Prueba de conectividad y tiempo de respuesta del protocolo IPV6 en redes LAN

Yezid Enrique Donoso Meisel*,
Jorge Luis García**, Giancarlo Gianmaria**

Resumen

En las redes de computadores que hoy en día utilizan TCP/IP con IP versión 4 tendrán en pocos años el problema de ocupar en su totalidad el espacio de direcciones posibles. Este ha sido el motivo para que investigadores y empresas que tengan que ver con redes y comunicaciones estén analizando el diseño y desarrollo de una nueva versión de IP. Esta nueva versión de IP ha sido denominada IPv6, IPng o Fast IP. Entonces el IPv6, como lo denominaremos de ahora en adelante, nace como una posible solución a los problemas presentados y no resueltos en la versión IPv4.

Palabras clave: TCP/IP, IPv6, IPng, redes de computadores.

Fecha de recepción: 4 de septiembre de 2001

Abstract

In a few years, computer networks that are currently using TCP/IP with IP version 4 will have the problem of totally fulfilling the space of possible addresses. This has been the reason for researchers and enterprise related to networks and communication to analyze the design and development of a new IP version. This new version has been named Ipv6, IPng or Fast IP. Then, Ipv6, as we call it from now on, arises as a possible solution to the problems posed and not yet solved in Ipv4 version.

Key words: TCP / IP, IPv6, IPNG, computer networks

* Ingeniero de Sistemas, Universidad del Norte; Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Actualmente cursa Ph.D. Universidad de Girona, España. Coordinador Especialización en Redes de Computadores. Profesor del Departamento de Ingeniería de Sistemas de la Universidad del Norte. *(ydonoso@uninorte.edu.co)*

** Estudiantes de décimo semestre del programa de Ingeniería de Sistemas. Grupo de Redes de Computadores. Departamento de Sistemas y Computación, Universidad del Norte, Barranquilla, Colombia.

1. INTRODUCCIÓN

Analizando el desarrollo del protocolo IPv6 a nivel técnico y comercial, se plantea la necesidad de conocerlo y experimentarlo, ya que en un futuro no muy lejano será necesario cambiar a este protocolo, y la idea es que este cambio de IPv4 a IPv6 sea lo menos traumático posible para las empresas. El objetivo de este artículo es el presentar las especificaciones de conectividad que se realizaron tanto en una red de área local como en una red de área extensa a través de un par de dedicado entre enrutadores cisco. Además, se analizaron los tiempos de respuestas para transmisión de información y se compararon con los resultados presentados por el protocolo actual IPv4. Queremos resaltar la importancia que tiene el conocer este nuevo protocolo, para que cuando sea necesario realizar las actualizaciones respectivas el proceso sea bien conocido y no presente traumatismos para las redes actuales. Las pruebas se llevaron a cabo con estaciones Windows NT con el protocolo IPv6, switches Alcatel de segundo y tercer nivel sin soporte de IPv6, lo cual indica que el switcheo se realizaba en este caso por direcciones MAC, con hubs y con enrutadores Cisco, estos últimos sí presentaban la pila del protocolo IPv6, es decir que los enrutamientos se realizaban mediante el direccionamiento de este nuevo protocolo. Las pruebas en la red LAN se realizaron mediante un enrutador Cisco con dos puertos Ethernet y en el cual era necesario realizar enrutamientos por las subredes definidas.

2. DIRECIONAMIENTO EN IPV6

2.1. **Espacio de direcciones de IPv6**

La característica distintiva más evidente de IPv6 es el uso de direcciones mayores. El tamaño de una dirección en IPv6 es de 128 bits, cuatro veces mayor que el de una dirección de IPv4. El espacio de direcciones de 32 bits permite hasta 4.294.967.296 direcciones. Un espacio de direcciones de 128 bits permite hasta 340.282.266.920.938.463.463.374.607.431.768.211.465 (o $3{,}4 \times 10^{38}$) direcciones.

A finales de la década de los setenta, cuando se diseñó el espacio de direcciones de IPv4, era inimaginable que pudiera agotarse. Sin embargo, debido a los cambios tecnológicos y a una práctica de asignaciones en la que no se previó el reciente aumento del número de hosts en Internet, el espacio de direcciones de IPv4 se fue agotando hasta tal punto que en 1992 se hizo evidente la necesidad de un reemplazo.

Con IPv6 resulta aún más difícil concebir que el espacio de direcciones de IPv6 se vaya a consumir. Para tener una idea algo más aproximada de lo que supone este

número, un espacio de direcciones de 128 bits proporciona 655.570.793.348.866.943.898.599 ($6,5 \times 10^{23}$) direcciones por metro cuadrado de la superficie terrestre.

Ciertamente, la decisión de que la dirección de IPv6 tenga una longitud de 128 bits no obedece a que pueda haber hasta $6,5 \times 10^{23}$ direcciones por cada metro cuadrado de la Tierra. El tamaño relativamente grande de una dirección IPv6 se ha diseñado así para que se pueda subdividir en dominios de enrutamiento jerárquico que reflejen la topología de Internet actual. El uso de 128 bits permite varios niveles de jerarquía y ofrece flexibilidad para diseñar un enrutamiento y un direccionamiento jerárquico, algo que actualmente no ofrece la tecnología Internet basada en IPv4.

2.2. **Asignación actual**

De modo similar al que se utiliza para dividir el espacio de direcciones de IPv4, el espacio de direcciones de IPv6 se divide según el valor de los bits de orden superior. Los bits de orden superior y su valor fijo se conocen como prefijo de formato (FP, *Format Prefix*).

2.3. **Sintaxis de las direcciones de IPv6**

Las direcciones de IPv4 se representan en formato de notación decimal con puntos. Esta dirección de 32 bits se divide en límites de 8 bits. Cada conjunto de 8 bits se convierte en su equivalente decimal y está separado por puntos. Para IPv6, la dirección de 128 bits se divide en límites de 16 bits y cada bloque de 16 bits se convierte en un número hexadecimal de 4 dígitos y se separa con signos de dos puntos (:). La representación resultante se denomina hexadecimal con dos puntos.

A continuación se muestra una dirección IPv6 en formato binario:

0010000111011010100100001101001100000000010100000010111100111011

0000001010101010000000001111111111111110001010001001110001011010

Esta dirección de 128 bits se divide en límites de 16 bits:

0010000111011010 1001000011010011 0000000001010000 0010111100111011
0000001010101010 0000000011111111 1111111000101000 1001110001011010

Cada bloque de 16 bits se convierte en hexadecimal y está delimitado por signos de dos puntos (:). El resultado es: 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

La representación de IPv6 se puede simplificar aún más si se quitan los ceros a la izquierda de cada bloque de 16 bits. Sin embargo, cada bloque debe tener un dígito como mínimo. Al suprimir los ceros a la izquierda, la representación de la dirección se convierte en: 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A

2.4. Compresión de ceros

Algunos tipos de direcciones contienen largas secuencias de ceros. Para simplificar aún más la representación de direcciones de IPv6, una secuencia contigua de bloques de 16 bits establecida como 0 en formato hexadecimal con dos puntos se puede comprimir como «::».

Por ejemplo, la dirección local de vínculo de FE80:0:0:0:2AA:FF:FE9A:4CA2 se puede comprimir en FE80::2AA:FF:FE9A:4CA2. La dirección de multidifusión FF02:0:0:0:0:0:0:2 se puede comprimir en FF02::2.

La compresión de cero sólo se puede utilizar para comprimir una serie contigua de bloques de 16 bits expresada en notación hexadecimal con dos puntos. No se puede utilizar la compresión de ceros para incluir una parte de un bloque de 16 bits. Por ejemplo, no se puede expresar FF02:30:0:0:0:0:0:5 como FF02:3::5.

Para determinar cuántos bits 0 se representan mediante «::», puede contar el número de bloques de la dirección comprimida, restar ese número a 8 y multiplicar el resultado por 16. Por ejemplo, en la dirección FF02::2 hay dos bloques (el bloque «FF02» y el bloque «2»). El número de bits expresado por «::» es 96 (96 = (8 – 2),16).

La compresión de ceros sólo se puede utilizar una vez en una dirección dada. De lo contrario, no se podría determinar el número de bits 0 representados por cada instancia de «::».

- Prefijos IPv6

El prefijo es la parte de la dirección que indica los bits con valores fijos o los bits del identificador de red. Los prefijos para IPv6 se expresan del mismo modo que la notación de Enrutamiento entre dominios sin clase (CIDR, *Classless Inter-Domain Routing*) para IPv4. Un prefijo IPv6 se escribe con la notación *dirección/longitud de prefijo*. Por ejemplo, FE80::2AA:FF:FE9A:4CA2/64 indica que los primeros 64 bits de la dirección corresponden al prefijo de red. La notación de prefijo también se utiliza para expresar los identificadores de red o de subred. Por ejemplo, 21DA:D3::/48 es una subred.

Una dirección de nodo, con su prefijo, se puede utilizar para obtener el identificador de subred. Por ejemplo, el identificador de subred derivado de la dirección y el prefijo 21DA:D3:0:2F3B:2AA:FF:FE28:9C5A/64 es 21DA:D3:0:2F3B::/64.

Nota: Las implementaciones de IPv4 suelen utilizar una representación decimal con puntos del prefijo de red, que se conoce como máscara de subred. Para IPv6 no se utiliza la máscara de subred; sólo se admite la notación de longitud de prefijo.

2.5. **Direcciones de compatibilidad**

Para ayudar a la migración de IPv4 a IPv6 y a la coexistencia de ambos tipos de hosts, se definen las siguientes direcciones:

- *Dirección compatible con IPv4*

  La dirección compatible con IPv4, 0:0:0:0:0:0:w.x.y.z o ::w.x.y.z (donde *w.x.y.z* es la representación decimal con puntos de una dirección IPv4), es utilizada por nodos de doble pila que se comunican con IPv6 sobre una infraestructura de IPv4. Los nodos de doble pila son nodos con protocolos IPv4 e IPv6. Cuando se utiliza la dirección compatible con IPv4 como destino de IPv6, el tráfico de IPv6 se encapsula automáticamente con un encabezado de IPv4 y se envía al destino mediante la infraestructura de IPv4.

- *Dirección asignada de IPv4*

  La dirección asignada de IPv4, 0:0:0:0:0:FFFF:w.x.y.z o ::FFFF:w.x.y.z, se utiliza para representar un nodo que es sólo de IPv4 ante un nodo IPv6. Se utiliza únicamente para la representación interna. La dirección asignada de IPv4 nunca se utiliza como dirección de origen o de destino de un paquete IPv6.

2.6. **Direcciones IPv6 para un host**

Por lo general, un host IPv4 con un solo adaptador de red tiene una única dirección IPv4 asignada al adaptador. Sin embargo, un host IPv6 suele tener varias direcciones IPv6, incluso con una sola interfaz. A un host IPv6 se le asignan las siguientes direcciones de unidifusión:

- *Una dirección local de vínculo para cada interfaz.*

- *Direcciones de unidifusión para cada interfaz (que podrían ser una dirección local de sitio y una o varias direcciones de unidifusión global agregables).*

- *Una dirección de bucle de retroceso (::1).*

Un host IPv6 típico es multitarjeta (tiene varias interfaces o direcciones) porque tiene al menos dos direcciones con las que puede recibir paquetes (una dirección local de vínculo para el tráfico del vínculo local y una dirección agregable o local de sitio que se puede enrutar).

Además, cada host escucha el tráfico en las siguientes direcciones de multidifusión:

- *La dirección de multidifusión de todos los nodos del ámbito local de nodo (FF01::1).*
- *La dirección de multidifusión de todos los nodos del ámbito local de vínculo (FF02::1).*
- *La dirección de nodo solicitado para cada dirección de unidifusión.*
- *Las direcciones de multidifusión de los grupos unidos.*

2.7. **Direcciones IPv6 para un enrutador**

A un enrutador IPv6 se le asignan las siguientes direcciones de unidifusión:

- *Una dirección local de vínculo para cada interfaz.*
- *Direcciones de unidifusión para cada interfaz (que podrían ser una dirección local de sitio y una o varias direcciones de unidifusión global agregables).*
- *Una dirección para cualquier difusión de Subred-Enrutador.*
- *Direcciones adicionales para cualquier difusión (opcional).*
- *Una dirección de bucle de retroceso (::1).*

Además, cada enrutador escucha el tráfico en las siguientes direcciones de multidifusión:

- *La dirección de multidifusión de todos los nodos del ámbito local de nodo (FF01::1).*
- *La dirección de multidifusión de todos los enrutadores del ámbito local de nodo (FF01::2).*
- *La dirección de multidifusión de todos los nodos del ámbito local de vínculo (FF02::1).*
- *La dirección de multidifusión de todos los enrutadores del ámbito local de vínculo (FF02::1).*
- *La dirección de multidifusión de todos los enrutadores del ámbito local de sitio (FF05::2).*
- *La dirección de nodo solicitado para cada dirección de unidifusión.*

- *Las direcciones de multidifusión de los grupos unidos.*

Para este proyecto nosotros utilizamos el esquema de prefijo con el valor de 64., es decir que los primeros 64 bits identifican a la red y los último 64 bits identifican a la interface.

3. ESPECIFICACIÓN Y CONFIGURACIÓN DE LA CONECTIVIDAD

Esta prueba la hemos realizado en los equipos Windows NT Server con la versión binaria de Microsoft MRIPV6 , la cual se puede obtener de *http://research.microsoft.com/msripv6*. Acto seguido se dispone a instalar el *software*.

En primer lugar se ejecuta el icono de red en el panel de control (otra manera de hacerlo es ingresar a través del entorno de red, se hace *clic* derecho y se elige «propiedades») y se elige la opción de «protocolos», haga *clic* en el botón de «Agregar», al aparecer el siguiente cuadro de diálogo, elija «Utilizar Disco».

Cuando pida el disco, se debe escribir el camino completo, donde se encuentra el archivo que contiene el instalador del Kit de distribución (Por ejemplo: C:\Ipv6kit). Entonces el kit se instalará por sí mismo.

La instalación procederá a copiar los archivos desde el kit de instalación hasta los lugares apropiados y en el registro del sistema para la configuración del Ipv6. Si posteriormente se modifican los componentes del IPv6, se pueden reemplazar sólo los programas afectados sin necesidad alguna de desinstalar y reinstalar el protocolo otra vez. La pila de información del protocolo (tcpip6.sys) estará instalada en el directorio «Windows\System32\drivers» y todas las aplicaciones de usuarios (ipv6.exe, ping6.exe, tracert6.exe, ttcp.exe, etc.) así como las librerías dinámicas de la familia de direcciones INET6 estarán ubicadas en el directorio «Windows\System32».

Estas son algunas de las utilidades que se utilizaron en las primeras pruebas del protocolo IPv6:

- **net.exe**

El comando net.exe puede ser utilizado para iniciar o detener la pila de información del IPv6. Reiniciar la pila del IPv6 significa comenzar todo nuevamente, como si la máquina se hubiera apagado. Note que los números de la interfase pueden cambiar cuando el servicio se reinicie, debido a que el asigna un nombre al azar para cada una de las interfaces.

Los subcomandos más importantes y sólo relevantes al IPv6 son los siguientes:

- net stop tcpip6

Detiene los servicios del protocolo IPv6 y lo descarga de memoria. Este comando falla si hay algún socket IPv6 abierto.

- net start tcpip6

Inicia la pila IPv6 si fue detenida. Si un nuevo archivo tcpip6.sys está presente en el directorio «C.\Windows\System32\drivers», este nuevo archivo es utilizado.

El uso de este comando con las palabras *net start* solamente ocasiona que se arroje la información sobre servicios de red activos.

- **ipv6.exe**

Con excepción de IPsec (programa de seguridad), todas las configuraciones del MSR IPv6 son hechas con el comando IPv6. Entre otras cosas, también es usado para consultas y configurar interfaces, direcciones, y rutas.

El comando ipv6.exe tiene numerosos subcomandos. Cada subcomando tiene su propio conjunto de argumentos y opciones.

- ipv6 if [if#]

Despliega información acerca de las interfaces. Si un número de interface es especificado, sólo despliega información sobre ella, si no, muestra los datos de todas las interfaces. La salida que presenta incluye la dirección de la interface de la capa de enlace y la lista de direcciones IPv6 asignadas a la interface. Incluye el MTU actual de la interfaz, y la «verdadera» o máxima MTU que la interfaz puede soportar.

Interface #1 es una seudo-interfaz usada para el loopback.

Interface #2 es una seudo-interfaz utilizada para el tunelaje configurado, automático y tunelaje 6to4.

Las otras interfaces son numeradas secuencialmente en el orden en el que son creados; este orden varía de máquina a máquina.

Si la dirección de la capa de enlace es de la forma aa-bb-cc-dd-ee-ff, entonces es una interfaz Ethernet o FDDI. Si la dirección es de la forma a,b,c,d, entonces es una interfaz Carpenter/Jung 6-over-4.

Las dos seudo-interfaces no utilizan ninguna característica de descubrimiento de entorno.

El comando ipv6 adu if#/address [lifetime VL[/PL]] [anycast] [unicast] adiciona o remueve una asignación de una dirección unicast o anycast sobre una interfaz. Por defecto toma unicast a menos que la opción anycast sea especificada.

Si la opción lifetime no es especificada, se convierte en infinita. Si solamente un valor valido es especificado, entonces el lifetime escogido es igual al seleccionado. Se puede seleccionar un valor de infinite, o un valor en segundos, el valor debe ser menor o igual que el lifetime ya establecido. Especificar un lifetime de cero causa que la dirección sea removida.

Lifetime puede ser abreviada como life

Para direcciones anycast, los únicos valores válidos son cero o infinito.

- ipv6 rt

Despliega los contenidos actuales de la tabla de ruteo.

ipv6 rtu prefix if#[/nexthop] [lifetime L] [preference P] [publish] [age] [spl site-prefix-length]

Adiciona o remueve una ruta de la tabla de ruteo.

- **Ping6.exe**

Es el comando ping de la versión IPv6 instalada en los NT.

- **Tracert6.exe**

Este comando rastrea la ruta que un paquete Ipv6 tiene que seguir para llegar a la dirección indicada

Tracert6 address

4. PRUEBAS DE CONECTIVIDAD

A continuación se mostrarán las pruebas de conectividad que se llevaron a cabo.

4.1. **Conexión a través de un Hub**

La primera prueba que se realizó fue a través de un Hub, como se muestra en la figura1:

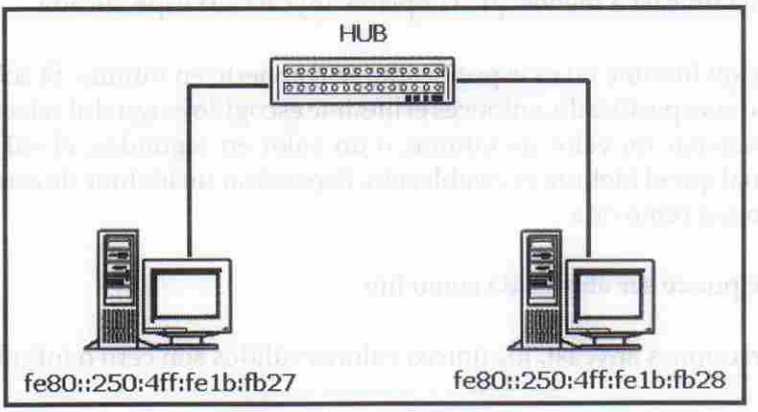


Figura 1. Conexión IPv6 a través de un HUB

En este caso, el objetivo fue probar el *software* de IPv6 de los equipos Windows NT Server. Las direcciones IPv6 que se utilizaron en los equipos se muestran en la figura 1.

La forma de configurarlas fue la siguiente:

ipv6 adu 4/fe80::250:4ff:fe1b:fb27 En la terminal 1

ipv6 adu 4/ fe80::250:4ff:fe1b:fb27 En la terminal 2

4.2. **Conexión IPv6 LAN con Subredes a través de un Enrutador**

La siguiente prueba que se realizó fue a través de dos puertos Lan en un enrutador Cisco 2611; para esto, primero se procedió a configurar las direcciones Ipv6 en el enrutador creando una configuración de subredes, que se aprovechó para esta medición. Las direcciones otorgadas a los puertos Lan fueron las siguientes:

Puerto Ethernet 0/0: 12AB::2:0:0:0:1/64

Puerto Ethernet 0/1: 12AB::1:0:0:0:2/64

Para esta configuración se tomó un prefijo Ipv6 de 64, es decir, 64 bits para la identificación de subredes, quedando el resto de bits para los nodos, el proceso de asignación se hizo mediante el siguiente procedimiento:

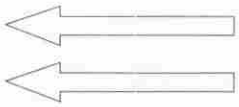
```
Ipv6 enable
Ipv6 route 12AB::2:0:0:0:1/64 Serial0/0
```

De esta manera queda configurado el puerto 0/0 del enrutador. De acuerdo con esto se trabajó el otro de manera análoga, especificando el puerto 0/1 y la dirección 12AB::1:0:0:0:2/64 correspondiente a la segunda subred.

Las dos configuraciones se pueden constatar mediante el comando *show ipv6 route*, en el cual nos muestra las tablas de enrutamiento de la direcciones Ipv6 de la siguiente manera:

```
sh ipv6 route local

L 0::11.0.0.10/128 [0/0]
  via 0::11.0.0.10, Null0, 18:03:20/never
L 12AB::1:0:0:0:2/128 [0/0]
  via 12AB::1:0:0:0:2, Ethernet0/1, 01:49:43/never
L 12AB::2:0:0:0:1/128 [0/0]
  via 12AB::2:0:0:0:1, Ethernet0/0, 18:03:23/never
L 12AB::3:0:0:0:1/128 [0/0]
  via 12AB::3:0:0:0:1, Serial0/0, 18:03:17/never
L FE80::0/64 [0/0]
  via 0::0, Null0, 18:03:23/never
```



Le añadimos la opción *local* porque sólo nos interesa saber las configuraciones locales.

Posterior a este procedimiento se configuraron las terminales NT para que hicieran parte de las dos subredes que estaban funcionando ya en el enrutador; para esto se asignaron las siguientes direcciones:

Terminal 1 (en la subred 1): 12AB::1:0:0:0:11/64

Terminal 2 (en la subred 2): 12AB::2:0:0:0:12/64

Estas direcciones fueron asignadas utilizando la instrucción *ipv6* (anteriormente expuesta) junto con la opción *adu*, de la siguiente manera:

ipv6 adu 4/12AB::1:0:0:0:11 En la terminal 1

ipv6 adu 4/12AB::2:0:0:0:12 En la terminal 2

Especificando la interfaz 4 en el comando, ya que las otras interfaces son utilizadas para loopback y configuración.

Podemos asegurarnos de que la asignación fue tomada por el protocolo consultándola con el siguiente comando: Ipv6 if 4

Al finalizar procedimos a configurar las rutas de la red por medio de la opción rtu del comando *ipv6*, de la siguiente manera: ipv6 rtu 12ab::1:0:0:0:11/64 4/12ab::2:0:0:0:1

Lo cual significa que cualquier información que vaya a la dirección 12ab::1:0:0:0:11 debe pasar por 12ab::2:0:0:0:1.

En la figura 2 se muestra la configuración de la conexión IPv6 a través del enrutador en los dos puertos Ethernet.

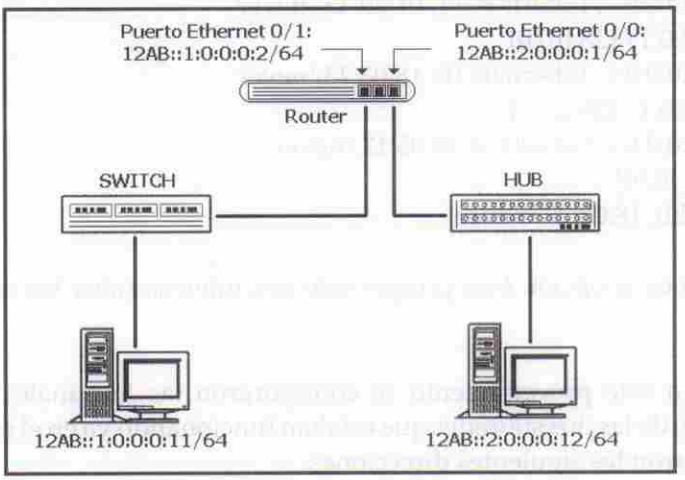


Figura 2. Conexión IPv6 a través de un ENRUTADOR
Conexión entre dos puertos LAN de un enrutador

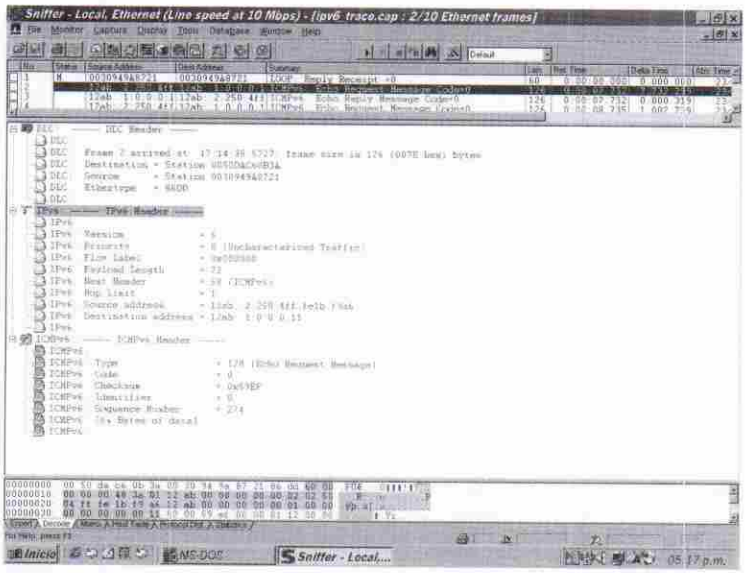
5. ANÁLISIS DE LA SOLUCIÓN PLANTEADA

Bajo el concepto de tiempo de respuesta se compararon las diferencias entre Ipv6 e Ipv4 en cuanto a envío y respuesta de paquetes de diferente tamaños, utilizando los comandos *ping* y *ping6*, con las respectivas direcciones en la misma estructura de red. A continuación presentamos los resultados obtenidos al medir los tiempos entre los dos host, 12ab::2:0:0:0:12 y 12ab::1:0:0:0:11, a través del enrutador Cisco.

Número de bytes	*IPv6*	*IPv4*
32	Entre 4 y 6 milisegundos	Menos de 10 milisegundos*
64	Entre 5 y 6 milisegundos	Menos de 10 milisegundos*
128	Entre 6 y 7 milisegundos	Menos de 10 milisegundos*
256	Entre 6 y 8 milisegundos	Menos de 10 milisegundos*
512	Entre 5 y 7 milisegundos	Menos de 10 milisegundos*
1.500	Entre 13 y 14 milisegundos	10 milisegundos
10.000	Entre 28 y 29 milisegundos	20 milisegundos
64.000	Entre 126 y 127 milisegundo	110 milisegundos

* No especificado (el comando *ping* arrojó <10ms).

Además, también realizamos un análisis de trama por medio de un sniffer para entender lo que IPv6 está enviando como información y a continuación mostramos un ejemplo de un mensaje ICMPv6 capturado por un sniffer en las pruebas realizadas.



CONCLUSIONES

Podemos mencionar como conclusiones lo siguiente:

- La importancia que presenta IPv6 como un protocolo con gran cantidad de direcciones disponibles, manejo de calidad de servicio y manejo de seguridad entre otros aspectos.

- La importancia de conocer y probar la configuración de IPv6 tanto en redes LAN como en redes WAN, para que cuando venga el momento de la transición, ésta no sea traumática para las organizaciones.

- La compatibilidad que presenta IPv6 con otras soluciones en el área de las redes actuales tales como: Calidad de servicio (QoS), MPLS (Multiprotocol Label Switching), Multicasting (Multidifusión), Traffic Engineering.

- La importancia de experimentar con enrutadores de marcas importantes tales como Cisco, los cuales están marcando la pauta en los mercados internacionales en el tema de las redes de datos y su conectividad con tecnologías tales como IPv6.

Referencias

Sitio Web de Microsoft. http://research.microsoft.com/msripv6. Junio 2001.
Sitio Web de IPv6. htttp://playground.sun.com/ipv6/. Junio 2001.