividad en UNLaM	X	X										
ETAPA 4 - Planificación de Aplicaciones		**X**	**X**	**X**	**X**							
11- Detectar los dominios en donde no se cuenta con la existencia de aplicaciones para IPv6 a) Enunciar Posibles Aplicaciones b) Seleccionar una aplicación candidata c) Modelar la aplicación		X	X	X								
12- Selección de un framework de programación para aplicaciones IPv6 a) Listado de Frameworks posibles b) Evaluación de Características c) Generación de un cuadro comparativo				X	X							
ETAPA 5 – Desarrollo de una Aplicación					**X**	**X**	**X**	**X**	**X**	**X**	**X**	
13- Justificación de las ventajas de IPv6 que aprovecha la aplicación					X							
14- Manejo del Framework a) Instalación b) Aprendizaje del manejo del Framework c) Generación de un instructivo básico d) Capacitación al resto del equipo					X	X						
15- Desarrollo de la aplicación a) Programación b) Instalación c) Pruebas d) Creación del Manual de Uso e) Publicación y Difusión para el uso Gratuito de la Aplicación							X	X	X	X	X	
16- INFORME FINAL DEL PROYECTO												**X**

3.2. Diseño de la Investigación

Como puede verse en el GANTT presentado en el apartado anterior las tareas del proyecto se encuentran divididas por Etapas. En la figura 4 se muestran las 5 etapas a realizar a lo largo del proyecto, las etapas 1 y 2 se corresponden con el primer año del proyecto (las cuales se presentaron en la tabla 1), las siguientes etapas corresponden al segundo año del proyecto (no realizadas durante este primer año).

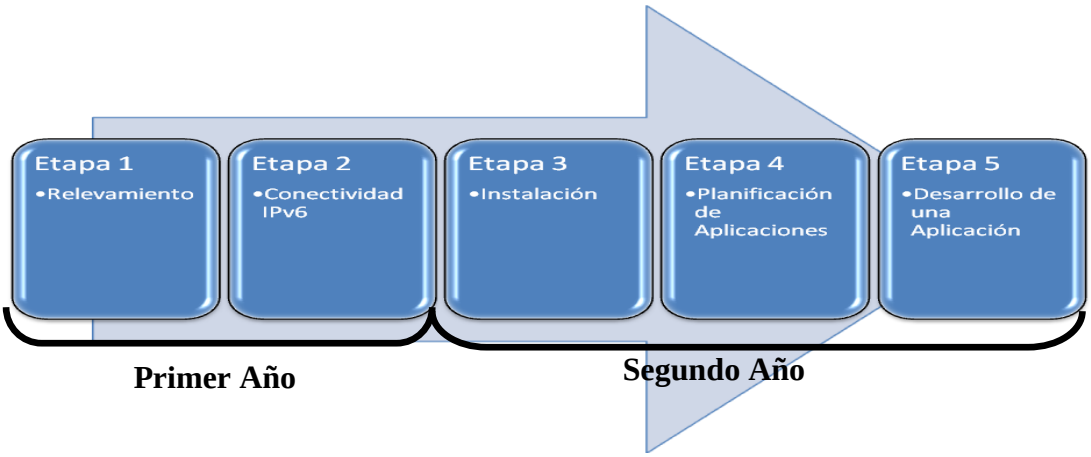


Figura 4. Etapas previstas

A continuación se detalla lo realizado en cada una de las etapas.

3.3. ETAPAS

3.3.1. ETAPA 1 - Relevamiento

En esta etapa las tareas involucradas son las que se muestran en la figura 5.

Figura 5. Conexión a IPv6 prevista

3.3.1.1. Tarea 1 - Estado del Arte

Esta primera tarea implicó una revisión de material bibliográfico sobre Generalidades de IPv6, en donde fue posible profundizar en las características más relevantes del protocolo (obtenido este resultado mediante la lectura de diversas publicaciones científicas en el área). También se presentará a continuación una síntesis de los trabajos que diversas universidades están realizando sobre IPv6.

Características de IPv6

Primeramente se efectuaron informes que permitieron sintetizar las características más importantes de IPv6: Multicast, Calidad de Servicio y Movilidad.

1. **Multicast:**

   Se basa en el concepto de grupo. Un grupo arbitrario de receptores que esperan recibir un particular flujo de datos. Dichos grupos no tienen sentido físico de ubicación, pueden encontrarse en cualquier parte de Internet.

   En la comunicación multicast existe una fuente y un grupo de destinos (ver figura 6), por lo tanto, es una relación de uno a muchos. En este tipo de comunicación, la dirección de origen es una dirección unicast, pero la dirección de destino es la dirección de un grupo, formado por uno o más receptores.

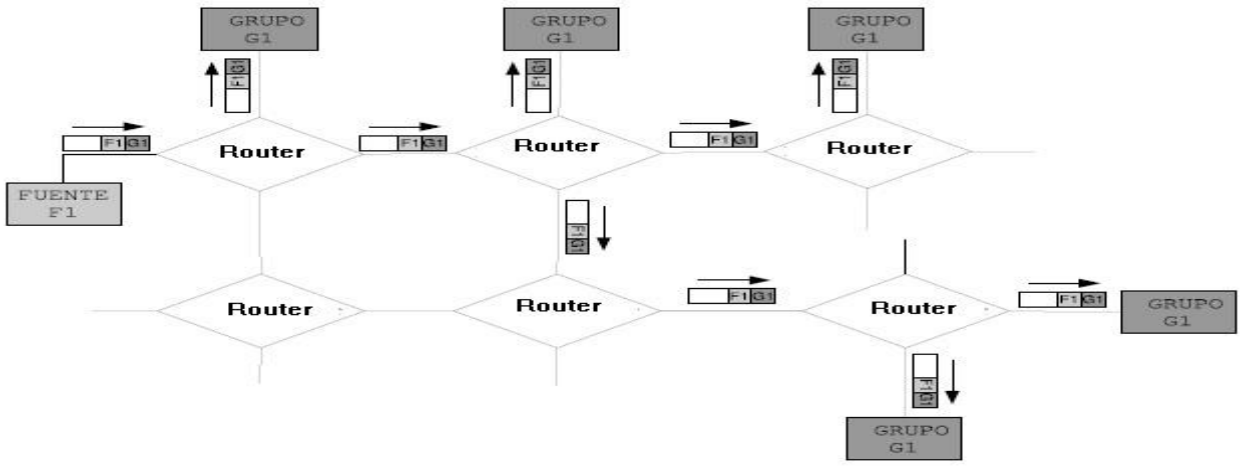


Figura 6. Comunicación Multicast

En la figura anterior se puede observar que la estructura de los paquetes es la misma: la dirección de origen es F1 (dirección del emisor) y la de destino es G1 (dirección del grupo).

Características generales:

- Se realiza un único envío desde el origen, independientemente del número de destinos. Cada router se encarga de realizar las copias, si fuera necesario.
- Menor consumo de recursos, ya que cada enlace solo transporta una copia del paquete.
- A diferencia de la unidifusión múltiple2, en multicast no hay retardo entre los paquetes ya que no se transmiten copias desde el emisor. Esto es una ventaja en ciertas aplicaciones de tiempo real.
- Las direcciones multicast solo puede aparecer como dirección IP de destino.
- Los sistemas finales pueden ser origen y/o destino de los paquetes IP de multidifusión.
- Los routers que manejan tráfico multicast son los routers de multidifusión de Internet: estos manejan las direcciones multicast y además se encargan de realizar la copia de la información cuando sea necesario. Usan algoritmos de enrutamiento dinámico de multidifusión.

Direcciones IPv6 Multicast

La figura 7 muestra el formato de una dirección Multicast.

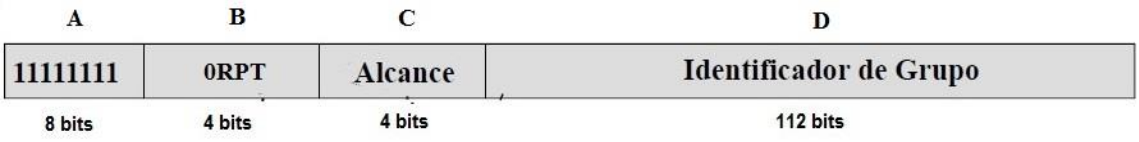


Figura 7. Formato de una dirección Multicast

A) Los primeros 8 bits de una dirección multicast siempre son “1” (11111111), que en hexadecimal sería FF. Sirve para diferenciarlas de las demás direcciones.

[2] La unidifusión múltiple es un método de comunicación en el cual el emisor envía N paquetes a N destinos. Presenta desventajas frente a la multidifusión, principalmente por el retardo que se genera en el origen al copiar los paquetes.

B) Banderas RPT:

Cada uno de estos *flags* tiene un significado. A continuación se detallan:

R = 1 (la dirección multicast incorpora la dirección de un Punto de Reunión)

P = 1 (la dirección multicast está basada en un prefijo unicast)

T = 0 es una dirección asignada permanentemente por la IANA/ICANN[3] (no es transitoria)

T = 1 no es una dirección asignada permanentemente (es transitoria)

C) Alcance del grupo de multidifusión (también llamado ámbito o límite):

Está representado por un número entero de 4 bits.

0 (0000): reservado.

1 (0001): alcance de nodo local.

2 (0010): alcance de enlace local.

5 (0101): alcance de sitio local (varios enlaces).

8 (1000): alcance de organización local (compuestas de varios centros o sitios).

E (1110): alcance global (en Internet).

F (1111): reservada.

D) El **identificador de grupo** permite identificar al grupo multicast al que nos referimos dentro de un determinado ámbito.

Los identificadores de grupo permanentemente asignados son independientes del ámbito. Los identificadores de los grupos temporales, en cambio, solo son relevantes para un ámbito determinado.

Direcciones Multicast reservadas

Tabla 3. Direcciones Reservadas en alcance nodo-local

Dirección IPv6	Descripción
FF01::1	Dirección de multidifusión a todos los nodos
FF01::2	Dirección de multidifusión a todos los routers

[3] La ICANN (Internet Corporation for Assigned Names and Numbers) es una organización mundial que se encarga de la asignación de direcciones IP, identificadores de protocolos, entre otras tareas.
La IANA (Internet Assigned Numbers Authority) es actualmente un departamento de la ICANN.

Tabla 4. Direcciones Reservadas en alcance enlace-local

Dirección IPv6	Descripción
FF02::1	Dirección de multidifusión a todos los nodos
FF02::2	Dirección de multidifusión a todos los routers
FF02::4	Todos los routers DVMRP[4]
FF02::5	Todos los routers OSPFIGP[5]
FF02::6	Todos los routers designados OSPFIGP
FF02::9	Todos los routers RIP[6]
FF02::D	Todos los routers PIM[7].
FF02::1:FFXX:XXXX	Solicited-Node Adress. Permite calcular la dirección multicast a partir de la unicast o anycast de un determinado nodo. Se sustituyen los 24 bits de menor peso (“X”) por los mismos bits de la dirección original.

Correspondencia IP-MAC en Multicast

Existe una correspondencia entre las direcciones IP y las MAC en unidifusión, difusión y multidifusión.

En el caso de la multidifusión, la dirección MAC se obtiene a partir de la dirección del grupo. Las tramas de multidifusión tienen que poder ser transmitidas o recibidas por la capa de enlace de datos. El prefijo de las tramas Ethernet de multidifusión en IPv6 es 33-33.

Las tarjetas de red “captan” todas las tramas que comiencen con 33-33 y se pasan al nivel de IP. Las tarjetas más actuales pueden analizar los octetos restantes para saber si pertenece a dicho grupo de multidifusión, y de esa manera evitar enviar información innecesaria al nivel IP.

Cuando un usuario se agrega a un grupo de multicast, se le informa a la tarjeta de red que filtre las tramas multicast de ese grupo.

[4] Protocolo de enrutamiento multicast basado en vector distancia, se desarrolla más adelante.
[5] Protocolo de enrutamiento basado en estado del enlace.
[6] Protocolo de Información de Enrutamiento basado en vector distancia, presenta ciertas limitaciones.
[7] Es una familia de protocolos de enrutamiento multicast, se desarrolla más adelante.

Existen dos casos en los que hay que realizar una conversión de la IP a la MAC:

A. Multidifusión a todos los nodos de la red

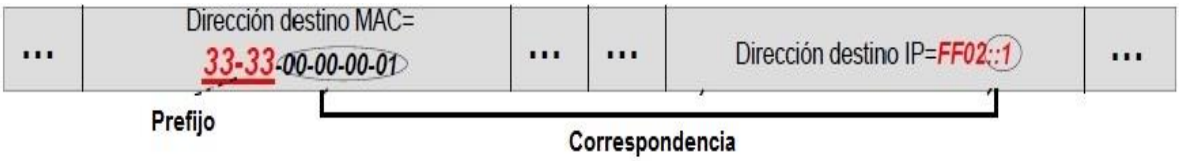


Figura 8. Equivalente a la difusión limitada en IPv4

En este caso, el objetivo es difundir un mensaje a todos los dispositivos de una red. Por lo tanto, se utiliza la dirección IP de multidifusión a todos los nodos vecinos (FF02::1).

Al realizar la correspondencia entre dicha dirección IPv6 y la MAC, se utiliza el prefijo 33-33 seguido de “00-00-00-01”, esto último está relacionado con el “1” de la dirección IPv6.

B. Multidifusión a un grupo específico

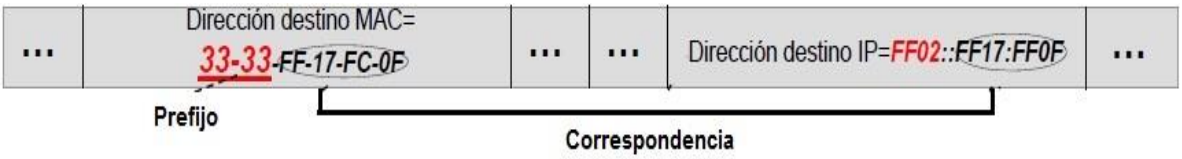


Figura 9. Ejemplo IPv6 – Multidifisión a un grupo específico

En este ejemplo, la dirección IPv6 del grupo multicast es: FF02::FF17:FF0F.

Para construir la dirección MAC, se toma el “FF-17-FC-0F” de la dirección IPv6, que representa al grupo multicast.

Protocolo MLD

El protocolo que administra los grupos multicast en una red se llama MLD (Multicast Listener Discovery Protocol). La versión actual es la MLDv2.

No es un protocolo de enrutamiento dinámico, sino que se encarga de administrar la pertenencia de “procesos activos” a grupos de multidifusión.

Los hosts usan este protocolo para indicarle a un router de multidifusión local (RML) que posee un proceso activo en un grupo de multidifusión de Internet.

Los RML mantienen, usando el protocolo MLD, una lista con los grupos que tienen al menos un proceso activo en la red.

El protocolo MLD está compuesto por 3 mensajes ICMPv6[8]

- **Multicast Listener Query (ICMPv6 Type 130):** es el mensaje de sondeo de pertenencia o consulta. Es enviado periódicamente por los routers. Hay dos tipos:
  - General Query: el campo de dirección multicast tiene valor “0”. De esa forma el router pregunta qué grupos multicast tienen participantes en la red local.
  - Group Specific: el campo de dirección multicast tiene una dirección específica. De esta forma el router pregunta si un grupo específico tiene participantes en la red.

- **Multicast Listener Report (ICMPv6 Type 131):** es el mensaje de informe de pertenencia al grupo. Un equipo deberá responder a cualquier consulta del RML con un mensaje de informe por cada grupo al que pertenece o desea pertenecer.

- **Multicast Listener Done (ICMPv6 Type 132):** es el mensaje de informe de abandono de grupo.

Cuando un equipo observa que ningún proceso local está activo envía un informe de abandono a dicho grupo. El RML, al recibirlo, envía un mensaje de consulta especial que incluye la dirección de dicho grupo multicast y espera 10 segundos a que otro equipo le responda. En caso que ningún equipo responda con el informe de pertenecía, asume que el grupo está vacío y lo elimina de la lista.

[8] Es el Protocolo de Mensajes de Control de Internet Versión 6.

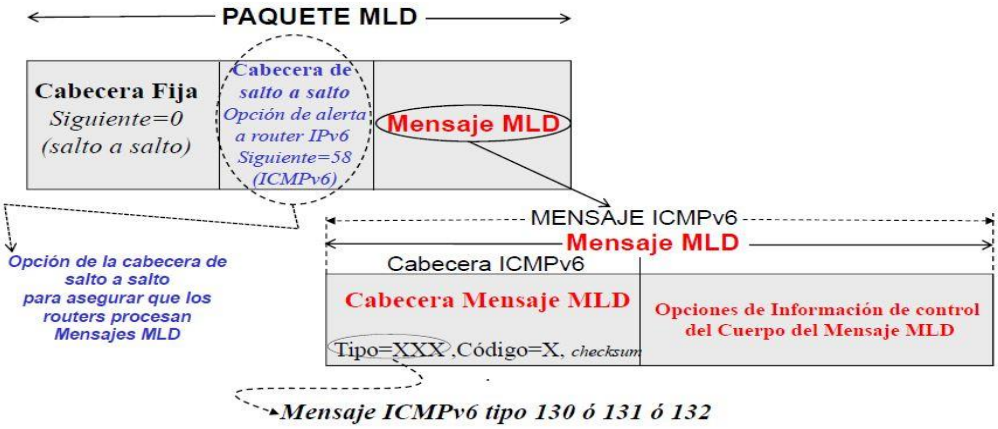


Figura 10. Ejemplo IPv6 – Multidifisión a un grupo específico

Enrutamiento Multicast:

El enrutamiento es un proceso por el cual se determina la ruta que van a tomar los paquetes para llegar a su destino. En el caso del tráfico multicast, existen ciertas funciones que se requieren para llevar a cabo el enrutamiento:

a) Establecer una convención para identificar direcciones multicast: las direcciones IPv6 utilizan un prefijo de 8 bits con valor “1”.

b) Cada router debe traducir una dirección multicast IPv6 a una lista de redes que contengan miembros del grupo multicast. Esta información permite construir un árbol de distribución de camino más corto (SPT) para llegar hacia todas las redes que tengan miembros del grupo.

c) El router debe poder traducir una dirección IP multicast a una dirección MAC para poder entregar en la red de destino el datagrama multicast.

d) Las direcciones multicast pueden ser estáticas, pero generalmente son dinámicas y los hosts se pueden unir o abandonar grupos multicast dinámicamente.

- Por eso se necesita un mecanismo que permita informar la incorporación o el abandono de un miembro al grupo.
- Los routers deben intercambiar dos tipos de información:
  - Qué redes contienen miembros de un grupo en particular.
  - Información para calcular los caminos más cortos a cada red que contenga miembros del grupo.

e) Se necesita un algoritmo de enrutamiento para calcular los caminos más cortos a todos los miembros del grupo.

f) Cada router debe determinar la ruta de distribución multicast basándose en las direcciones destino y fuente.

En el enrutamiento multicast, un paquete recibido por un router puede ser reenviado a distintos destinos de distintas redes.

Para reenviar un paquete multicast se requiere de un árbol SPT.

Existen dos enfoques para construir dicho árbol:

- **Árbol source-based:** cada router tiene un SPT por cada grupo multicast que existe. Este SPT define el próximo salto para cada red que tenga miembros registrados para ese grupo.

- **Árbol group-shared:** en este caso, solo un router designado, llamado Rendevouz Point (RP) se encarga de la distribución del tráfico multicast. Cuando un router recibe un paquete multicast, lo encapsula en uno unicast y lo envía al RP, que luego consulta su tabla de enrutamiento para dirigir el paquete. En este enfoque, solo el RP, que tiene un SPT por cada grupo, está involucrado en la transmisión multicast.

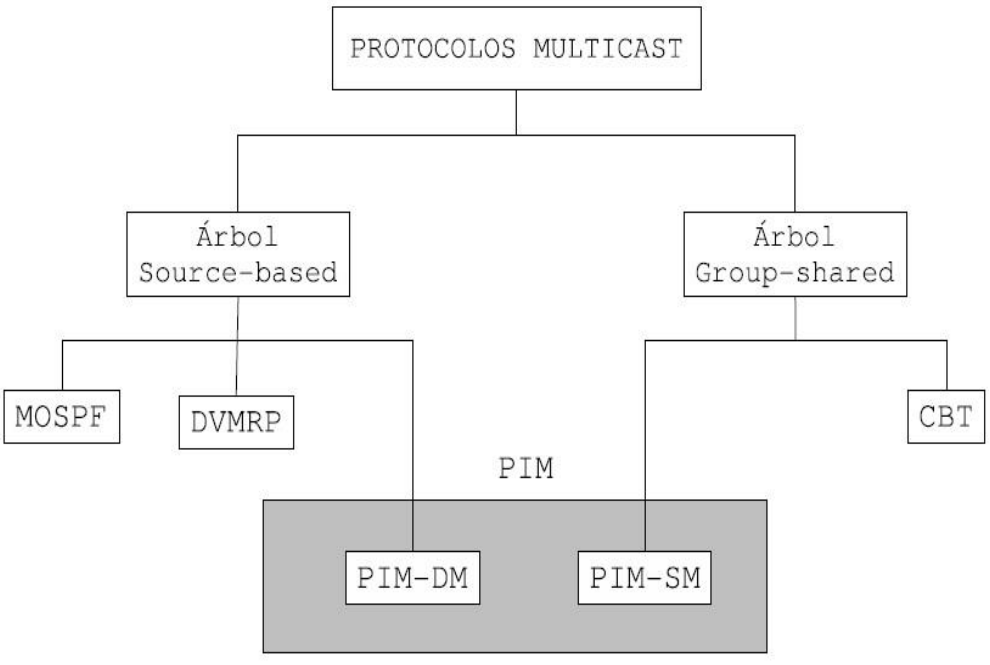


Figura 11. Modelo de Protocolo de Enrutamiento Multicast

Protocol Independent Multicast (PIM)

Es una familia de protocolos que se desarrolló a fines de la década de los 90. Se caracterizan por no depender de ningún protocolo de enrutamiento específico, sino que aprovechan las tablas de enrutamiento existentes para reenviar los datos multicast.

PIM Dense Mode (PIM-DM)

Este protocolo se recomienda cuando hay probabilidades que todos los routers participen en la distribución multicast y también para entornos multicast numerosos (por ejemplo, redes LAN).

Este protocolo implementa el enfoque de árbol source-based, es decir, que cada router tiene una tabla con la interfaz de salida que tiene el camino más óptimo a cierto destino.

PIM-DM utiliza un mecanismo push (empuje), es decir, empujar los datos multicast hacia los receptores.

El router que implemente este protocolo envía tráfico multicast por todas sus interfaces. Si los routers downstream[9] no tienen conectados ningún receptor del tráfico multicast, envía un mensaje stop hacia el router upstream[10]. Estos mensajes se conocen como prune (poda) porque el router upstream podará su árbol de reenvío para eliminar esa rama en particular. El tráfico multicast es enviado hasta que un router downstream lo rechace.

PIM Sparse Mode (PIM-SM)

Este protocolo se recomienda cuando existe alguna posibilidad que el router participe en la distribución multicast y es apropiado para entornos multicast dispersos, tales como redes WAN.
Implementa el enfoque de árbol group-shared, es decir que tiene un RP como fuente del árbol. En caso que exista un área numerosa de actividad

[9] Son los routers que se encuentran conectados por "debajo" del router que envía el tráfico, son los que lo reciben.
[10] Es el router que se encuentra por "arriba", el que envía los datos.

lejos del RP, ésta puede ser administrada más eficientemente con una estrategia de árbol source-based.

PIM-SM utiliza una estrategia pull (solicitud), contrastando con la técnica push de PIM-DM.

Esto significa que los routers deben hacer una solicitud específica de tráfico multicast antes de que los datos sean reenviados a ellos.

Este protocolo se adapta a Internet, ya que reduce la sobrecarga y el ancho de banda utilizado para el tráfico multicast.

Los routers generan periódicamente un mensaje hello para descubrir y mantener sesiones de estado con los vecinos. El router downstream puede enviar un mensaje join al upstream para unirse a un grupo multicast, indicando el grupo y la fuente a los que el router desea unirse. A partir de ese momento el router downstream empieza a recibir el tráfico multicast.
Esto demuestra la gran diferencia que tiene con PIM-DM, donde el router upstream siempre está enviando tráfico multicast hasta que el downstream le indique que deje de hacerlo.

Distance Vector Multicast Routing Protocol (DVMRP)

Es el más antiguo de los protocolos para enrutamiento multicast. Es análogo a RIP, es decir, que es un protocolo por vector distancia que proporciona una limitada flexibilidad y funcionalidad.

Es adecuado para redes pequeñas (no para Internet) debido a sus problemas de escalabilidad.

El funcionamiento es muy similar al del protocolo PIM-DM, ya que ambos son protocolos del tipo denso. La principal diferencia es que DVMRP genera sus propias tablas de enrutamiento basándose en el vector distancia, mientras que PIM-DM aprovecha las tablas existentes en el router.

Multicast Open Shortest Path First (MOSPF)

Es una extensión del protocolo OSPF, por lo tanto requiere su utilización para poder funcionar. Esto hace que su aplicación esté limitada a

universidades, empresas u organizaciones, donde se pueda implementar el protocolo OSPF en su totalidad. Es un protocolo basado en el estado de enlace. Esto significa que cada router realiza una serie de pruebas sobre sus enlaces para poder determinar el "costo" de cada uno de ellos. La principal diferencia con los basados en vector distancia (como DVMRP), es la velocidad de convergencia, que es mayor con MOSPF. Esto quiere decir que tarda menos en realizar una actualización del "mapa" de la red.

Core-Based Trees (CBT)

Cada grupo de multicast en la red posee un único árbol, con centro en un nodo llamado core o nodo central.

Todos los mensajes a un grupo en particular son enviados como mensajes unicast hacia el core hasta que alcanzan un router que pertenezca al árbol de destino.

Cuando un nodo del árbol de destino recibe el paquete, lo envía hacia todos sus enlaces, excepto por el que vino.

Implementación de Multicast

Las ventajas de implementar Multicast:

- Existe un considerable ahorro de ancho de banda de la red y, por lo tanto, de la utilización de la red en recursos económicos. Este ahorro se obtiene principalmente porque un mensaje multicast transmitido a N receptores no se envía N veces, sino que se realiza un solo envío y cada router realiza las copias que fueran necesarias. Además, en cada enlace solo se transmite una copia del paquete, reduciendo la carga de la red.
- Otro beneficio es que los receptores reciben los paquetes al mismo tiempo (sin tener en cuenta los retardos o los factores externos). Esto es muy útil para las aplicaciones time-sensitive[11], como por ejemplo los grids[12].

[11] Son aplicaciones en tiempo real, donde es importante que no existan retrasos en la comunicación.
[12] Son sistemas que permiten compartir recursos que se encuentran distribuidos por todo el mundo.

- Las aplicaciones de gran escala y con gran cantidad de receptores, como la transmisión de video por Internet, son técnica y económicamente viables utilizando multicast.
- La seguridad en las transmisiones multicast suele ser muy compleja. Sin embargo, como IPv6 implementa en forma nativa IPSEC, no tendría que haber problemas.

Las desventajas encontradas son:

- Al utilizar el mecanismo de transporte UDP, no se garantiza la entrega de paquete y el orden en que son recibidos.
- Requiere el soporte y la cooperación entre los routers para poder funcionar correctamente.

Aplicaciones Multicast

A continuar se listan las aplicaciones que justifican el uso de multicast:

- Acceso a bases de datos distribuidas
- Distribución de software y de información
- Servicios de tiempo
- Servicios de resolución de nombre, como DNS
- Replicación de base de datos
- Video y audio streaming
- Computación distribuida
- Educación a distancia
- Videoconferencias
- Video bajo demanda

2. Calidad de Servicio

La calidad del servicio (QoS) se define como la capacidad de una red para proporcionar diversos niveles de servicio a los diferentes tipos de tráfico.

“Al contar con QoS es posible asegurar una correcta entrega de la información, dando preferencia a aplicaciones de desempeño crítico, donde

se comparten simultáneamente los recursos de red con otras aplicaciones no críticas. QoS hace la diferencia al proveer un uso eficiente de los recursos en caso de presentarse congestión en la red, seleccionando un tráfico específico de ésta, priorizándolo según su importancia relativa, y utilizando métodos de control y evasión de la congestión para darles un tratamiento preferencial. Implementando QoS en una red, se logra un rendimiento de ésta más predecible y una utilización de ancho de banda más eficiente". [SAL11]

Decimos que una red o un proveedor ofrece "Calidad de Servicio" o QoS cuando garantiza un valor límite (máximo o mínimo) de alguno de los parámetros de QoS.

Niveles de QoS [13]

Existen tres niveles de servicio: mejor esfuerzo, servicio diferenciado y servicio garantizado/integrados.

a) **Mejor esfuerzo o best-effort:** Es cuando la red hace todo lo posible para entregar el paquete a su destino, pero no hay garantía de que esto ocurra. Este es el modelo utilizado por las aplicaciones de FTP y HTTP.

b) **Servicios integrados:** El modelo de Servicios Integrados provee a las aplicaciones de un nivel garantizado de servicio, negociando parámetros de red de extremo a extremo. La aplicación solicita el nivel de servicio necesario con el fin de operar apropiadamente y se basa en la QoS para que se reserven los recursos de red necesarios antes de que la aplicación comience a operar.

c) **Servicios diferenciados:** Este incluye un conjunto de herramientas de clasificación y de mecanismos de cola que proveen a ciertas aplicaciones o protocolos con determinadas prioridades sobre el resto del tráfico en la red.

[13] Este apartado está basado en [SAL11] y [3Cu13].

Congestión y Calidad de Servicio

Con ancho de banda suficiente se resuelven “casi” todos los problemas. Sería muy fácil dar Calidad de Servicio (QoS) si las redes nunca se congestionaran. Para ello habría que sobredimensionar todos los enlaces, cosa no siempre posible o conveniente. Para dar QoS con congestión es preciso tener mecanismos que permitan dar un trato distinto al tráfico preferente y cumplir el SLA (Service Level Agreement). La figura 12 plantea los efectos de la congestión en el tiempo de servicio y rendimiento y ha sido extraida de [3Cu13].

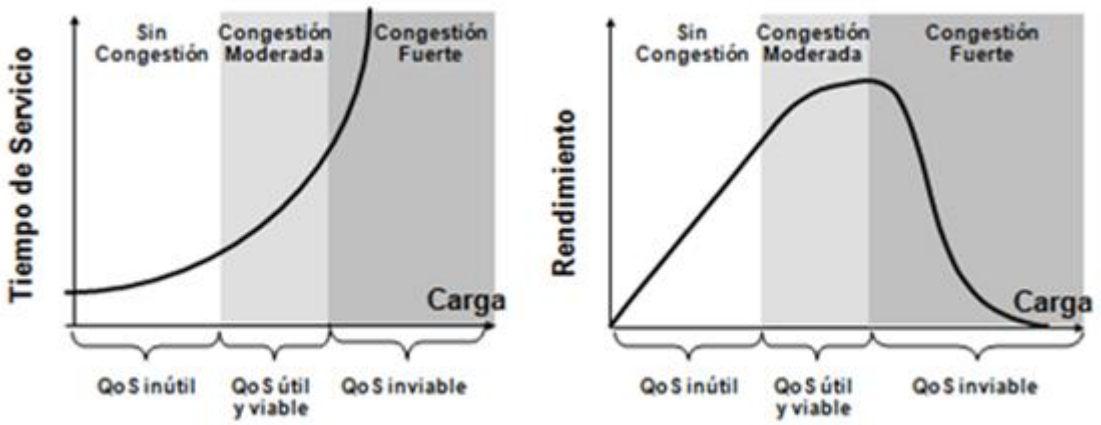


Figura 12. Efectos de la congestión en el tiempo de servicio y rendimiento

Es bien sabido que incluso desde una perspectiva de optimizar el uso global de los recursos no es deseable una excesiva carga en los enlaces. Cuando la carga aumenta el tiempo de servicio crece de forma exponencial y como consecuencia de esto las aplicaciones no pueden funcionar o retransmiten la información que creían perdida. Por tanto a partir de un cierto nivel de carga no solo crece el tiempo de servicio, sino que disminuye el rendimiento obtenido del enlace debido a las retransmisiones.

El objetivo de la Calidad de Servicio es asegurar que en casos de carga relativamente elevada (la zona marcada como de ‘congestión moderada’ en la gráfica) las aplicaciones que lo requieran podrán disfrutar de un tiempo de servicio reducido. Si la red tiene siempre niveles de carga inferiores el funcionamiento se complica y no se obtiene beneficio al aplicar mecanismos de Calidad de Servicio. Si la red tiene normalmente niveles fuertes de congestión los mecanismos de Calidad de Servicio difícilmente serán capaces de asegurar el nivel de calidad pedido a las aplicaciones que así lo requieran.

Tabla 5. Parámetros de Calidad de Servicio

Parámetro	Unidades	Significado
Ancho de Banda (bandwidth)	Kb/s	Indica el caudal máximo que se puede transmitir
Retardo (delay) o latencia (latency)	Ms	El tiempo medio que tardan en llegar los paquetes
Jitter	Ms	La fluctuación que se puede producir en el Retardo
Tasa de Pérdidas (loss rate)	%	Proporción de paquetes perdidos respecto a los enviados

QoS en IPv6 [14]

El campo ToS fue implementado dentro del grupo de diseño de IPv4 como un campo de ocho bits, compuesto por un valor de precedencia IP de tres bits y cuatro bits indicadores. Su función es especificar parámetros de prioridad, retardo, rendimiento y fiabilidad. De este modo, los paquetes con diversas opciones de ToS se pueden manejar con diferentes niveles de servicio dentro de la red.

De acuerdo a la recomendación RFC 791 [13], el ToS proporciona una indicación de los parámetros de calidad de servicio deseados. Éstos se utilizan para especificar el tratamiento del datagrama durante su transmisión en una red en particular. Algunas redes ofrecen prioridad de servicio, lo cual consiste en considerar el tráfico de alta prioridad como más importante que el resto (generalmente aceptando sólo tráfico por encima de cierta prioridad en momentos de sobrecarga). La elección más común es un compromiso de tres factores: bajo retardo, alta fiabilidad y alto rendimiento.

El campo ToS está compuesto por un campo de precedencia, tres indicadores D, T, R y dos bits no utilizados; el campo de precedencia utiliza ocho niveles, de cero (rutinaria) a siete (paquete de control de red); los tres bits indicadores permiten especificar qué es lo que más interesa, el retardo, el rendimiento o la fiabilidad. A continuación se presenta un resumen del campo ToS:

- Bits 0-2 : prioridad.
- Bit 3:0 = retardo normal, 1 = bajo retardo.
- Bit 4:0 = rendimiento normal, 1 = alto rendimiento.
- Bit 5: 0 = fiabilidad normal, 1= alta fiabilidad.

[14] Este apartado es una síntesis del material [SAL11]

- Bits 6-7: reservado para uso futuro.

El subcampo de precedencia es una medida de importancia relativa al datagrama. Se utilizan ocho-niveles de precedencia. IP tratará de proporcionar un tratamiento preferencial a los diagramas con precedencias superiores.

- 111-Control de Red
- 110-Control Entre Redes
- 101 - CRITICO/ECP
- 100 - Muy urgente (Flash Override)
- 011-Urgente (Flash)
- 010-Inmediato
- 001-Prioridad
- 000 - Rutina

El uso de los indicadores de retardo, rendimiento y Habilidad puede incrementar el coste (en cierto sentido) del servicio. En muchas redes un mejor desempeño de uno de estos parámetros significa un peor desempeño de otro. Por lo tanto, excepto para casos excepcionales, no se deben establecer más de dos indicadores.

Por su parte, el protocolo IPv6 tiene dos campos que pueden ser utilizados como herramientas para implementar QoS: Etiqueta de Flujo y Clase de Tráfico (ver figura 13).

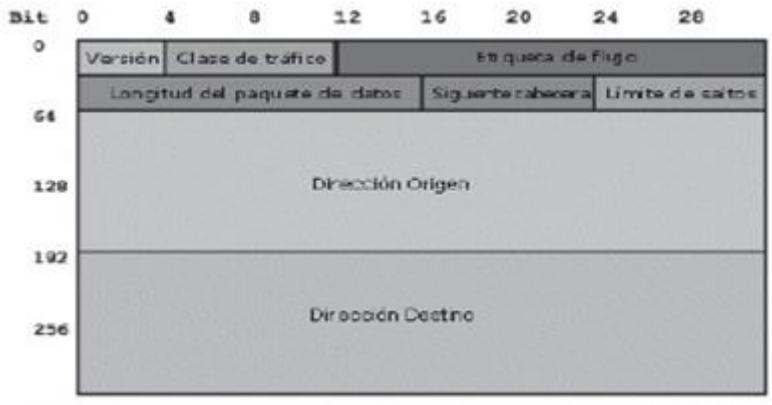


Figura 13. Estructura del Encabezado de un paquete IPv6

El campo Etiqueta de Flujo de 20 bits en la cabecera IPv6 se agrega para permitir el etiquetado de paquetes que pertenecen a flujos de tráfico particulares

y puede ser usado por el origen para etiquetar secuencias de paquetes para las cuales solicita un manejo especial por parte de los enrutadores IPv6, tal como la calidad de servicio no estándar o el servicio en tiempo real. Se exige a los hosts o a los enrutadores, que no dan soporte a las fondones del campo Etiqueta de Flujo, poner el campo en cero al enviar un paquete, pasar el campo inalterado al reenviar un paquete e ignorar el campo al recibir un paquete.

El campo de ocho bits Clase de Tráfico en la cabecera IPv6 es utilizado por los nodos origen y/o enrutadores intermedios para identificar y distinguir entre las diferentes clases o prioridades de paquetes IPv6; su fondón es similar al campo ToS de IPv4.

Los siguientes requisitos generales se aplican al campo Clase de Tráfico:

- La interface de servicio para el servicio IPv6 dentro de un nodo debe proporcionar un medio para que un protocolo de capa superior proporcione el valor de los bits Clase de Tráfico en los paquetes originados por éste. El valor por defecto debe ser cero para todos los ocho bits.
- Los nodos que soportan un uso específico de algunos o todos los bits Clase de Tráfico se les permite cambiarlos en los paquetes que los nodos originan, reenvían o reciben, como sea requerido para ese uso específico. Los nodos deben ignorar y dejar sin alterar los bits del campo Clase de Tráfico para los cuales no dan soporte a un uso específico.
- Un protocolo de capa superior no debe asumir que el valor de los bits Clase de Tráfico en un paquete recibido es el mismo que el valor enviado por el origen del paquete.

3. Movilidad[15]

Actualmente cuando un usuario se desplaza entre redes (roaming), cada una de las redes visitadas le facilita un IP diferente, como consecuencia de esto, un usuario no puede mantener una misma sesión, es decir, cada vez que el usuario cambia de red su sesión se corta y debe comenzar una nueva.

Se entiende por movilidad a la capacidad que tiene un nodo de una red para mantener la misma dirección IP, a pesar que se desplace físicamente a otra red. Es decir que sin importar su ubicación este puede seguir siendo accesible a través de su misma dirección IP.

[15] Este apartado está basado en [DIA13]

Una dirección IPv6 está compuesta de la siguiente manera:

dirección IPv6 / prefijo

Para que un nodo tenga la capacidad de movilidad, la misma debe ser habilitada en el mismo. Mientras este nodo se encuentra en su red, Home Network, la dirección IP que tiene asignada se conoce como Home Address. Siempre que su ubicación sea en su red origen, los paquetes enviados a esa dirección serán ruteados utilizando los mecanismos tradicionales de Internet.

Cuando el nodo se desplaza hacia otra red, adquiere una nueva dirección, conocida como Care of Address, con igual prefijo de red al de la red visitada. Una vez que configuró su nueva dirección debe informársela a un nodo, ubicado en su Home Network, que se conoce como Home Agent. Este proceso de asociar la home address con la nueva care-of address se conoce como Binding.

El momento en que el nodo móvil se mueve a otra red es el punto crítico del proceso. Esto se conoce como handover, y es el momento en el que el nodo móvil pierde conectividad con el otro extremo hasta que termine todo el procedimiento de obtener la nueva dirección y registrarse con el home agent. Este lapso debe ocupar el menor tiempo posible para evitar que se pierdan muchos paquetes, que luego tendrán que ser retransmitidos, porque mientras se encuentra en este estado el nodo no es capaz de recibir paquetes enviados a su home address.

El handover también se produce cuando un nodo se mueve entre diferentes Access Points (AP) pertenecientes a una misma red wireless, es decir, al desplazarse el nodo va cambiando su asociación entre los diferentes AP pero mantiene su dirección IP. Este proceso se realiza a nivel de enlace, y es transparente a las capas superiores. Estas no se enteran de este desplazamiento, con lo cual la dirección IP no se modifica.

En los últimos años el tamaño de Internet se ha disparado haciéndose necesario el uso generalizado de direccionamiento privado y dispositivos de traducción de direcciones (NAT). NAT: El acceso comercial a Internet para particulares y pequeñas empresas suele ser de este tipo. El abonado sólo

dispone de una IP pública, fija o no, que virtualmente comparten todos los nodos de su red local.

Desde el punto de vista de un servidor, es bastante probable que la dirección y el puerto origen de las peticiones recibidas no sean las mismas que usan sus clientes. Y para un nodo (host) que tenga un dispositivo NAT entre él e Internet, le será difícil determinar la dirección y el puerto con que un servidor recibe sus paquetes y tendrá complicaciones para actuar él mismo como servidor. El direccionamiento dinámico, ideado inicialmente para utilizar de forma más eficiente las escasas direcciones públicas disponibles, ha encontrado otros usos. Los nodos son ahora mucho más móviles de lo que eran hasta hace pocos años y, gracias al direccionamiento dinámico, pueden obtener una dirección topológicamente válida al cambiar de punto de conexión a Internet. Esto permite la denominada portabilidad de un nodo, aunque no una auténtica movilidad; dado que las conexiones TCP incluyen la dirección IP en su información de estado, al cambiar de dirección se perderá cualquier conexión abierta con la dirección antigua.

Pero uno de los mayores cambios habidos en Internet está en sus contenidos, la clase de recursos que los usuarios utilizan y cómo se conectan a ellos. Mientras que en el pasado lo habitual era acceder a un nodo a través de una dirección IP concreta, hoy probablemente estamos más interesados en acceder a un servicio. Deseamos conectarnos con nuestro banco, un periódico o una tienda de comercio electrónico, y poco importa el nodo en que reside dicho servicio.

En MIPv6 se diferencian tres agentes [MOVNE]:

- **Home Agent (HA):** se despliega en la red del operador que despliega el servicio de movilidad, registra la "verdadera posición" del nodo móvil.
- **Mobile Node (MN):** es el dispositivo del usuario que cuando se encuentra en la red de su operador tiene un dirección IPv6 denominada Home of Address (HoA) y cuando se desplaza adquiere un dirección diferente en la red visitada, denominada Care of Address (CoA).
- **Correspondent Node (CN):** es un nodo que pretende contactar con el MN y que, si no sabe cuál es su posición real, trata de contactar usando la HoA de MN.

Cuando el MN se encuentra en una red visitada lo primero que hace es enviar a su HA un mensaje de señalización para notificar su verdadera posición (1) (figura 14), es decir, informa de la dirección IPv6 que tiene en ese momento (CoA).

El HA actualiza su base de datos para enlazar la dirección que tendría el MN en la red del HoA con la que realmente tiene CoA.

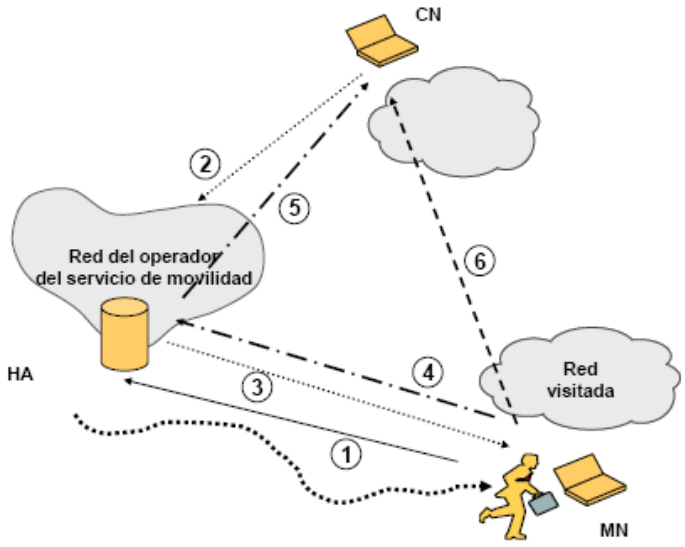


Figura 14. Funcionamiento básico de movilidad en IPv6

Cuando un CN quiere contactar con el MN, lo que hace es intentar contactar con el MN a través de su HoA (2) ya que es la dirección fija conocida por el CN. Los paquetes enviados a la red del operador y dirigidos a la HoA del MN son intercepatdo por el HA, encapsulados en un paquete MIPv6 y redirigidos hacia la nueva dirección CoA que el nodo movil tiene en la red visitada (3).

El MN contesta al CN encapsulando los paquetes de datos en un paquete MIPv6 y se lo envía al HA (4), que extrae el paquete original y se lo envía al CN (5).

Si el CN no tiene soporte MIPv6, es posible que el MN contacte con el CN para informarle de que un IPv6 cuando está en la red visitada es la CoA y no la HoA, de forma que el CN envía los paquetes de datos directamente a la CoA del nodo móvil (6). Este procedimiento se denomina Route Optimazation y es una mejora en el camino seguido por los paquete ya que no tiene que pasar por el HA evitando retrasos innecesarios. Si el CN no

posee soporte MIPv6 no es posible que el CN y el MN se comuniquen usando Route Optimazation.

Si el MN vuelve a cambiar de red, obtendrá una nueva CoA que deberá registrar en su HA con el fin de estar alcanzable con cualquier CN que quiera comunicarse con él.

Objetivos de la movilidad de IPv6:

- no estar limitado a una ubicación
- tener siempre conectividad IP
- que sea independiente del transporte
- conexiones en roaming robustas
- movilidad de las aplicaciones
- continuidad de las aplicaciones
- que un server pueda ser un dispositivo móvil

Problemas de la Movilidad:

Dentro de la arquitectura tradicional de Internet la movilidad es causa de cuatro problemas fundamentales a nivel de red (identificados por [MEL09]).

a) Direccionamiento: El direccionamiento y enrutamiento está definido de forma jerárquica para mayor escalabilidad. Como resultado, los nodos móviles cuando se conectan a una nueva red se encuentran casi siempre con una dirección topológicamente incorrecta.

b) Gestión de la localización: Si un nodo móvil cambia su dirección IP para solucionar el problema anterior, no podrá ser alcanzado por el resto de la red; a menos que esa nueva información esté disponible para los otros nodos.

c) Gestión de la conexión: La transición a una nueva dirección puede romper las conexiones activas (flujos) con otros nodos, ya que los protocolos de nivel de transporte utilizan la dirección IP como parte del identificador de conexión. Aún más, los largos periodos de desconexión pueden hacer que las aplicaciones de niveles superiores fallen, incluso si la gestión subyacente del tránsito entre redes funciona correctamente.

d) Seguridad: Los nodos móviles, cada vez que se mueven, deben ser capaces de autenticarse contra aquellos nodos con los que mantiene conexiones abiertas, y mantener o restablecer las asociaciones de seguridad a nivel de red.

El problema del direccionamiento se resuelve habitualmente mediante la asignación dinámica de direcciones, algo factible hace tiempo mediante el protocolo DHCP o la autoconfiguración de IPv6. La localización y la gestión de la sesión, sin embargo, requieren cambios bien en la infraestructura de red, bien en los nodos finales o en ambos al tiempo, mientras que las soluciones a los problemas de seguridad son todavía un tema bastante abierto.

Aunque el problema de obtener una dirección IP válida tras un movimiento puede parecer resuelto con la asignación dinámica de direcciones, este aspecto de la movilidad presenta dificultades con la latencia propia de los protocolos disponibles. Estos fueron diseñados específicamente para proporcionar portabilidad de nodos pero no movilidad, la cual exige tiempos cortos de asignación de direcciones. Con el protocolo DHCP, el proceso de configuración IP debe ser iniciado a petición del propio nodo móvil. Y en el caso del protocolo ND (Network Discovery) de IPv6, aunque establece el envío periódico de anuncios RA (Router Advertisement) por parte del router local, la tasa de envío de dichos mensajes es configurable y suele ser demasiado alta. El problema está, por tanto, en la capacidad del nodo móvil de detectar sus propios movimientos lo antes posible para forzar una re-configuración.

Trabajos Relacionados

Muchas empresas y entidades públicas están interesadas en implantar el protocolo IPv6 realizando un periodo de transición desde IPv4 a IPv6. Por ejemplo, en España el gobierno ha publicado las bases del “plan de fomento para la incorporación de IPv6” y la implantación del protocolo en el Ministerio de Industria, Energía y Turismo [ESP11]. Se prevé que para el 2013 los diversos países hayan completado gran parte de las etapas de pruebas del protocolo IPv6 y comiencen a ver como extender el ámbito de alcance, así como poner el foco en Servicios y Aplicaciones. En particular el grupo GRIDTICs (UTN - FRM) [GRI12], se plantea la importancia de comenzar a aprovechar las ventajas del nuevo protocolo (seguridad, multicast, etc),

en aplicaciones y el 6 de Junio del 2012 dejó planteada esta necesidad “Ya lo probamos, ahora llegó la hora de usarlo”.

GT IPv6 [CLA12], tiene un listado de proyectos realizados, vigentes y planificados, en el área de IPv6, entre los planificados se encuentran:

- Desarrollo de aplicaciones con soporte IPv6 (Programación de Sockets)
  - Universidad Nacional Autónoma de México (México)
- VoIPv6 con SIP para IPv6
  - Universidad Nacional Autónoma de México (México)
  - Universidad Nacional de Río Cuarto (Córdoba - Argentina)
- Multicast IPv6 (Opera Oberta, Open Student Television Network (OSTN), etc.)
  - Universidad Nacional Autónoma de México (México)
  - Universidad Nacional del Sur (Buenos Aires - Argentina)
- Firewalls con soporte IPv6
  - Universidad Nacional Autónoma de México (México)
  - Universidad Nacional de Río Cuarto (Córdoba - Argentina)

Se realizó un relevamiento en los sitios web de las Universidades de Argentina y se encontró que el 40% de las Universidad Nacionales tienen mención sobre cursos, conferencias ó trabajos que se están llevando a cabo en la temática de IPv6. En cuanto a las Universidades Privadas 15%.

En el caso de la Universidad Tecnológica Nacional se evaluaron todas sus facultades regionales e incluso el sitio del rectorado encontrándose que en el rectorado y algunas regionales se mencionaba IPv6. Conformando un 19% de los sitios los que hacen mención.

3.3.1.2. Tareas 2 y 3 - Aplicaciones existentes Clasificadas según su uso

En la tabla 6 se presenta un listado de aplicaciones que cuentan con soporte IPv6 clasificadas según su uso.

Tabla 6. Direcciones Reservadas en alcance enlace-local

	Aplicación	Versión	Nativa	Objetivo
1	RealVNC	Enterprise Edition	NO	Permite conexión remota entre equipos
2	HTTrack	3.46.1	NO	Reconstruye páginas web para utilizarlas sin conexión a Internet
3	Bit Cricket	1.0.2007.1030	NO	Calculadora de IP's
4	Ekiga	3.2.7	NO	Permite enviar mensajes instantáneos, videoconferencias y comunicación de VoIP
5	VLC	2.0.2	NO	Reproductor Multimedia
6	Información Meteorológica	No especificada	SI	Informa el clima de cualquier lugar del mundo
7	Konqueror Browser (forma parte del paquete de aplicaciones KDE)	0.9.9-7	NO	Permite la navegación de diversas páginas Web a través de Internet
8	Mozilla Firefox	17.0	NO	Permite la navegación de diversas páginas Web a través de Internet
9	Internet Explorer	9	NO	Permite la navegación de diversas páginas Web a través de Internet
10	Google Chrome	23.0.1271.95 m	NO	Permite la navegación de diversas páginas Web a través de Internet
11	Opera Browser	12.11	NO	Permite la navegación de diversas páginas Web a través de Internet
12	Safari	5.1.7	NO	Permite la navegación de diversas páginas Web a través de Internet
13	Seamonkey	2.14.1	NO	Permite la navegación de diversas páginas Web a través de Internet

14	Dolphin 3D Browser	1.60	NO	Permite la navegación de diversas páginas Web a través de Internet
15	CometBird Browser	11.0	NO	Permite la navegación de diversas páginas web a través de Internet
16	Smartalec Voyager XG	6.15	NO	Permite la navegación de diversas páginas web a través de Internet
17	MGET (Marine Geospatial Ecology Tools)	0.8a48	NO	Herramienta de geoprocesamiento de datos ecológicos y oceanográficos
18	Mozilla Thunderbird	17.0.5	NO	Gestor de correos electrónicos
19	KMail	4.10.2	NO	Gestor de correos electrónicos
20	The Bat!	5.4.0	NO	Gestor de correos electrónicos

3.3.1.3. Tarea 4 – Selección de Aplicaciones de Utilidad para el Laboratorio de I+D

De las 20 aplicaciones analizadas, si bien no son nativas para IPv6, se instalaron y se seleccionaron una por cada una de las utilidades descriptas. Luego de implementar IPv6 se probarán las mismas para analizar su funcionamiento en este protocolo.

3.3.2. ETAPA 2 – Conectividad IPv6

En esta etapa las tareas involucradas son las que se muestran en la figura 15. Los números de tareas retoman de las numeraciones de la etapa 1.

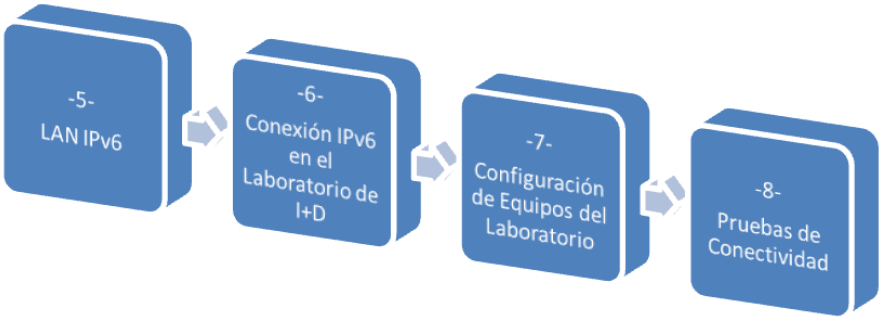


Figura 15. Tareas previstas en la Etapa 2

3.3.2.1. Tarea 5 - LAN IPv6

Las máquinas del laboratorio cuentan con Windows 7, un sistema operativo en el que habilitar IPv6 resulta sencillo.

Para la configuración de la LAN en primera instancia se configuraron las direcciones IPv6 que se asignaron a cada computadora. Para ello se accede a al Símbolo de Sistema a través del botón Inicio → Todos los Programas → Accesorios → Símbolo del Sistema → Ejecutar como Administrador (ver figura 16).

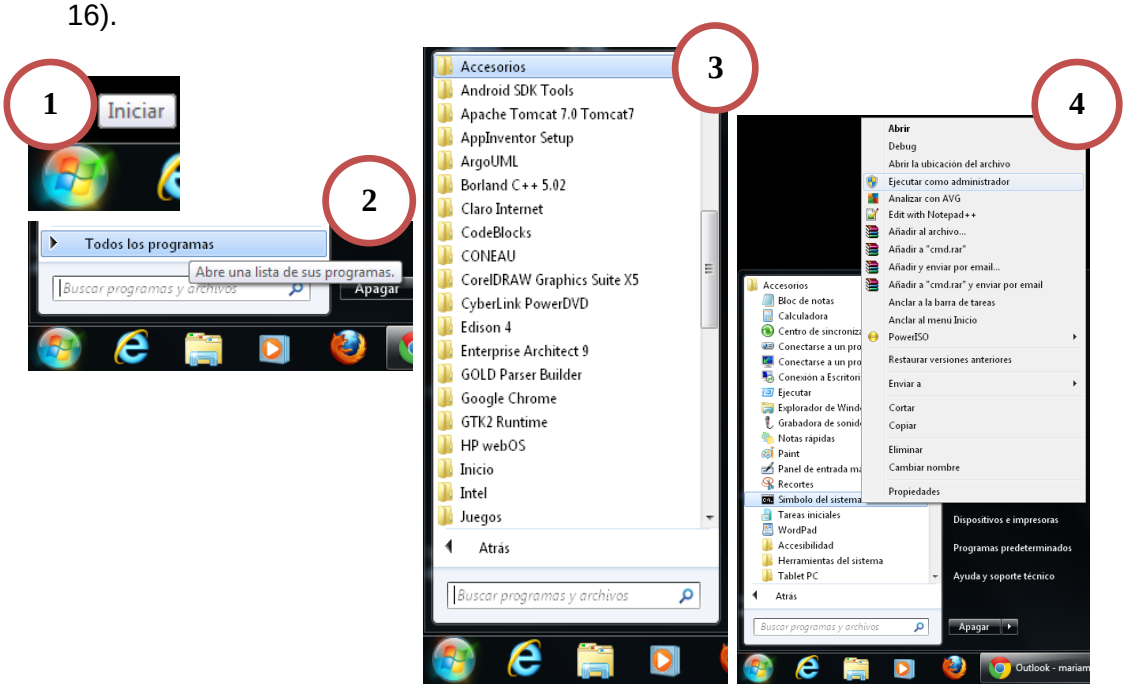


Figura 16. Pasos Seguidos

Como se puede observar en la figura 17, con el Símbolo del Sistema (en modo Administrador) ya abierto ejecutamos el comando: ‘netsh interface ipv6 add address “Interfaz” Dirección IPv6’.

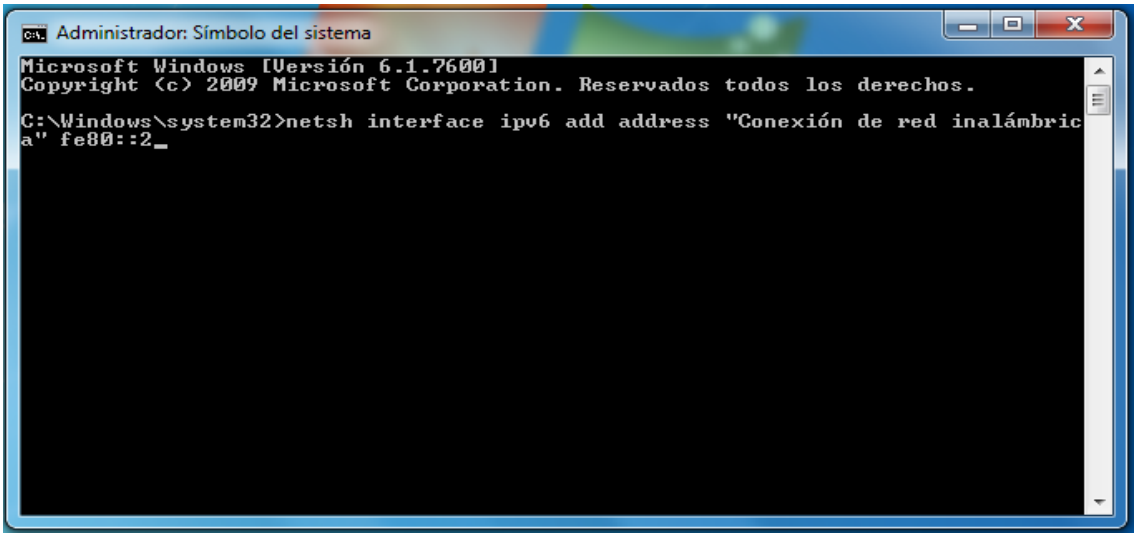


Figura 17. Asignación de dirección IPv6 al equipo

Luego se verifica que la dirección IPv6 elegida se asignó correctamente, también desde el Símbolo del Sistema (no fue necesario que estuviese en modo Administrador), ejecutamos el comando: 'ipconfig' (ver figura 18).

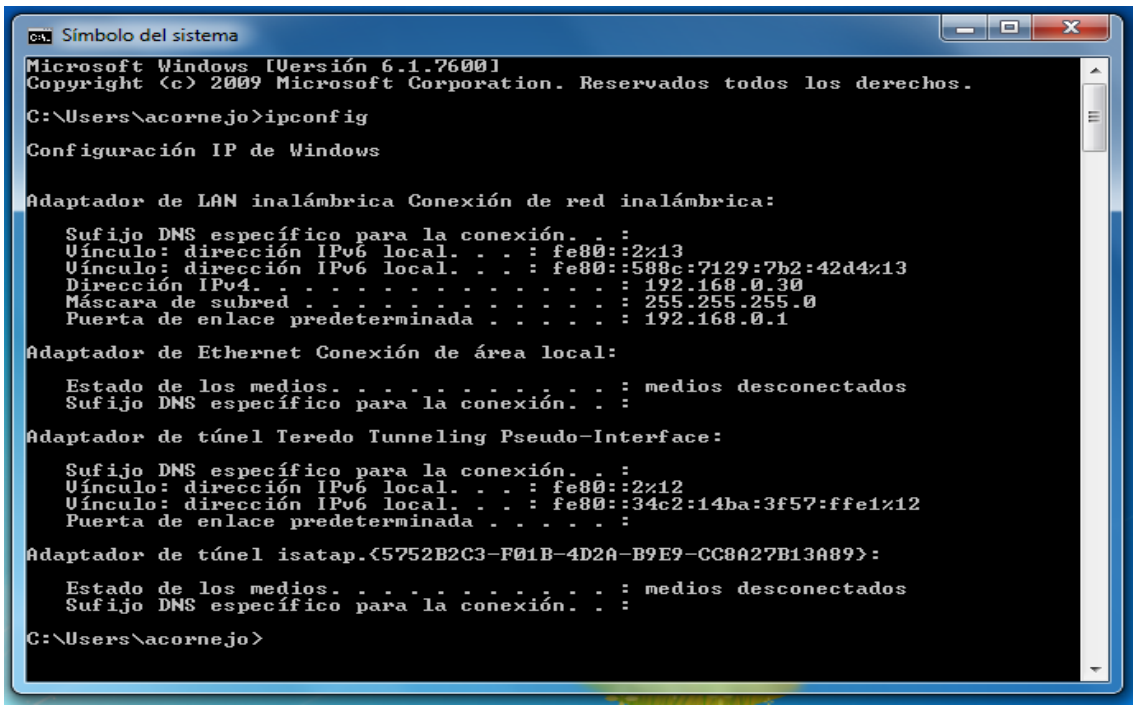


Figura 18. Verificación de asignación de dirección IPv6 al equipo

El mismo procedimiento de configuración de direcciones IPv6 se realizó con el otro equipo.

Prueba de conectividad entre computadoras

La prueba se realizó por medio del Símbolo del Sistema haciendo uso del comando ‘ping’ para observar si se configuraron correctamente las direcciones IPv6, en la figura 19 podemos observar la prueba desde el Equipo 1 y en la figura 20 la prueba desde el Equipo 2.

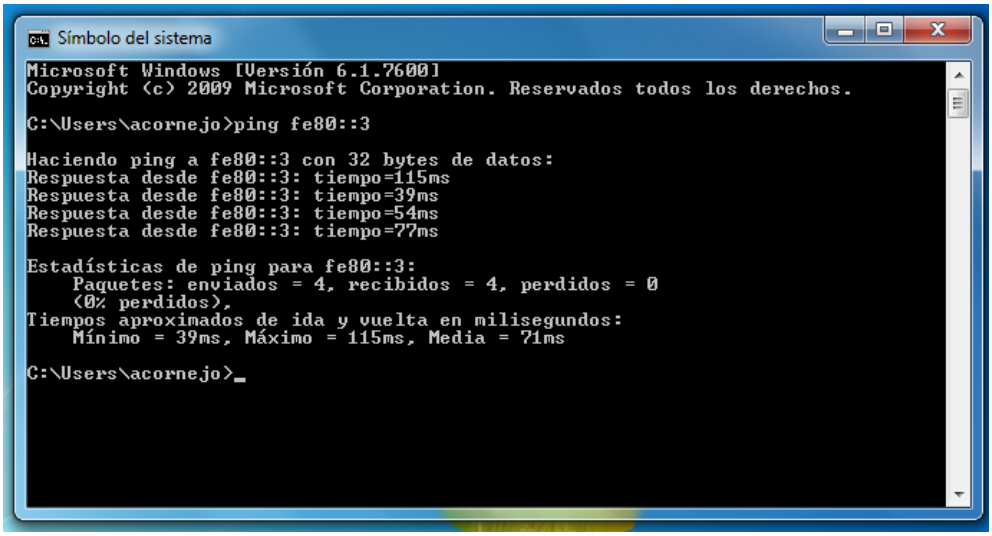


Figura 19. Prueba desde Equipo 1

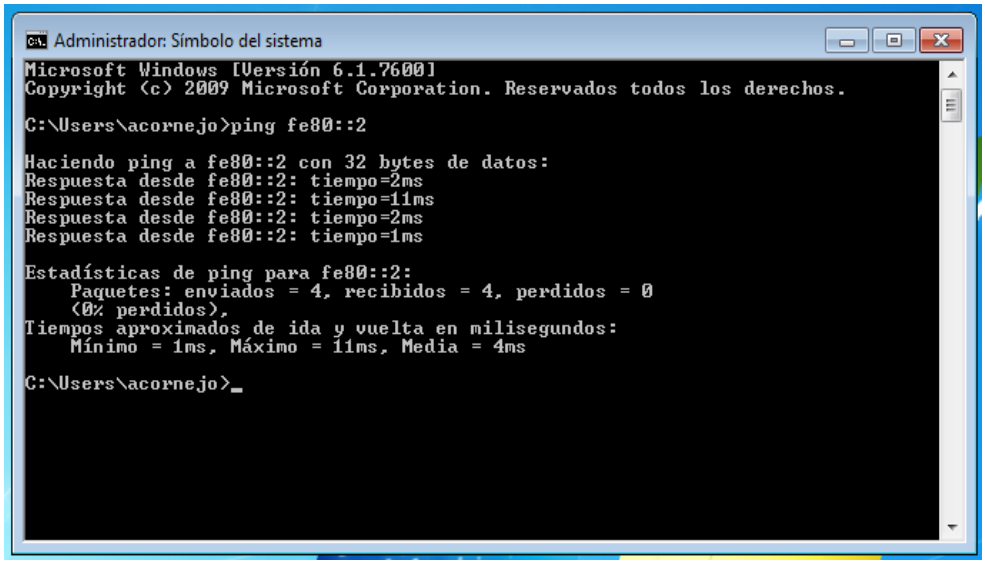


Figura 20. Prueba desde Equipo 2

Siendo exitosas las pruebas realizadas se concluyó que la configuración de la LAN IPv6 ha sido correcta.

3.3.2.2. Tarea 6: Conectividad a Internet mediante IPv6

Primeramente con la LAN creada por medio de tunneling fue posible acceder a páginas web IPv6, luego se avanzó con el tema de conectividad para poder extender la conexión existe al laboratorio del GIDFIS. Teniendo en la boca de red 71 asignada la IP 2800:110:1010::71 (ver figura 21).

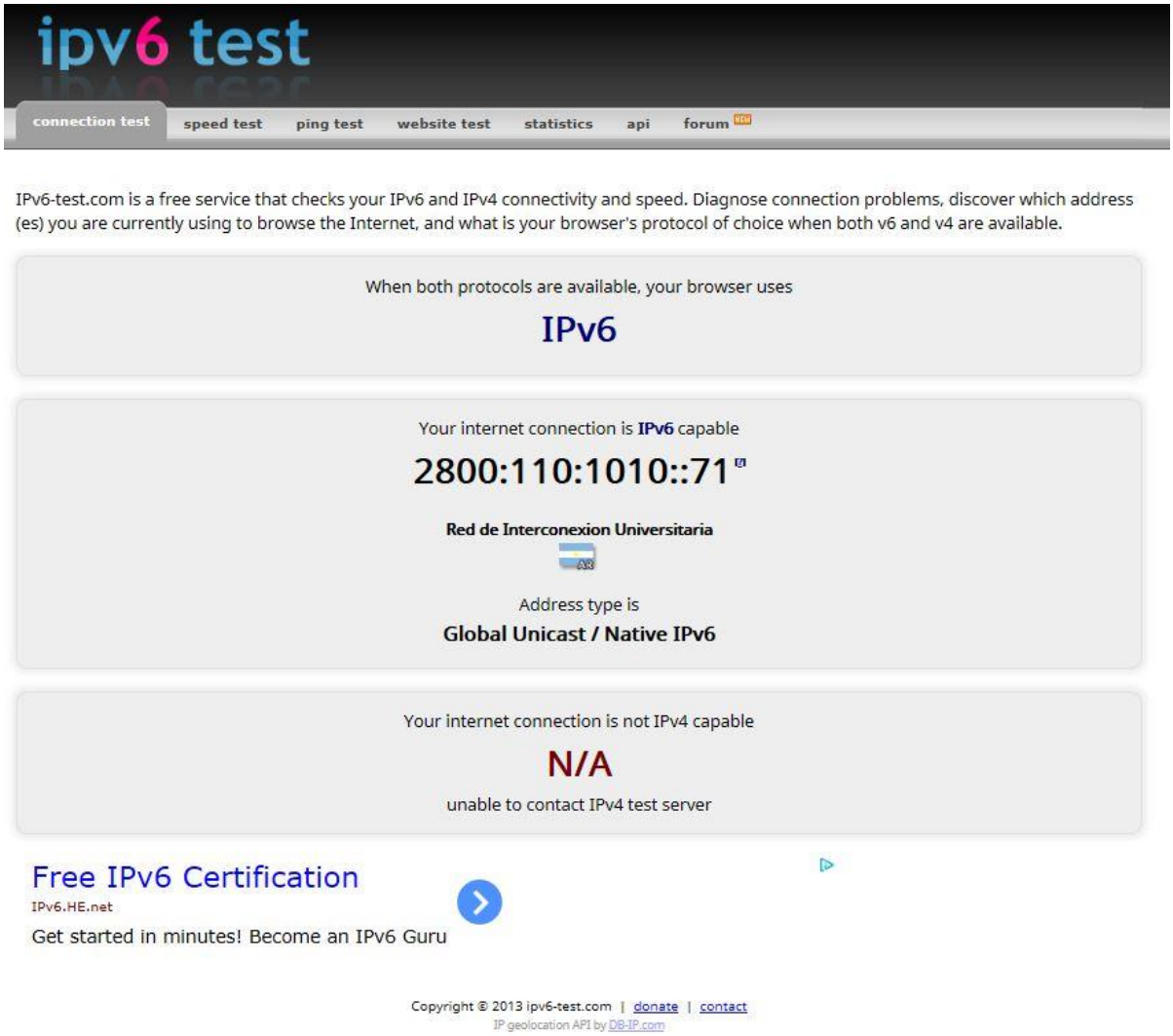


Figura 21. Testing Conexión IPv6 en el laboratorio del GIDFIS

Actualmente la ARIU (Asociación de Redes de Interconexión Universitaria) entrega el servicio de acceso a Internet a las instituciones asociadas. Los costos de funcionamiento de la RIU (Red Internet Universitaria) son soportados por las instituciones asociadas y el Ministerio de Educación de la Nación. La topología de la red es full mesh con un sitio central en dependencias del Data Center de Telecom Argentina. Allí se encuentra instalado un router con administración de la RIU y conexión a la Internet mediante Telecom Argentina y

conexión a Redes Avanzadas Internacionales a través de InnovaRed (Red Nacional de Investigación y Educación de Argentina) y CLARA (Cooperación Latino Americana de Redes Avanzadas). Ver figura 22, la cual fue tomada de la página oficial de ARIU [ARI13].

Figura 22. Topología IPv6 - Universidades Argentinas

Lograr una solución de conectividad que permita disponer el servicio de ipv6 al laboratorio del GIDFIS fue el objetivo de la implementación que se describe en el gráfico que mostramos a continuación.

En el mismo se distinguen 4 sitios relevantes como ser:

1. la infraestructura de la universidad UNLAM para su red de conectividad ipv4
2. la infraestructura de la universidad UNLAM para su red de conectividad ipv6
3. la instalación de LAN local para el laboratorio GIDFIS
4. la instalación de LAN local para el laboratorio 262

La UNLAM disponme de acceso a la red ipv6nativa mediante un esquema de direccionamiento público provisto por la RIU (red interuniversitaria), que corresponde al prefijo 2800:0110:1010::/48

Tiene presencia en la misma mediante un servidor web cuyo link es http://ingenieriaipv6.unlam.edu.ar

El mismo se encuentra instalado en el lab 262 desde el cual se accede directamente tanto hacia el exterior como al interior de la UNLAM. En lo referente al exterior se conecta al router perimetral que nos brinda acceso a la

nube ipv6. Además el lab 262 sirve de acceso al laboratorio GIDFIS para su salida a IPv6. Esta última solución fue el objetivo del trabajo que se describe.

Desde allí se conecta un switch cisco 300 mediante una fibra óptica dedicada de más de 200m de longitud que atraviesa distintos pabellones de nuestra universidad hasta llegar a otro switch de idénticas características en el lab gidfis.

Una de las características de esta implementación es que la red ipv6 se encuentra aislada físicamente de la red ipv4 para mantener un entorno de trabajo más ordenado y transparente.

Para lograr lo descripto anteriormente fue necesario comprar 2 Switches. En la figura 23 se muestra el mapa de conectividad.

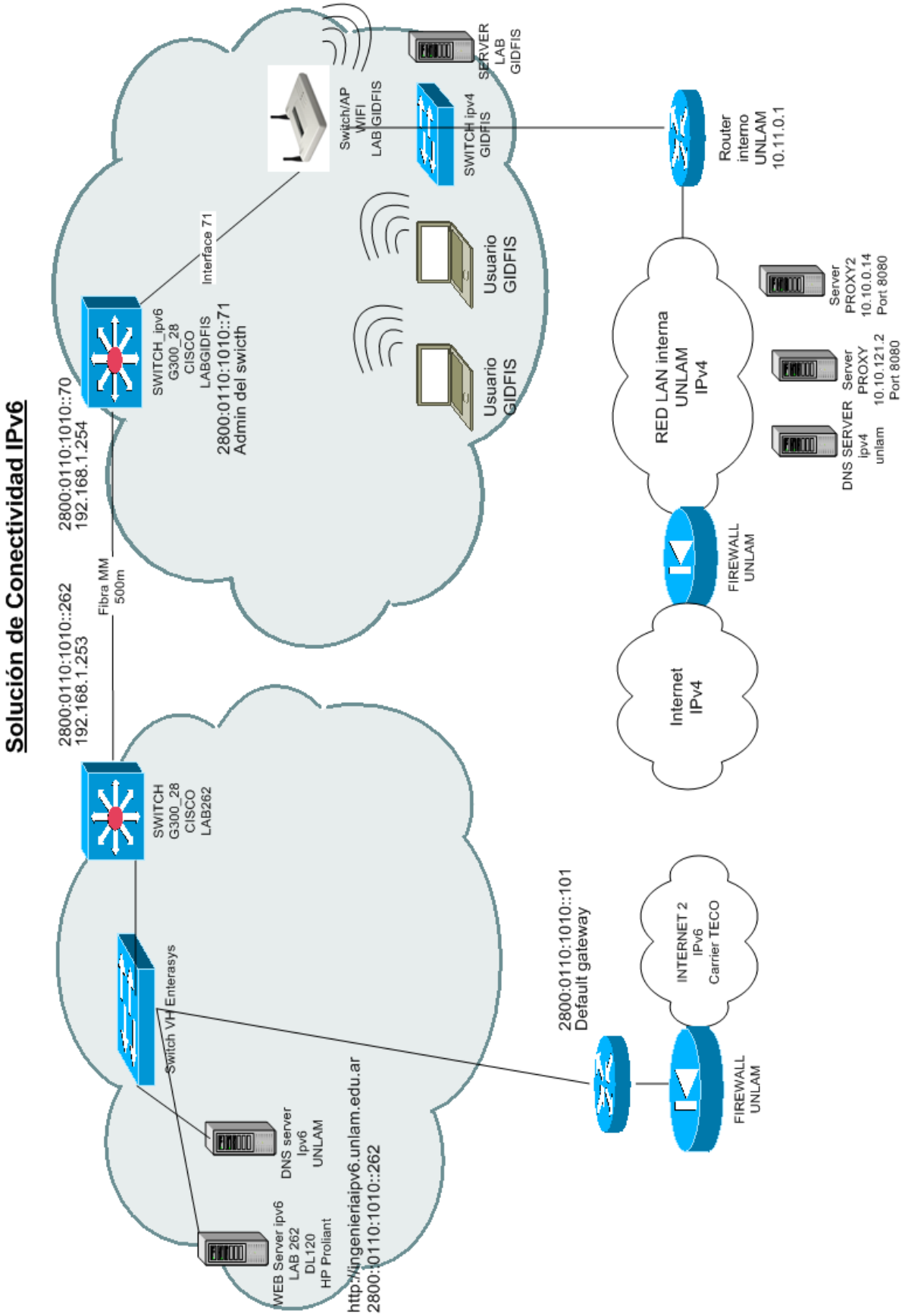


Figura 23. Mapa de Solución de Conectividad

En particular mediante este proyecto la Universidad Nacional de La Matanza cuenta con dos laboratorios con IPv6 físicamente distantes los cuales tienen conectividad mediante unos switches de fibra óptica. En particular uno de esos laboratorios corresponde al GIDFIS (Grupo de Investigación, Desarrollo y Formación en Innovación de Software) donde todas las computadoras cuentan con Windows 7. En cuanto a hardware se compro un router de carga balanceada que tiene la posibilidad de conectar hasta cuatro redes distintas (ver figura 24).

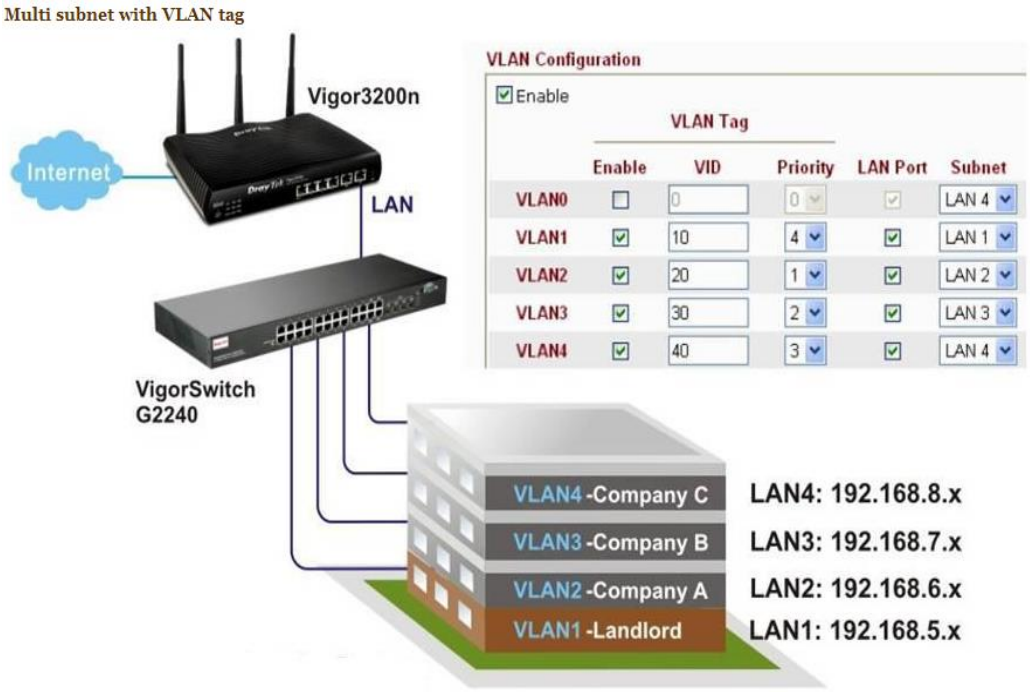
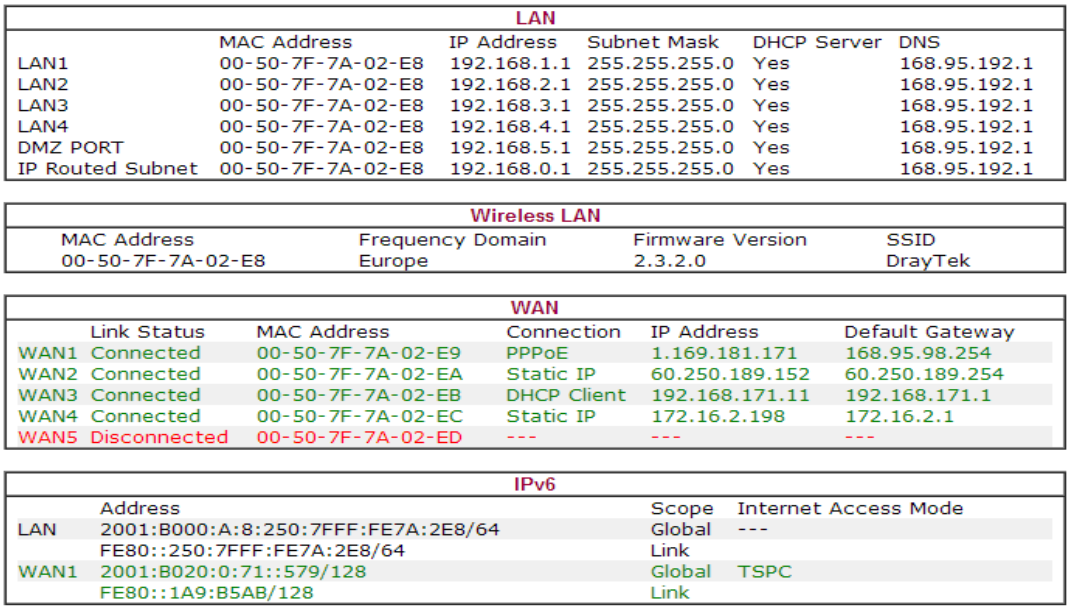


Figura 24. Características del equipamiento

El proveedor cuenta con una demostración online sobre la configuración del mismo [DRA13] (ver figura 25).



LAN

	MAC Address	IP Address	Subnet Mask	DHCP Server	DNS
LAN1	00-50-7F-7A-02-E8	192.168.1.1	255.255.255.0	Yes	168.95.192.1
LAN2	00-50-7F-7A-02-E8	192.168.2.1	255.255.255.0	Yes	168.95.192.1
LAN3	00-50-7F-7A-02-E8	192.168.3.1	255.255.255.0	Yes	168.95.192.1
LAN4	00-50-7F-7A-02-E8	192.168.4.1	255.255.255.0	Yes	168.95.192.1
DMZ PORT	00-50-7F-7A-02-E8	192.168.5.1	255.255.255.0	Yes	168.95.192.1
IP Routed Subnet	00-50-7F-7A-02-E8	192.168.0.1	255.255.255.0	Yes	168.95.192.1

Wireless LAN

MAC Address	Frequency Domain	Firmware Version	SSID
00-50-7F-7A-02-E8	Europe	2.3.2.0	DrayTek

WAN

	Link Status	MAC Address	Connection	IP Address	Default Gateway
WAN1	Connected	00-50-7F-7A-02-E9	PPPoE	1.169.181.171	168.95.98.254
WAN2	Connected	00-50-7F-7A-02-EA	Static IP	60.250.189.152	60.250.189.254
WAN3	Connected	00-50-7F-7A-02-EB	DHCP Client	192.168.171.11	192.168.171.1
WAN4	Connected	00-50-7F-7A-02-EC	Static IP	172.16.2.198	172.16.2.1
WAN5	Disconnected	00-50-7F-7A-02-ED	---	---	---

IPv6

	Address	Scope	Internet Access Mode
LAN	2001:B000:A:8:250:7FFF:FE7A:2E8/64	Global	---
	FE80::250:7FFF:FE7A:2E8/64	Link	
WAN1	2001:B020:0:71::579/128	Global	TSPC
	FE80::1A9:B5AB/128	Link	

Figura 25. Ejemplo - Configuración Router

En el caso particular del GIDFIS, este router se ha utilizado para tomar desde 2 bocas de red conectividad dos para IPv6 e IPv4.Cada una de las máquinas del laboratorio cuenta con una placa WIFI de modo que no se encuentran cableadas al router. Salvo el servidor del laboratorio que sí está cableado al router. En el laboratorio se cuenta también con una mesa redonda que se aprovecha como área de trabajo donde algunos investigadores llevan sus notebooks de forma que no tener una solución cableada y contar con WIFI es sumamente importante.

3.3.2.3. Tarea 7: Configuración de Equipos

No fue necesario aplicar una configuración adicional a la ya realizada en el momento de creación de la LAN para poder conectar las 6 computadoras del laboratorio del GIDFIS para poder tener conexión IPv4 e IPv6 al mismo tiempo.

3.3.2.4. Tarea 8: Pruebas de Conectividad

Las pruebas de conectividad consistieron en:

- Comunicación entre máquinas de la red interna con IPv6. Pruebas básicas mediante comandos DOS.
- En forma separada fue posible navegar tanto con IPv4 como con IPv6 en forma nativa.
- La conectividad llega en dos bocas aisladas y el router permite navegar con IPv4 ó IPv6 pero no seleccionaba automáticamente la boca involucrada, habiendo contactado al proveedor de los equipos se pudo

establecer contacto con el fabricante (Taiwan) quien efectuó un cambio en el firmware para poder desde el router realizar el cambio de boca según se requiera en para navegar con IPv4 o IPv6 (ver figura 26).

Figura 26. Router Laboratorio – Boca IPv4 y Boca IPv6

3.3.3. ETAPA 3 – INSTALACION

En esta etapa respetando la tarea 10, predefinida en el cronograma original, se instalaron aplicaciones seleccionadas presentadas en este informe en la tabla 5. Algunas de ellas nativas y otras con soporte a IPv6 pero no nativo. Se analizaron aspectos de funcionamiento, interfaz, etc. No solo se efectuaron pruebas de uso internas dentro del laboratorio del GIDFIS sino con otros nodos de la universidad (Laboratorio de Redes por ejemplo). En la figura 27 se muestran los pasos efectuados.

Figura 27. Pasos efectuados para la Instalación y Prueba de Aplicaciones

Y se comenzaron a hacer pruebas de lectura de paquetes mediante un sniffer las cuales sirvieron como base para las pruebas a realizar luego sobre las aplicaciones desarrolladas por el equipo de trabajo.

3.3.4. ETAPA 4 – PLANIFICACION DE APLICACIONES

En esta etapa se llevaron a cabo las tareas 11 y 12.

- Tarea 11: Seleccionar una aplicación de interés para su posterior desarrollo para IPv6 nativo.
- Tarea 12: Seleccionar un framework de desarrollo.

3.3.4.1. Tarea 11: Dominio de Interés

Se eligió como dominio de interés efectuar aplicaciones para redes P2P que permita manejar archivos. Bajo esta temática se consideraron dos aplicaciones:

- **Aplicación 1:** Se analizó e implemento un proyecto existente que permite compartir archivos entre los hosts con un funcionamiento similar a software P2P como eMule. Decidiéndose realizar la adaptación del código para ser implementado en el laboratorio de GIDFIS. Esto implicó analizar e implementar PNRP y WCF para transmitir y compartir los archivos (lo cual será detallado en la etapa siguiente Etapa 5-Desarrollo).

  La aplicación consta de un pequeño server donde se graba la identificación de las máquinas disponibles y los archivos que ellas comparten, (solo la información). Esta infraestructura de aplicación realiza las siguientes operaciones:

  - Generar el nombre de peer correspondiente con el host
  - Notificar al servidor del host para que este lo registre
  - Compartir un archivo informando al servidor que el host tiene el archivo disponible. Solo comparte el nombre del archivo y que lo tiene disponible
  - Buscar un archivo para descargar en el servidor
  - Descargar archivo comunicándose con el peer que está registrado en el servidor. De esta forma la transmisión del archivo es entre los hosts
  - Al recibir una petición de archivo se envía el mismo mediante una técnica de streaming por partes del archivo.

- **Aplicación 2:** Se generó una aplicación que además de permitir el envío de archivos añadiera otras funcionalidades y pudiera ser utilizada por los docentes al dar clase en los laboratorios de la universidad.

  Los usuarios se deben conectar a una red que tendrán en común el nombre de la red y el password, la variante estará en el nombre del usuario. La aplicación que posee el docente le permite:

  - Escribir en el chat
  - Transmitir imágenes
  - Video con audio
  - Envío de archivos.

Se documentó en detalle las características de ambas aplicaciones planteándose tareas precisas basadas en consideraciones de requerimientos, modelado con UML, diseño de pantallas (para lo cual se utilizó una herramienta de mockup).

3.3.4.2. Tarea 12: Selección del Framework

Se selecciona .NET por ser el entorno de desarrollo en el cual más miembros del grupo cuentan con experiencia. Por otra parte la Universidad cuenta con un convenio con Microsoft mediante el cual obtienen licencias, las que permitieron instalar el Visual Studio en tres de las computadoras del laboratorio, las que estuvieron afectadas al desarrollo y en 1 notebook utilizada para tener el ambiente replicado. Los framework de desarrollo cuentan con funciones ya implementadas para IPv6 (ver figura 28).

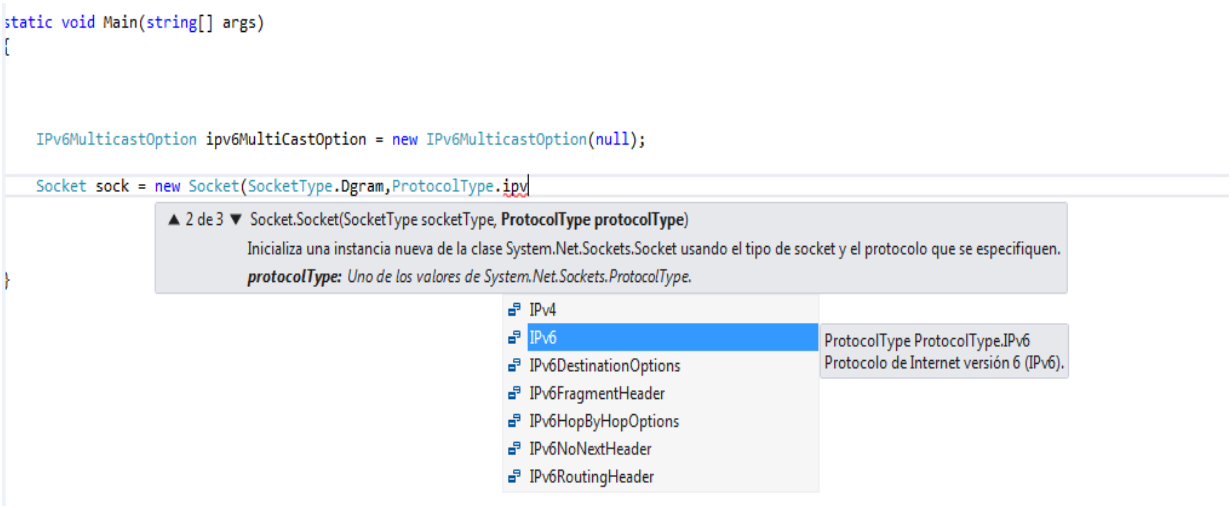


Figura 28. Framework de Desarrollo – Funciones para IPv6

Por otra parte se analizó el plugin específico “C4F Toolkit” (Coding for fun – Peer to Peer Toolkit) [C4F07]. Evaluándose sus características entre las que podemos resumir las siguientes:

- ✓ Incorpora controles para generar aplicaciones nativas en IPv6 los cuales sólo requieren configuración evitando de este modo una programación completa para generar los mismos.
- La documentación de C4F se ha descontinuado, no hay actualizaciones recientes de la documentación en forma oficial. C4F07 No obstante hay algunos ejemplos que permiten analizar detalles del framework
- ✓ Es posible obtener el código fuente de la aplicación, incluyendo los controles agregados por C4F, con lo cual se manipular el mismo para generar una solución diferente a la que se obtiene por defecto.

Las figuras 29 y 30, presentan está herramienta adicional.

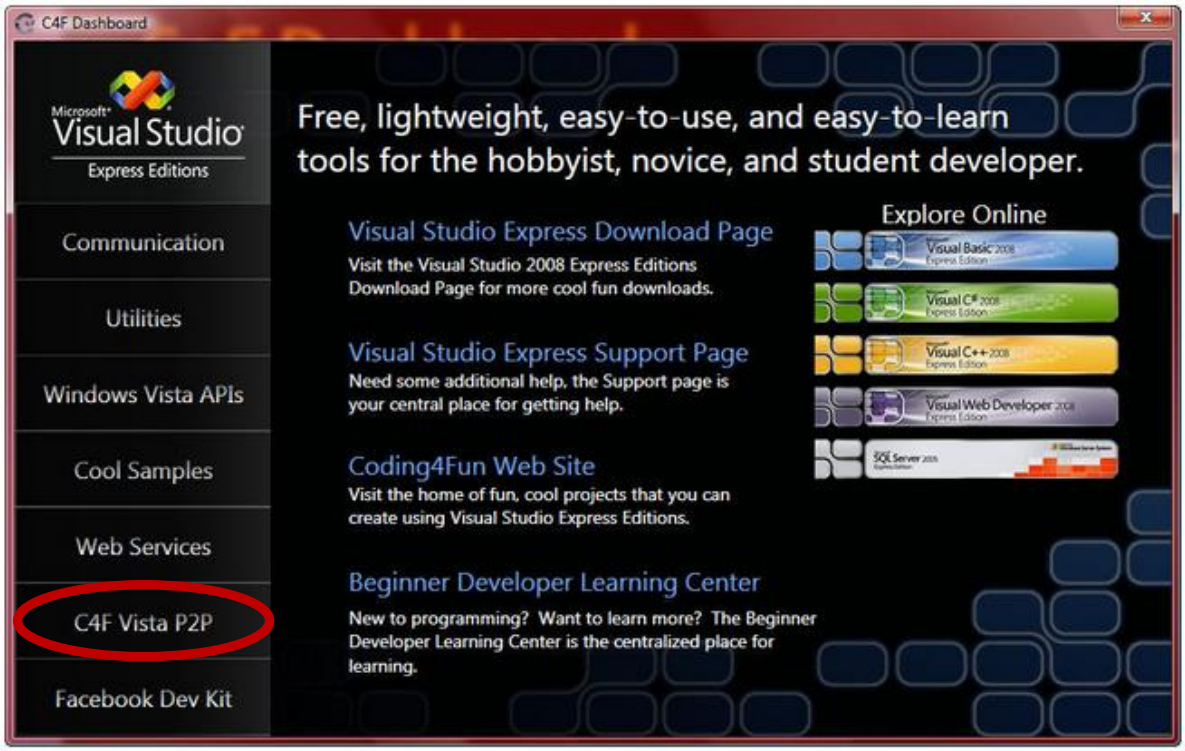


Figura 29. C4F Vista P2P

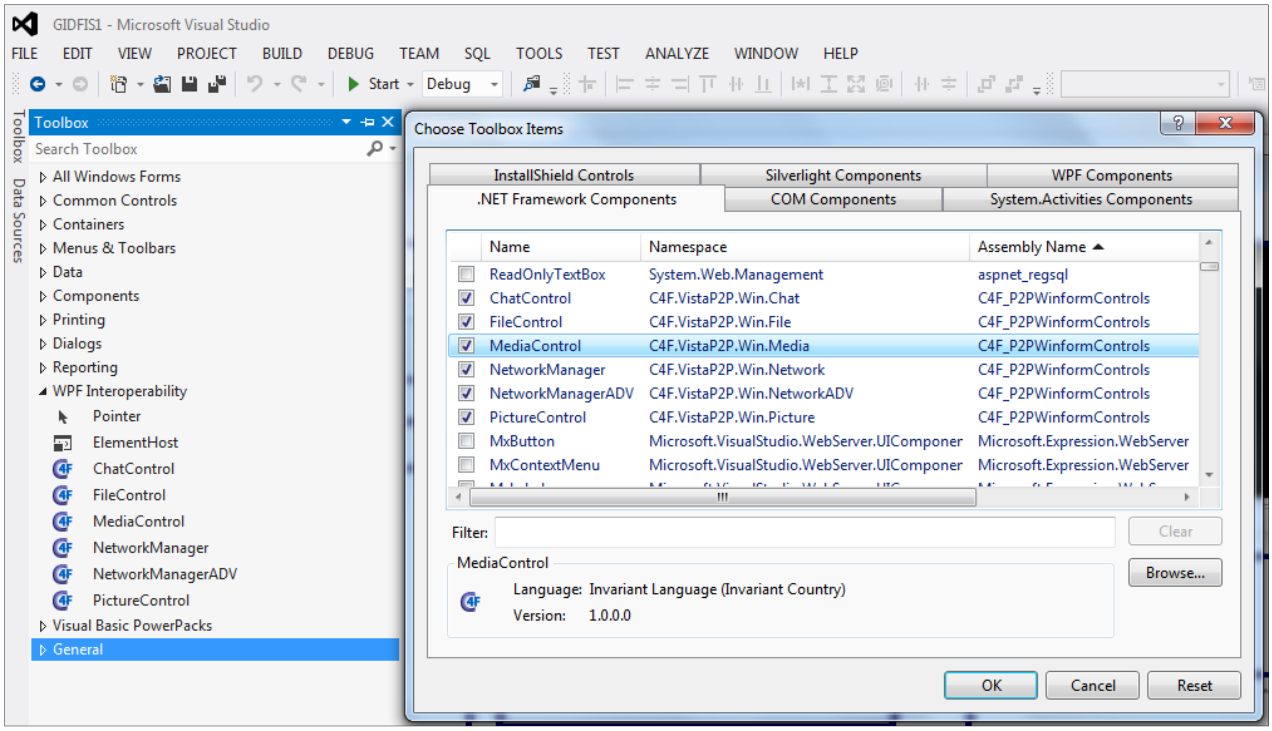


Figura 30. Controles Propios del Toolbox de C4F

3.3.5. ETAPA 5 – Desarrollo de una Aplicación

Para el desarrollo de la aplicación se utilizó .NET en particular se programó en #C, sin instalar en primera instancia C4F. Efectuándose las tareas descriptas en la figura 31.

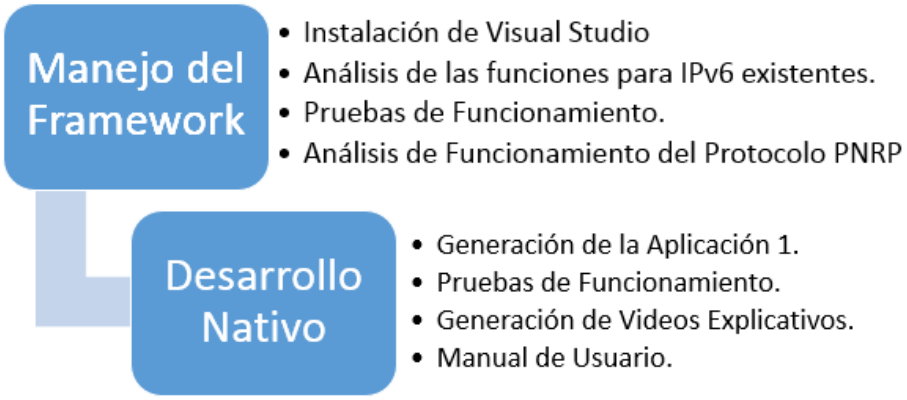


Figura 31. Tareas comprendidas en la Etapa 5

Para llevar a cabo esto fue necesario utilizar las siguientes tecnologías:

- **Protocolo PNRP** (Peer Name Resolution Protocol - Protocolo de resolución de nombres de pares) [MIC14]. Este protocolo permite resolver la dirección de red (dirección, protocolos y puertos). Las propiedades más destacadas del protocolo son: (A) No se necesita servidor para generar el nombre del peer; (B) Nombra no solo el ordenador (dirección IP), puede nombrarse una dirección y un puerto, de esta forma se puede nombrar un servicio o una aplicación. El framework ofrecido por .net tiene la posibilidad de generar el nombre del peer de manera segura e insegura.

- **Clouds:** A través de esta tecnología los nodos se pueden comunicar a través de clouds, el cual es un grupo de computadoras que se pueden comunicar entre sí. Pueden clasificarse en: (1) Global Cloud: El cloud global corresponde a direcciones en IPV6 en Internet. (2) Link Local Cloud: El cloud local corresponde a direcciones IPV6 locales por ejemplo en un a LAN.

- **PNRP Name:** El nombre de un peer es un nodo de comunicación que puede ser una computadora, un usuario o un grupo, un servicio, o lo que sea necesario resolver a través de una dirección IPV6. Los nombres pueden ser:
    1) Inseguros pueden utilizarse en una red privada o en algún tipo de red que ya se encuentre protegida.
    2) Seguros son protegidos con un certificado y una firma digital, el cual maneja el generador del nombre.

Un PNRP ID está compuesto por 256 bits. Los 128 bits altos que son conocidos como (P2P ID), los cuales son un hash con la clave pública que se utiliza para generar los nombres de los nodos. Los 128 bits bajos son usados para determinar la ubicación del servicio el cual representa las diferentes instancias del mismo P2P ID en el mismo cloud (ver figura 32).

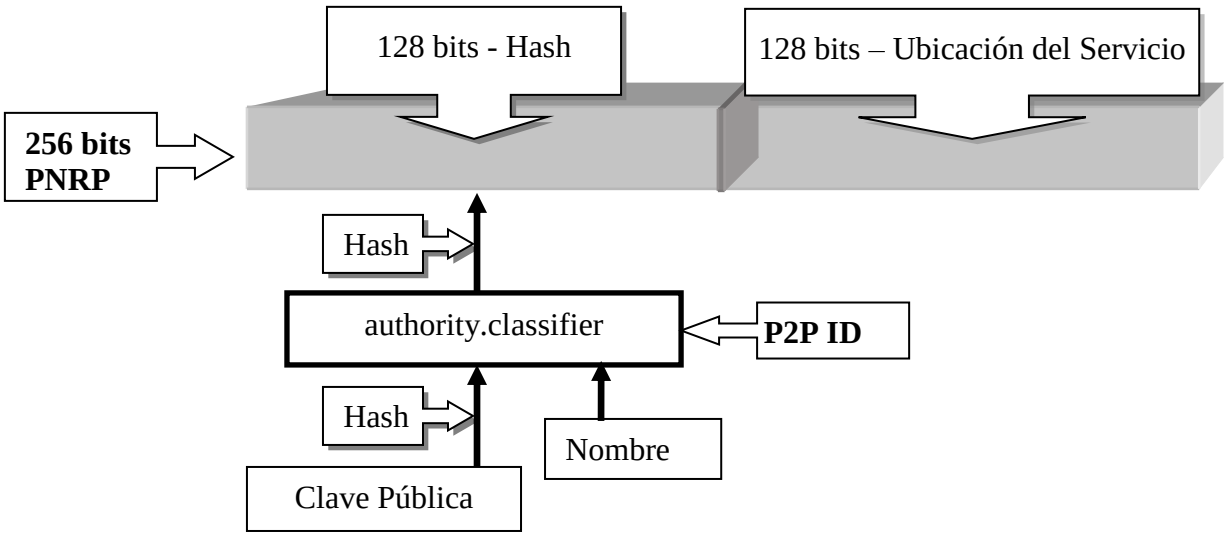


Figura 32. Protocolo PNRP

Desarrollo en .NET

Para implementar un servicio Peer to Peer para IPv6 en .NET primeramente deben realizarse tres pasos:

1. Registración de un Peer [WIN06] [MSD14c] - La codificación correspondiente se muestra en la figura 33.

```
public  void RegisterLocaPeer(PeerInfo info)
{
    PeerName peerName = new PeerName(info.Classifier,PeerNameType.Unsecured);
    PeerNameRegistration peerNameRegistration = new PeerNameRegistration();
    peerNameRegistration.PeerName = peerName;

    peerNameRegistration.Port = info.PortNumber;
    peerNameRegistration.Comment = info.Comment;
    peerNameRegistration.Cloud = Cloud.AllLinkLocal; // cloud local
    peerNameRegistration.Start();
    info.PeerHostName = peerNameRegistration.PeerName.PeerHostName;
}
```

Figura 33. Registración de un Peer

2. Resolución de Dirección a través del PeerHostName (Id) [WIN06], [MSD14c] - La codificación correspondiente se muestra en la figura 34.

```
public List<PeerInfo> ResolveByPeerHostName(string peerHostName)
{
 List<PeerInfo> foundPeers = new List<PeerInfo>();

 PeerNameResolver resolver = new PeerNameResolver();
 var resolvedName = resolver.Resolve(new PeerName(peerHostName, PeerNameType.Unsecured), Cloud.AllLinkLocal);


 foreach (var foundItem in resolvedName)
 {
     foreach (var endPointInfo in foundItem.EndPointCollection)
     {
         PeerInfo info = new
         info.PeerHostName =
         info.Classifier = fo
         info.Comment = found
         info.PortNumber = en

         if (endPointInfo.Add
             info.Ipv6Adress
         foundPeers.Add(info)
         endPointInfo.Address
     }

 }

 return foundPeers;
```

```
IsIPv4MappedToIPv6
IsIPv6LinkLocal
IsIPv6Multicast
IsIPv6SiteLocal
IsIPv6Teredo
MapToIPv4
MapToIPv6
ScopeId
ToString
```

```
string IPAddress.ToString()
Converts an Internet address to its standard notation.

Exceptions:
  System.Net.Sockets.SocketException
```

Figura 34. Resolución de Direcciones

3. Llamado a Servicio de un Peer a través de WCF (Windows Communication Foundation) usando la URL (Uniform Resource Locator) indicada [MSD14b], [MSD14a]. La codificación correspondiente se muestra en la figura 35.

```
        public void CallHost(PeerInfo peerinfo)
        {
            string Address = string.Format("net.tcp://{0}:{1}/TransferEngine",
              peerinfo.PeerHostName, peerinfo.PortNumber);
            Uri uri = new Uri(Address);
        }
    }
}
```

Figura 35. Llamado a Servicio de un Peer

Es posible el desarrollo de una aplicación a través de la utilización de PNRP y WCF de forma directa con el .Net framework. Las clases para el desarrollo se encuentran en el espacio de nombres System.Net.PeerToPeer. En el mismo se encuentran las herramientas que permiten generar la construcción de identificadores a través de las direcciones de los hosts y la resolución de los identificadores para obtener su correspondiente dirección IPV6.[16, 17]

Implementación nativa

Para la implementación nativa se hicieron pruebas con la utilización de sockets y el protocolo de transporte UDP. En el formato nativo se hizo posible la prueba y verificación de la utilización de grupos multicast.

Para la investigación se analizó e implemento un proyecto existente que permite compartir archivos entre los hosts con un funcionamiento similar a software P2P como eMule. Se hizo una adaptación del código para ser implementado en el laboratorio de GIDFIS, con este sistema se pudo ver como se implementaba PNRP y WCF para transmitir y compartir los archivos.

La aplicación consta de un pequeño server donde se graba la identificación de las maquinas disponibles y los archivos que ellas comparten, (solo la información). Esta infraestructura de aplicación realiza las siguientes operaciones:

- Generar el nombre de peer correspondiente con el host
- Notificar al servidor del host para que este lo registre

[16] http://msdn.microsoft.com/en-us/library/system.net.peertopeer(v=vs.110).aspx
[17] http://msdn.microsoft.com/en-us/magazine/cc188685.aspx

- Compartir un archivo informando al servidor que el host tiene el archivo disponible. Solo comparte el nombre del archivo y que lo tiene disponible
- Buscar un archivo para descargar en el servidor
- Descargar archivo comunicándose con el peer que está registrado en el servidor. De esta forma la transmisión del archivo es entre los hosts
- Al recibir una petición de archivo se envía el mismo mediante una técnica de streaming por partes del archivo.

Además de informes se generaron unos videos explicativos que han permitido contribuir a la capacitación de los alumnos en formación que son miembros del equipo, los cuales fueron subidos en forma privada a YOUTUBE y compartido el enlace entre los miembros del grupo. Los videos detallaron las siguientes cuestiones:

- Explicación general sobre el entorno y configuración del servidor (ver captura en la figura 36).
- Ejecutar un Peer (ver captura en la figura 37).
- Chequear Peer (ver captura en la figura 38).
- Demostración de Ejecución de la Aplicación en el laboratorio (ver captura en la figura 39).

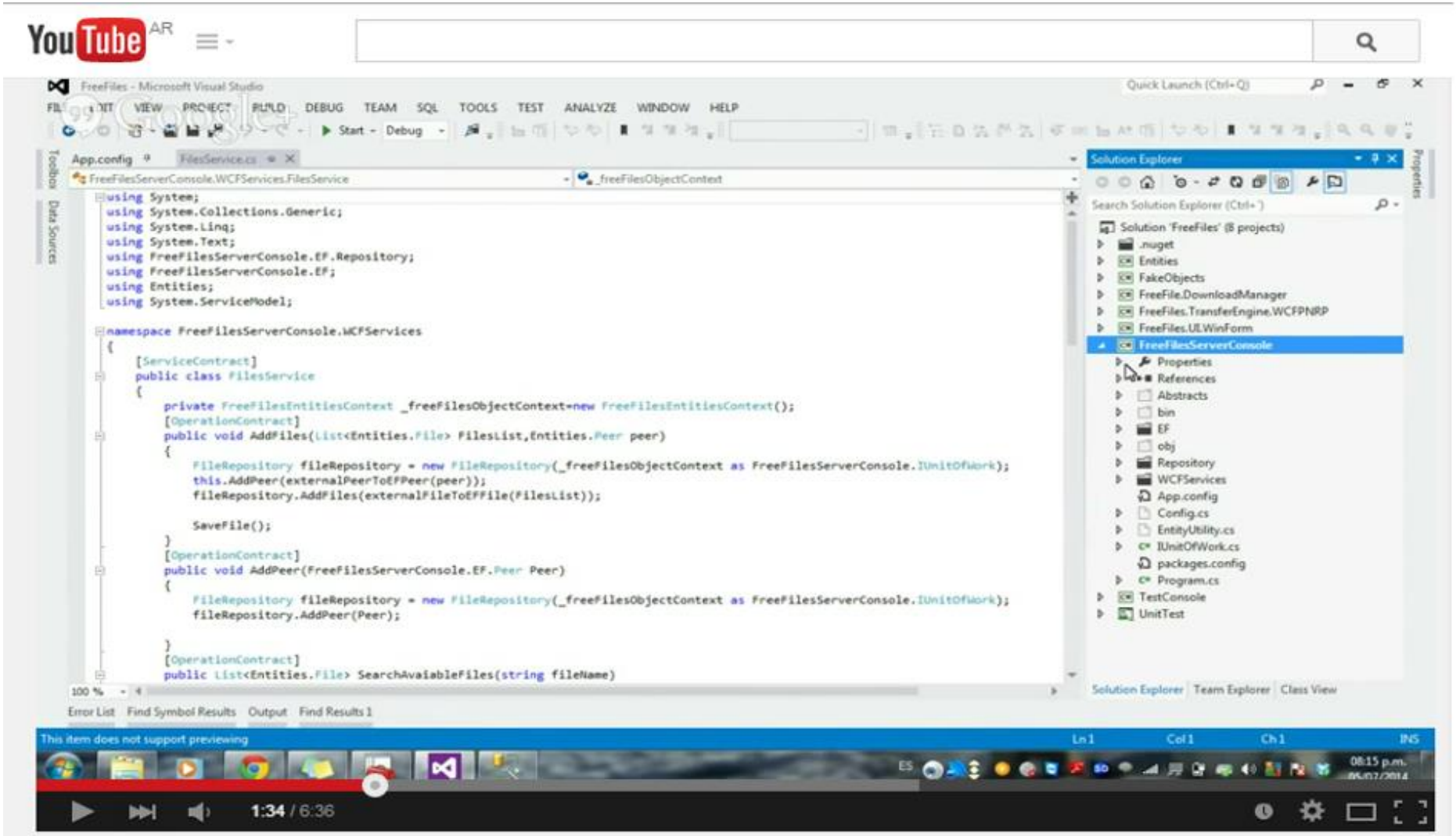


Figura 36. Explicación general sobre el entorno y configuración del servidor

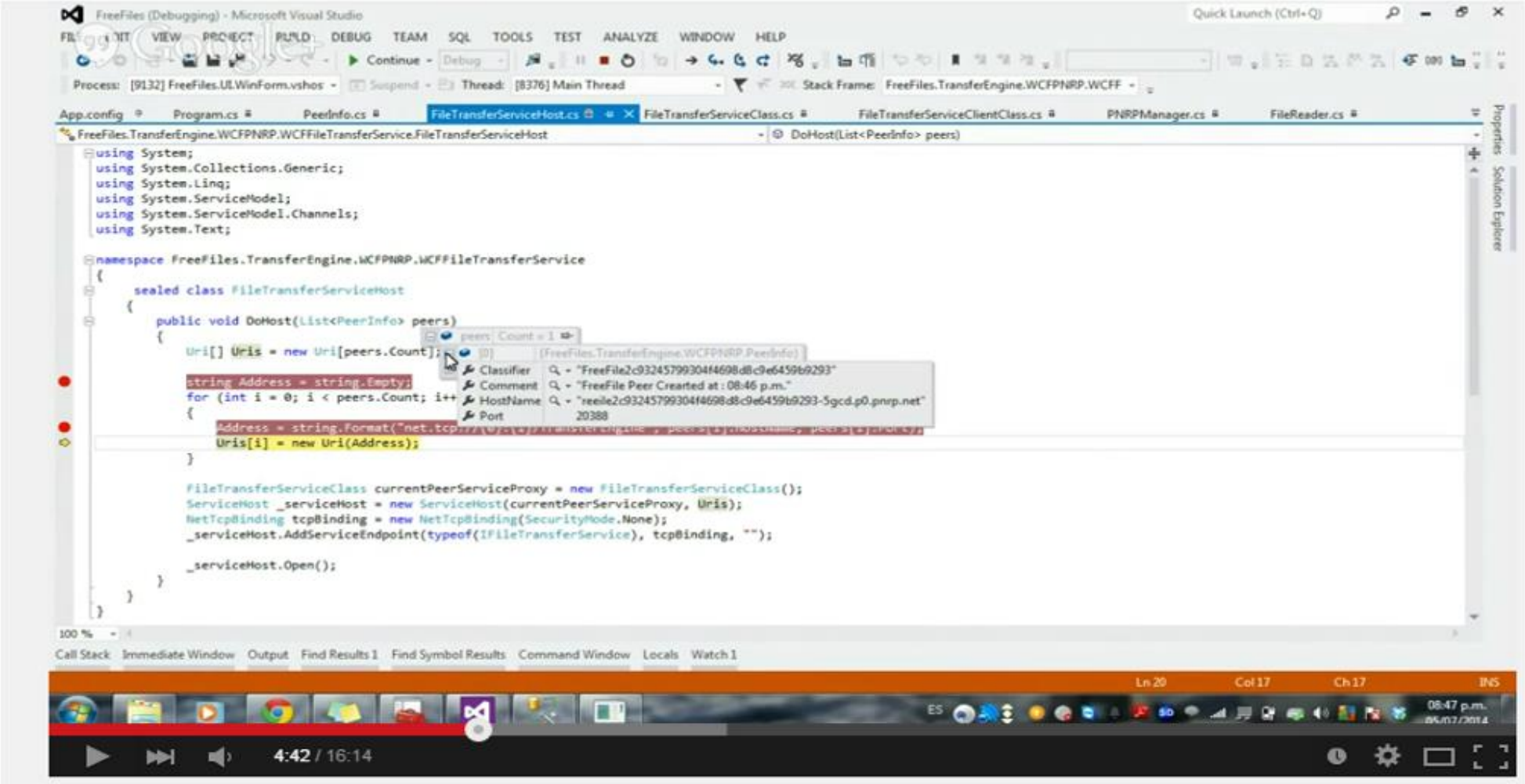


Figura 37. Ejecutar un Peer

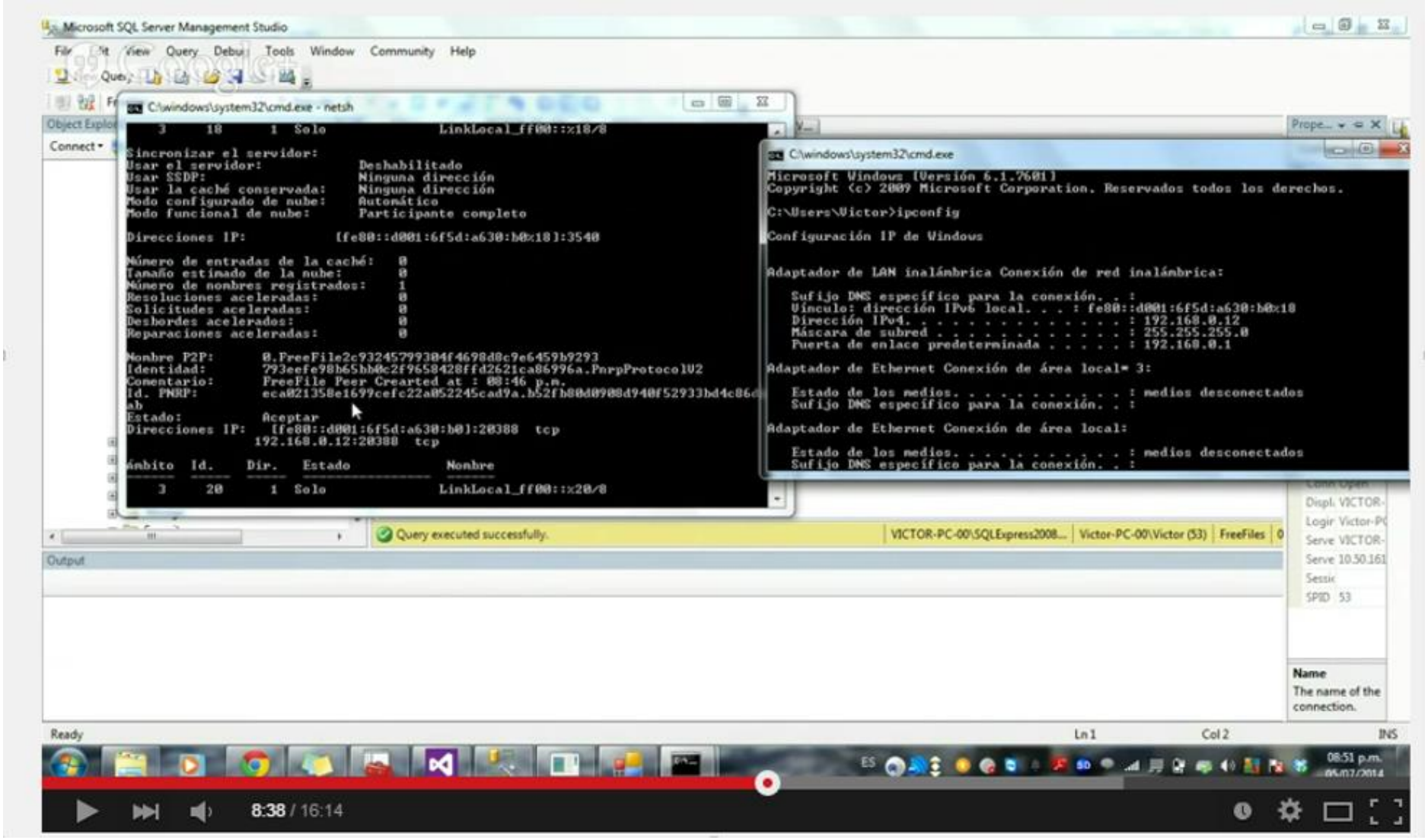


Figura 38. Chequear Peer

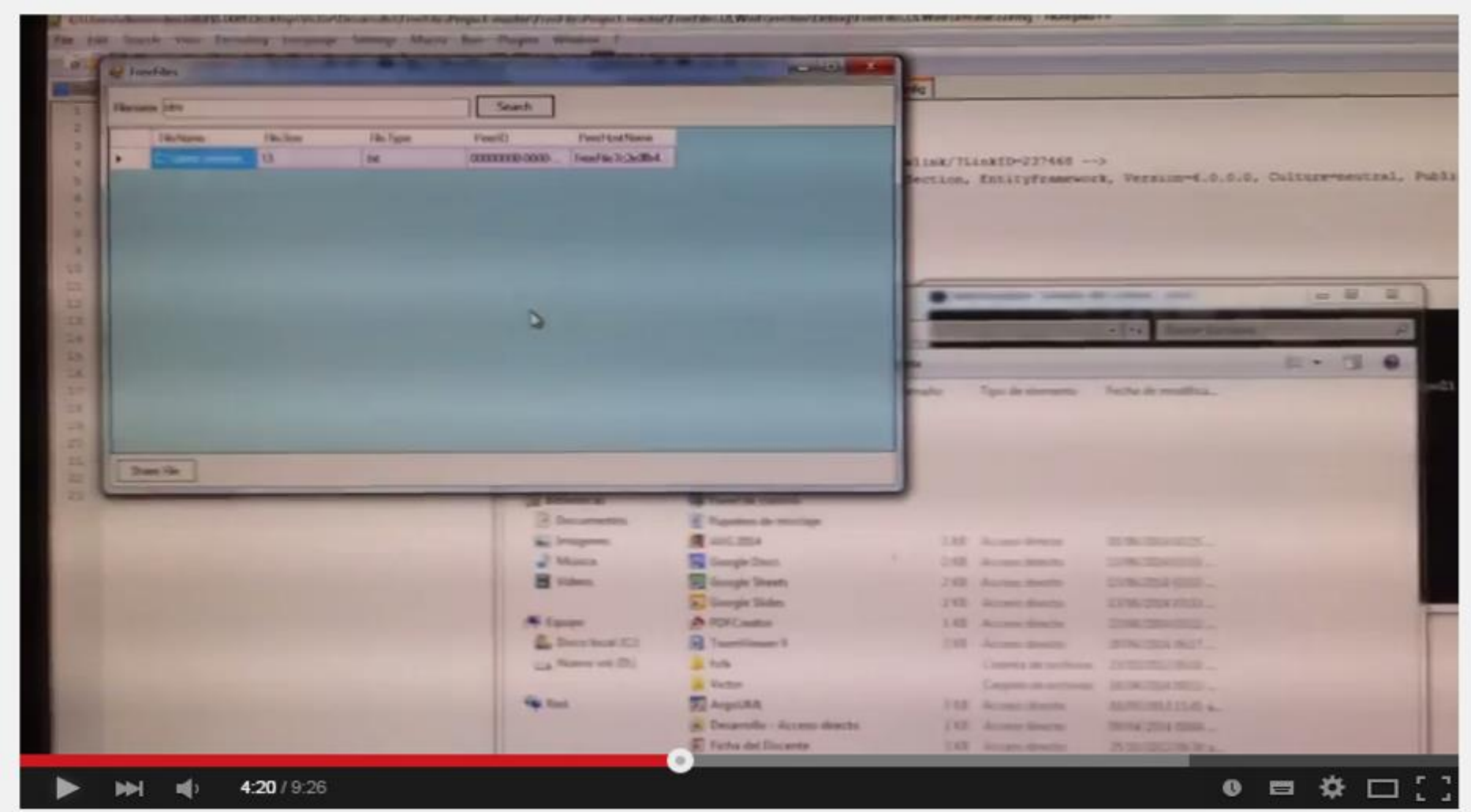


Figura 39. Demostración de Ejecución de la Aplicación en el laboratorio

Los videos generados conforman un total de 32 minutos de grabación siendo un importante elemento construido como instructivo para otros miembros del grupo, quienes no habían participado activamente en el desarrollo de la aplicación.

En la figura 40 se puede ver la aplicación corriendo desde el Debug.

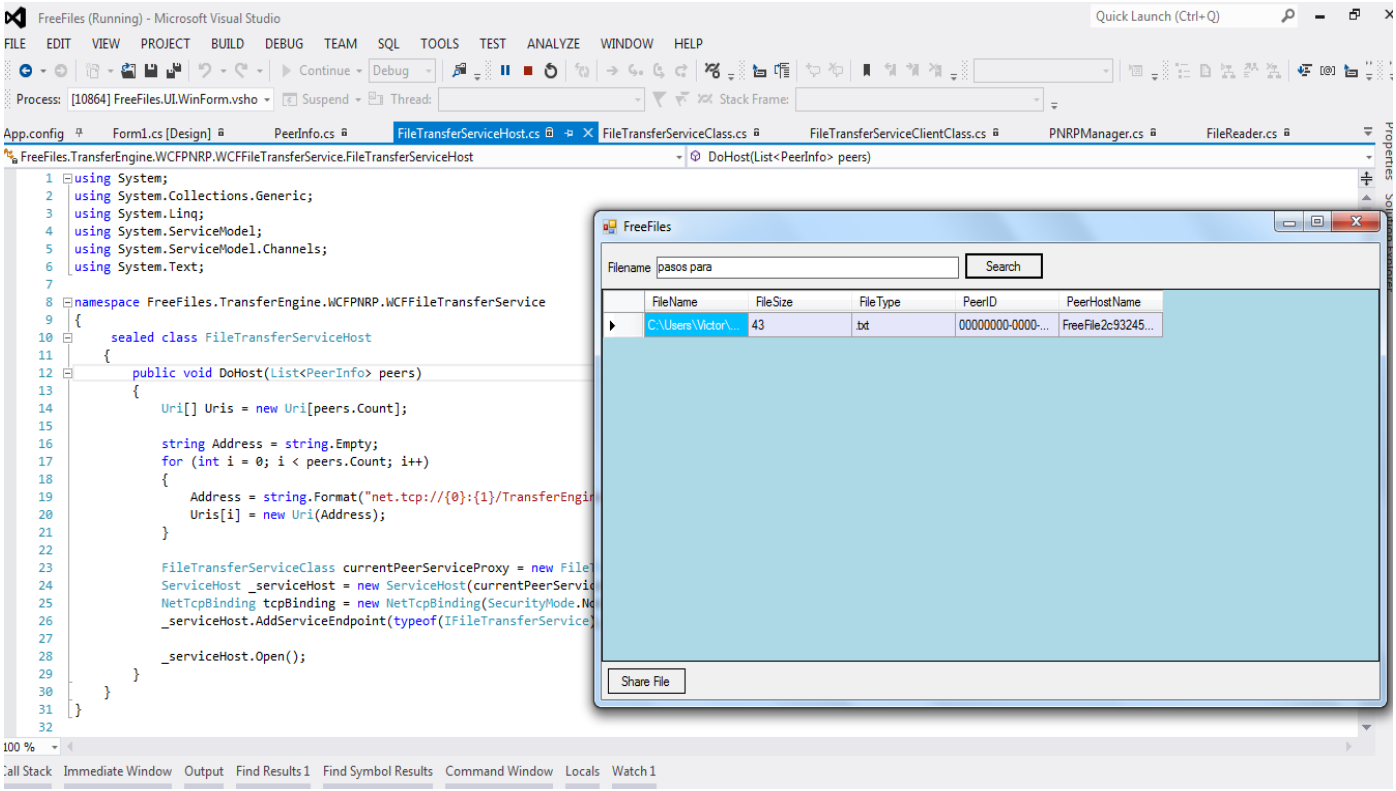


Figura 40. Aplicación corriendo desde el Debug

Luego se ha realizado el manual de usuario de la aplicación. La experiencia adquirida al desarrollar esta aplicación a permitido desarrollar una segunda aplicación.

Aplicación 2 - Chat para laboratorio de clase, bajo IPv6

Se generó una aplicación que además de permitir el envío de archivos añadiera otras funcionalidades. Planificada para ser utilizada en el laboratorio del GIDFIS inicialmente y luego se generó una solución pensada para su uso en los laboratorios de la Universidad.

Los usuarios se deben conectar a una red que tendrán en común el nombre de la red y el password, la variante estará en el nombre del usuario. La aplicación que posee el docente le permite: Escribir en el chat; Transmitir imágenes; Video con audio; Envío de archivos.

Esta aplicación podría ser utilizada tanto por el docente como por el alumno sin variantes, no obstante se realizó una versión resumida para alumnos que sólo permita recibir información, evitando así en alumnos de los primeros años que puedan darle un uso no académico a la herramienta. Tanto los alumnos como el docente pueden escribir en el chat, la información escrita le es enviada a toda la red.

En la figura 41 puede observarse como es la vista inicial de la aplicación con los controles configurados provistos por C4F Vista.

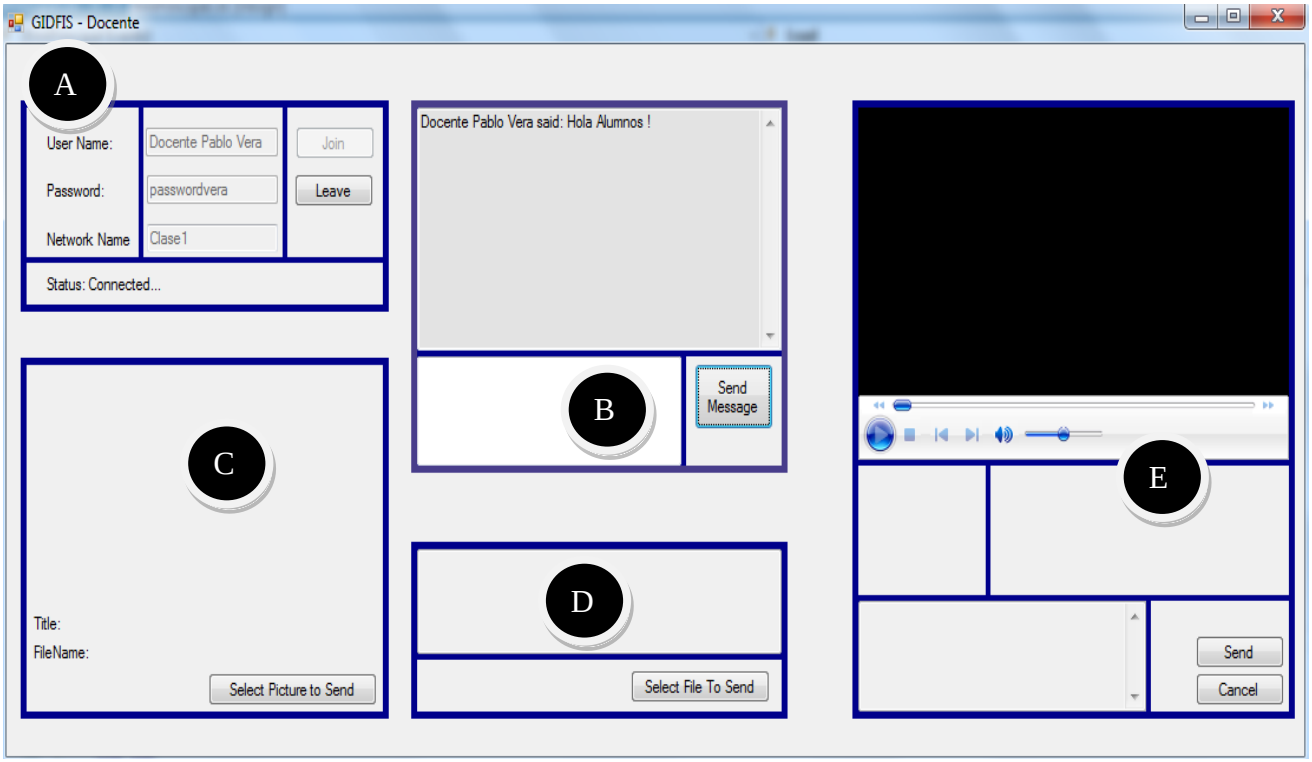


Figura 41. Aplicación desarrollada con C4F Vista

En la figura 41 pueden observarse diversos bloques, los cuales se describen a continuación:

A) Inicio de sesión del usuario en la red
B) Sección en donde se puede escribir a modo chat, lo escrito en el cuadro de texto en blanco se ve en la parte superior del control
C) Envío de Imagen una vez seleccionado el archivo la imagen que se envía se visualiza en este control
D) Selección de un archivo a enviar se muestra el nombre del archivo que se ha enviado en este control
E) Envío de un video el cual se reproduce arriba del control (utilizándose Windows Media Player)

Se muestra a continuación la captura desde la pantalla del docente (figura 42) en se ha utilizado el chat, se ha enviado una imagen y además luego un video para trabajar en la clase. La figura 43 muestra en ese mismo momento la vista del alumno del video, cada usuario puede pausar el video, de no hacerlo la reproducción en todas las máquinas es en tiempo real, no se registran retardos.

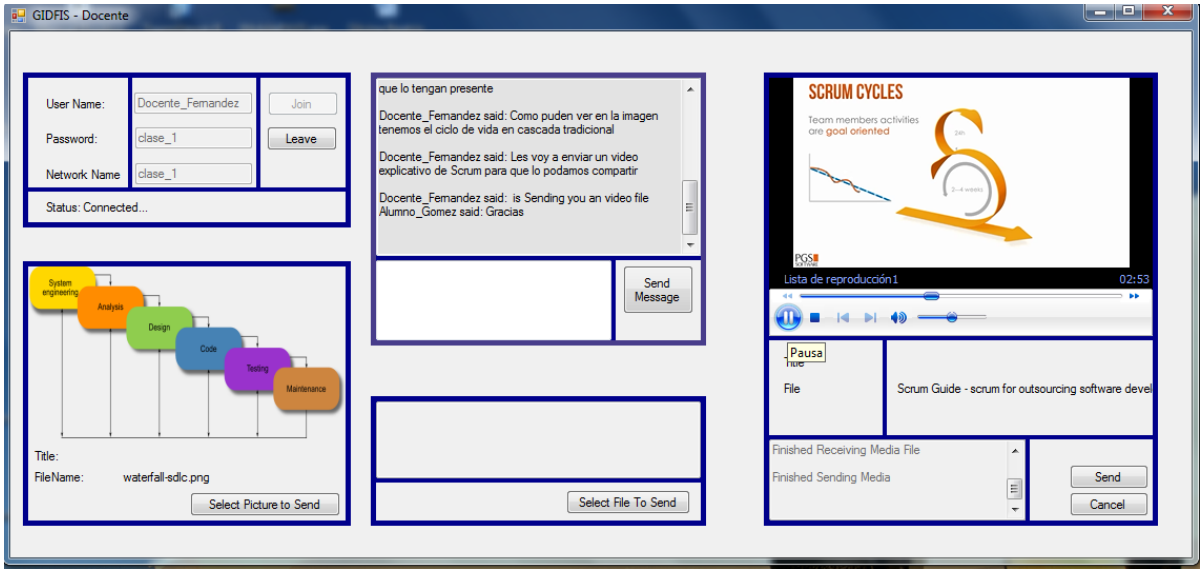


Figura 42. Aplicación desarrollada con C4F Vista

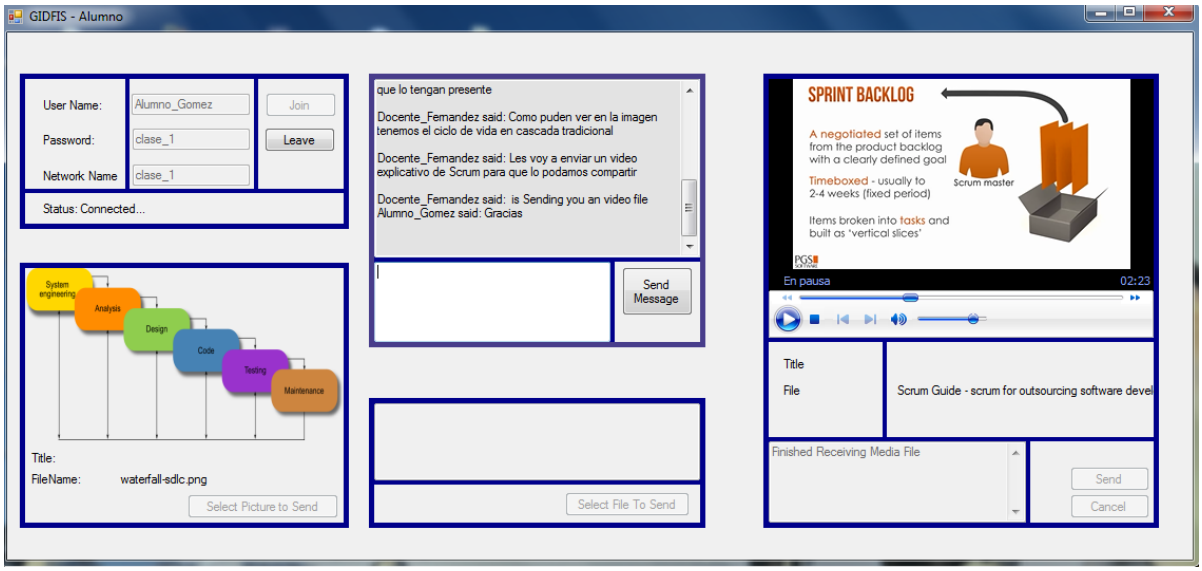


Figura 43. Aplicación desarrollada con C4F Vista

En esta aplicación fue importante el uso de C4F Vista. No obstante en la etapa de pruebas se evidenció un problema grave que hizo que se requiera modificar el código generado por la aplicación.

Problema encontrado en la etapa de pruebas:

Todas las pruebas en cuanto a funcionalidades funcionaron bien, se probó en primera instancia dentro del laboratorio del GIDFIS en 5 computadoras en simultáneo enviando contenidos y chateando. Antes de probar la aplicación en los laboratorios destinados a los alumnos, se analizó con un sniffer los paquetes que la aplicación enviaba y se detectó que C4F Vista no implementa en sus controles MULTICAST.

El analizador de paquetes utilizado fue Wireshark, en la figura 44 se muestra los paquetes capturados por Wireshark cuando se envía texto mediante la aplicación creada por el GIDFIS utilizando C4F Vista. Los paquetes IPv6 se envían a cada host conectado uno a uno. Esto se puede advertir observando al destino de cada paquete. Una pequeña prueba de 3 computadoras puede mostrar que los paquetes desde una máquina se envían a las dos restantes en forma individual siendo las direcciones:

- fe80::c11b:8faa:6d0c:86e5
- fe80::c098:2d9d:bc9a:c4e1

Si C4F Vista utilizara multicas la dirección destino debería ser fe02::1 correspondiente a todos los nodos conectados a la red.

Siendo Multicast una de las características más relevantes para este tipo de aplicación, se decidió modificar el código fuente generado logrando hacer uso de esta característica lo que redujo notablemente los tiempos.

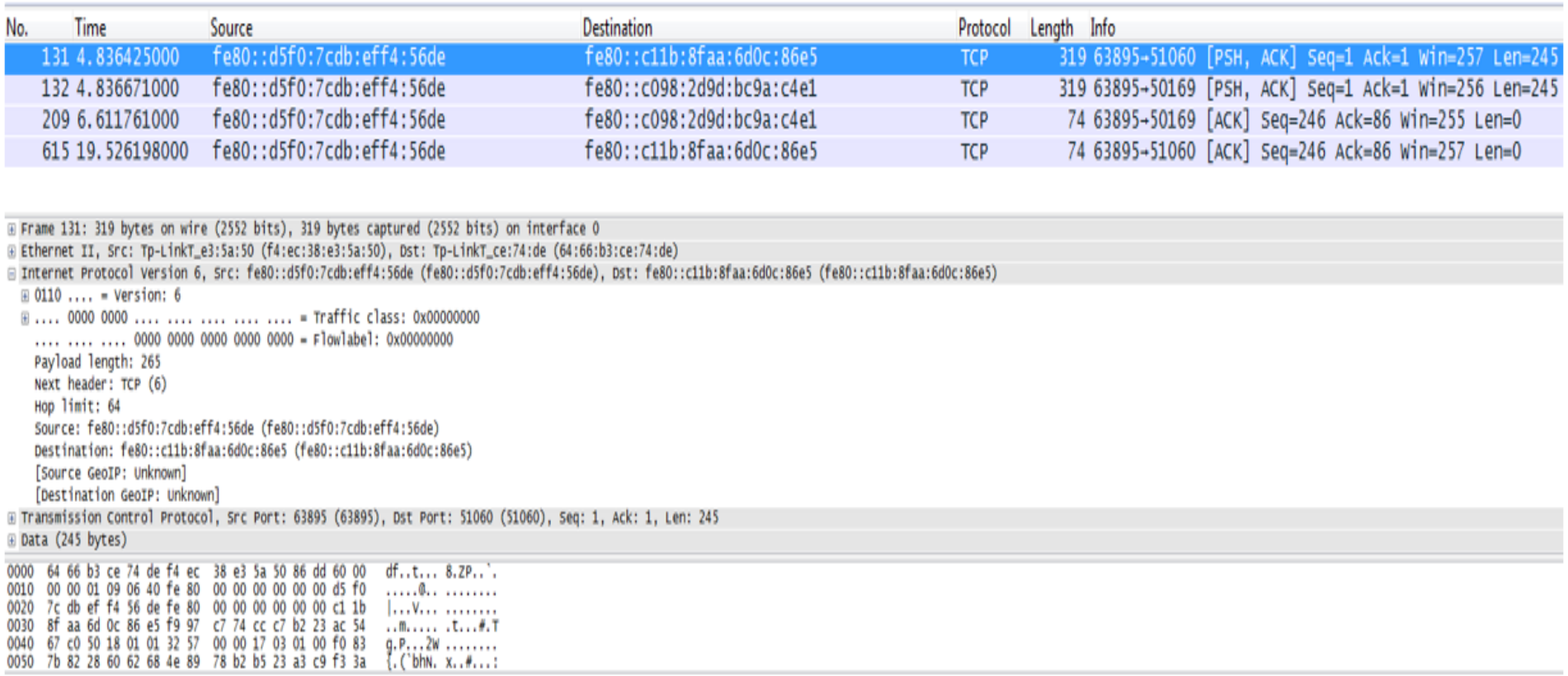


Figura 44. Análisis de los paquetes

3.4. Resultados

Los resultados de este proyecto de I+D (Investigación y Desarrollo) han tenido que ver por una parte con el conocimiento adquirido sobre el protocolo de IPv6 y otras tecnologías descriptas en el presente informe; pero por otra parte también la concreción de dos aplicaciones nativas para IPv6 relacionadas con el envío de archivos. La primera de ellas se ha generado en .NET (codificada en #C) tomando como base algunos ejemplos disponibles en internet y logrando una solución funcional la cual ha sido implementada en distintos ambientes y es utilizada actualmente en el laboratorio del GIDFIS. La segunda aplicación estuvo destinada inicialmente para el GIDFIS pero luego adaptada para el uso de laboratorios de la universidad destinados a clases, en donde el docente puede comunicarse con esta herramienta con los alumnos. Esta aplicación permitió trabajar con recursos más ricos (videos, audios, etc) integrados dentro del software construido, fue desarrollada íntegramente por el equipo de investigación utilizando C4F Vista y luego refinando la aplicación generada para que utilice Multicast.

En cuanto a la difusión de los resultados del proyecto se realizaron diversas publicaciones que son listadas en la sección siguiente del presente informe final.

4. Producción Científico-Tecnológica

A continuación se listan las actividades efectuadas en relación con la producción científica vinculada con el presente proyecto.

- Artículos Aprobados en Evento Académicos:
  1. Encouraging Students Participation in the Classroom by Taking Advance of Mobile Devices and Ad Hoc Networks. Rocío A. Rodríguez; Pablo M. Vera; Daniel Giulianelli; Federico Ezequiel Valles; Mariano Dogliotti; Gabriela Vallés, Graciela Cruzado. International Conference on Interactive Mobile Communication Technologies and Learning (IMCL 2014). Thessaloniki, Grecia. Noviembre 2014.

  2. Análisis de las Características del Protocolo de Red IPv6 que benefician a las Aplicaciones. Daniel Giulianelli, Rocío Rodríguez, Pablo Vera, M. Antonella

Cornejo, Víctor M. Fernández, Isabel Marko, Artemisa Trigueros. Workshop de Investigadores en Ciencias de la Computación (WICC 2014). Tierra del Fuego, Argentina. Mayo 2014.

3. Ambient Intelligence and Healthcare: Hybrid Network Approach based in IPv6. Carina González González; Alberto Mora Carreño, Daniel Giulianelli, Graciela Cruzado, Rocío Rodríguez. ISBN: 978.88.96.471.27.2 - DOI 10.978.8896471/272. International Conference on Software and Emerging Technologies for Education, Culture, Entertainment, and Commerce (SETECEC 2014). Venecia, Italia. Marzo 2014.

4. Native Development and Implementation of IPv6 - Experience in Argentina. Daniel A Giulianelli, Víctor M Fernández, Pablo M Vera, Rocío A Rodríguez, María A Cornejo, Pablo Cammarano, Graciela S. Cruzado. International Conference on Multimedia, Scientific Information and Visualization for Information Systems and Metrics (MSIVISM 2014). Maribou, Eslovenia. Enero 2014.

5. Desarrollo de Aplicaciones Nativas para Ipv6. Daniel Giulianelli, Rocío Rodríguez, Pablo Vera, María Antonella Cornejo. Workshop de Investigadores en Ciencias de la Computación (WICC 2013). Entre Ríos, Argentina. Abril 2013.

- Capítulo de libro – En edición

6. Título del Capítulo: Native Development and Implementation of IPv6 - Experience in Argentina.
   Editorial: IGI GLOBAL - 2015

- Seminario Realizado

7. Título del Seminario: IPv6
   Carácter: Actualización Tecnológica
   Duración: 2 horas
   Fecha: 28/06/2013
   Oradores: Rocío Andrea Rodríguez, Pablo Vera, Marcelo Caifa, María Antonella Cornejo y Pablo Cammarano
   Lugar: Universidad Nacional de La Matanza, Buenos Aires, Argentina

5. Conclusiones

De acuerdo con las aplicaciones disponibles y conectividad lograda concluimos que la adopción de IPV6 tiene que ser un hecho inminente llevado de la mano de hardware, fabricantes y software. Además de los proveedores de acceso, ya que brinda un direccionamiento que cubriría las expectativas del mercado en cuanto a dispositivos / equipos.

Por otro lado, hemos comprobado que:

- Los routers tienen menos trabajo para gestionar las IPs.
- Hay flexibilidad desde el mismo dispositivo de red
- La conexión es más rápida y tiempo de respuesta mucho menor

Con todas estas ventajas nos parece relevante desarrollar aplicaciones nativas para poder profundizar y afianzar el potencial de IPV6.

En cuanto al desarrollo es de destacar que los framework de desarrollo ya traen incorporadas algunas funciones de IPv6, tal como se mostró en este informe final para el caso de .NET. También C4F Vista permitió agilizar el desarrollo empleando controles predeterminados, el problema encontrado es que no utiliza MULTICAST, una de las ventajas de IPv6 en aplicaciones de envío de paquetes entre distintas computadoras. Esto pudo ser detectado gracias a las pruebas de los paquetes enviados por la solución generada mediante un Sniffer. Por ser esta una falencia muy importante hubo que dedicar bastante tiempo y esfuerzo en analizar el código generado de los controles predeterminados y poder realizar los cambios necesarios para implementar multicast. Es importante destacar este hecho porque si bien C4F Vista permitió agilizar el tiempo de desarrollo en componentes configurables que trae la herramienta, luego parte de ese tiempo ganado tuvo que ser dedicado a corregir una solución no conocida a fondo para poder aprovechar multicast.

El resultado final ha sido positivo ya que se ha avanzado en buen medida con el conocimiento de desarrollo nativo en IPv6 teniendo por resultado dos aplicaciones las cuales podrán ser aprovechadas no sólo por el grupo de investigación sino también en otros ambientes de trabajo dentro de la Universidad y compartidas con otras instituciones de forma gratuita.

6. Bibliografía

[ARI13] ARIU (Asociación Redes de Interconexión Universitaria). “Topología”. 2013. http://www.riu.edu.ar/topologia.html

[AZA07] AZAEL FERNANDEZ ALCANTARA. “Direcciones IPv4 ¿Recurso de Internet en Agotamiento?”. México, 2007 http://www.enterate.unam.mx/Articulos/2007/junio/art1.html

[C4F07] C4F Developer Kit. 2007. https://c4fdevkit.codeplex.com/

[CIL13] Cicileo Guillermo (2013). LACNIC (Latin America and Caribbean Network Information Centre). IPv6 en el Ambiente Académico. http://portalipv6.lacnic.net/es/ipv6/ipv6-en/ambiente-acad-mico-0

[CIS14] Cisco Systems 2014. CISCO IOS IPv6 Multicast Technologies. http://www.cisco.com/en/US/technologies/tk648/tk828/tk363/technologies_white_paper0900aecd8014d6dd.html

[CLA12] RED CLARA. “Proyectos” 2012 http://wiki-gtipv6.reuna.cl/wiki/index.php/PROYECTOS#.2A_Desarrollo_de_aplicaciones_con_soporte_IPv6._.28Programaci.C3.B3n_de_Sockets.29

[DAV12] DAVIES JOSEPH."Understanding IPv6: Your Essential Guide to IPv6 on Windows Networks". O´Reilly. Estados Unidos. 2012

[DIA13] Díaz Javier, Demasi Mauricio, Robles Matías, Vodopivec Germán, “Movilidad en IPv6”. 2013 http://sedici.unlp.edu.ar/bitstream/handle/10915/20873/Documento_completo.pdf?sequence=1

[DRA13] DRAYTEK. “Vigor 3200 Series Multi-WAN Security Router”. 2013 http://tw.draytek.com:13200/

[FER14] Fernandez Alcantara Azael (2007). Direcciones IPv4 ¿Recurso de Internet en Agotamiento? Enter@te. http://www.enterate.unam.mx/Articulos/2007/junio/art1.html

[ESP11] GOBIERNO DE ESPAÑA, Ministerio de Industria, Energía y Turismo. “IpV6 - Más direcciones para Comunicarnos Mejor”, España. 2011 http://www.ipv6.es

[GRI12] GRIDTICS (grupo de investigación y desarrollo en tecnologías de la información y comunicación / utn – frm). “IPV6 -Ya lo probamos, llego la hora de usarlo”. Argentina, Junio 2012. http://gridtics.frm.utn.edu.ar/site/?p=150

[INN12] INNOVA RED (Red Nacional de Investigación y Educación de Argentina). “Acceso IPV6”, 2012 http://www.innova-red.net/node/38

[LACne] LACNIC (Latin America and Caribbean Network Information Centre). CICILEO GUILLERMO. “IPv6 en el Ambiente Académico” http://portalipv6.lacnic.net/es/ipv6/ipv6-en/ambiente-acad-mico-0

[MEL09] Melero de la Torre Francisco. Javier, Bernardos Cano Carlos Jesús, “MOVILIDAD EN IPv6 CON HIP“, 2009 http://e-archivo.uc3m.es/bitstream/handle/10016/6104/Movilidad%20en%20IPv6%20con%20HIP%20-%20Memoria.pdf?sequence=1

[MIC14] Microsoft. Peer Name Resolution Protocol (PNRP) Version 4.0. 2014. http://download.microsoft.com/download/9/5/E/95EF66AF-9026-4BB0-A41D-A4F81802D92C/[MS-PNRP].pdf

[MOVne] “Movilidad IPv6”. Universidad Miguel Hernández. España http://redesdecomputadores.umh.es/ipv6/Movilidad.html

[MSD14a] MSDN Library. ¿Qué es Windows Communication Foundation? 2014 http://msdn.microsoft.com/es-es/library/vstudio/ms731082(v=vs.100).aspx

[MSD14b] MSDN Library. Peer-to-Peer Networking. 2014 http://msdn.microsoft.com/en-us/library/ms733761(v=vs.110).aspx

[MSD14c] MSDN Library. System.Net.PeerToPeer Namespace. 2014 http://msdn.microsoft.com/en-us/library/bb726971.aspx

[SAL11] Salcedo Parra Octavio José, López Danilo, Ríos Ángela Patricia, “Desempeño de la calidad del servicio (QoS) sobre IPv6”. 2011 http://www.scielo.org.co/scielo.php?pid=S0123-921X2011000100004&script=sci_arttext

[WIN06] Windows TechNet Library. Peer Name Resolution Protocol. 2006. http://technet.microsoft.com/en-us/library/bb726971.aspx

[3Cu13] Cu Electrónica. “Calidad de Servicio”. 2013. https://sites.google.com/site/3cuelectronica/home/ethernet/calidad-de-servicio