ISSN 0041-8811
DEPÓSITO LEGAL pp 76-634

Revista de la Universidad del Zulia

Fundada en 1947
por el Dr. Jesús Enrique Lossada

Ciencias Exactas Naturales y de la Salud

65 Aniversario

Año 3 N° 6
Mayo - Agosto 2012
Tercera Época
Maracaibo- Venezuela

Revista de la Universidad del Zulia. 3ª época.
Ciencias Exactas, Naturales y de la Salud///
Año 3 N° 6, Myo-Agst 2012, 9 - 30
ISSN 0041-8811 - Depósito legal pp 76 - 654

Calidad de servicio entre sistemas autónomos con enlaces a 5.7 GHz y servicios de última milla inalámbricos con el uso de IPv6.

Alfredo Acurero[1]
David Bracho[1]
Carlos Rincón[1]
Jianfeng Wu[2]

RESUMEN

El estudio de conectividad inalámbrica entre Sistemas Autónomos no ha sido muy explorado, por lo que se busca asociar el nuevo protocolo de direccionamiento IPv6 con dicha problemática. Consecuentemente, se analizó el comportamiento del protocolo IPv6 en Sistemas Autónomos conectados por enlaces de 5.7 GHz usando parámetros de medición de Calidad de Servicio (QoS) y nodos móviles en los extremos. Aplicando los principios de Bisquerra (2000), la metodología constó de cuatro (4) fases: recopilación de información, diseño de topologías de pruebas, rutinas de medición y recopilación de los resultados y análisis estadístico. Del análisis-comparativo entre el protocolo IPv6 e IPv4 se desprende que IPv6 presentó en general un menor desempeño frente a IPv4, pero mediante el uso del método estadístico ANOVA se concluye que a causas de diferencias no considerables, IPv6 no influye significativamente en el rendimiento, considerando factible su uso en una red con las características estudiadas.

Palabras clave: IPv6, BGP, QoS, 802.11a

[1] Departamento de Computación, Facultad Experimental de Ciencias, Universidad del Zulia. E-mail: aacurero@fec.luz.edu.ve
[2] Licenciatura en Computación, Facultad Experimental de Ciencias, Universidad del Zulia.

Recibido: 15/10/2012 Aceptado: 17/01/2013

Quality of Service between autonomous systems with links at 5.7 GHz and last mile wireless services by using IPv6.

ABSTRACT

Nowadays, the study of wireless connectivity between Autonomous Systems has not been explored widely, therefore is sought to relate the new addressing protocol IPv6 with this problem. Consequently, the objective of this research was to analyze the behavior of IPv6 Autonomous Systems connected by links of 5.7 GHz using QoS metrics and mobile nodes. Applying the principles of Bisquerra (2000), methodology was established in four (4) phases divided into: information compilation, topology design and / or test environments, test data collection and measurement of results and, treatment and statistical analysis of the data. The results of the comparative analysis between IPv6 and IPv4 in this network environment, showed that IPv6 generally has a lower performance compared to IPv4, but also through the use of ANOVA statistical method it is concluded that dues to irrelevant differences, IPv6 does not influence the performance of a network with the studied features significantly.

KEYWORDS: IPV6, BGP, QOS, 802.11A

Introducción

El crecimiento exponencial de Internet está llevando hacia el agotamiento de las direcciones IPv4, es decir a la progresiva merma de la cantidad de direcciones IPv4 disponibles. Como consecuencia, este crecimiento desmesurado se ha convertido en el factor impulsor en la creación y adopción de diversas nuevas tecnologías, incluidas las direcciones CIDR (Classless Inter-Domain Routing, en inglés) y NAT (Network Address Translation, en inglés) como soluciones a corto plazo, mientras que el IPv6 se ve como un remedio a largo plazo para el agotamiento de las direcciones IPv4 (Bagnulo, 2004).

El nuevo protocolo, no sólo ofrece un espacio mayor de direcciones, sino que además mejora o soluciona algunos problemas de su antecesor IPv4, tales como Direccionamiento público a cada dispositivo conectado a Internet, Movilidad basado en IPv6 (MIPv6) y mayor nivel de Seguridad (IPsec) por defecto (Díaz et al, 2007).

Estas nuevas características de IPv6 permiten dar mayor confiabilidad a las redes inalámbricas. Por lo tanto, su implementación se extiende hasta las redes a gran escala como el caso de los Sistemas Autónomos, que según Fabero (2008), son comúnmente los Proveedores de Servicios de Internet (ISP, por sus siglas en inglés) de un país, organizaciones trasnacionales e instituciones de gran flujo de datos en sus redes, y que por razones geográficas no siempre puede enlazarse con medios alámbricos.

Actualmente, los Sistemas Autónomos se comunican entre sí bajo el protocolo IPv4 y BGP (Border Gateway Protocol, en inglés), el cual es un protocolo de enrutamiento externo que comunica enrutadores de diferentes sistemas autónomos (Cisco Systems, 2012). Sin embargo, la gran madurez que está experimentando últimamente IPv6, obliga que los Sistemas Autónomos lo implementen lo más rápido posible. Además, debido a la diferencia del tamaño de la cabecera de los paquetes entre el protocolo Ipv4 e IPv6 se hace notable el estudio comparativo en este ambiente de los Sistemas Autónomos, especialmente en enlaces inalámbricos donde se ha comprobado que se obtienen notables pérdidas de señal con respecto a los enlaces cableados (Flickenger, 2006).

Una de las motivaciones principales de este estudio radica en que "…mientras más tiempo se deje pasar en empezar a habilitar y probar IPv6, mayores serán los costos en inversión en aspectos como actualizaciones en Humanware, software y hardware; aunque se estima que los precios más altos en la transición a IPv6 ocurrirán con el entrenamiento y no con el software" (Fernández, 2007, s/p).

Además, la implementación de este protocolo IPv6 resuelve ampliamente las deficiencias nativas del IPv4, tanto a nivel de seguridad como movilidad, sin olvidar de la solución que daría IPv6 al problema del agotamiento de direcciones IP. Con esto, se permitiría la incorporación de nuevos dispositivos que tendrán direcciones IP públicas sin ningún inconveniente, logrando que estos aparatos se comuniquen entre sí sin restricciones de redes privadas del NAT. (Millán, 2012)

Sin embargo, en la actualidad existe muy poco material sobre el estudio de conectividad inalámbrica entre Sistemas Autónomos tanto en la Web como los libros textuales. Por lo tanto, se buscó con esta investigación ofrecer a estos sistemas las grandes ventajas del enlace no cableado, de las cuales cabe destacar que el vínculo inalámbrico puede ser un reemplazo idóneo para aquellas situaciones que el cableado es imposible de implementar.

Además la frecuencia 5.7 Ghz es una frecuencia autorizada sin licencia y muy poco usada ya que en el mercado disponen principalmente de dispositivos inalámbricos de frecuencia 2.4 Ghz, por lo que se puede obtener mayores beneficios tales como la casi inexistencia de interferencia de dispositivos operativos en el nivel del espectro 5.7 Ghz, logrando una mejor distribución y aprovechamiento de aparatos inalámbricos.

De esta forma, con el problema antes descrito, fue necesario desarrollar un esquema para medir el rendimiento de una red con políticas de Calidad de Servicio, en Sistemas Autónomos bajo BGP conectadas inalámbricamente a 5.7 Ghz y nodos móviles en los extremos usando el protocolo emergente IPv6, a fin de verificar la estabilidad del enlace a esa frecuencia, estudiando, entre otros aspectos, la relación de las características del nuevo protocolo con respecto a las pérdidas asociadas a enlaces de este tipo.

1. Aspectos teóricos

1.1. Protocolo de Internet versión 6 (IPv6)

Díaz y colaboradores (2007) manifiestan que IPv6 es la nueva versión del protocolo de Internet, que es básico para el funcionamiento de la Red y cuyas primeras especificaciones fueron desarrolladas por Internet Engineering Task Force (IETF) en los años noventa. La motivación principal de la transición al nuevo protocolo es la expansión de las direcciones públicas disponibles de Internet, que permitirá la conexión a la Red de múltiples dispositivos como PDAs y teléfonos móviles. Otro factor clave para la adopción del nuevo protocolo es la expansión del uso de las tecnologías basadas en el concepto 'always-on' o siempre conectados como DSL, cable, Ethernet hasta la casa, fibra óptica, PLC, entre otros.

Las ventajas de IPv6 son, además de un mayor espacio para las direcciones, la escalabilidad, ya que ha sido diseñado para crecer sin los límites y parches de IPv4; una seguridad implícita, pues IPsec es obligatorio como parte del protocolo; y la movilidad, ya que facilita la nueva generación de aplicaciones (Millán, 2012), teniendo cabida en la creciente movilidad de los usuarios de Internet y las redes domésticas con avanzados sistemas de televigilancia, control, y seguridad, entre otros.

Entre sus aspectos más importantes está un mayor espacio de direcciones, paquetes eficientes y extensibles, renumeración y multihoming (que facilita el cambio de proveedor de servicios), movilidad, calidad de servicio y clases de servicios, seguridad, auto configuración de los nodos, aplicaciones anycast y multicast, Wireless, End to end (no usa NAT).

1.2. Calidad de Servicio

La calidad de servicio (QoS, por sus siglas en inglés) se encarga de proveer un nivel de servicio para que las diferentes aplicaciones que usen la red se puedan beneficiar de ella de manera apropiada, y ya que no todas las aplicaciones tienen los mismos niveles de exigencia de la red, busca asignar a cada una la exigencia que requiera. Al utilizar la calidad de servicio, distintas aplicaciones de red pueden coexistir en la misma red sin consumir cada una el ancho de banda de las otras (Certain, 2009).

Según Álvarez (2005), cada red puede tomar ventaja de distintos aspectos en implementaciones de QoS para obtener una mayor eficiencia, ya sea para redes de pequeñas corporaciones, empresas o proveedores de servicios de Internet.

En términos generales, explica el mismo autor que puede definirse la Calidad del Servicio (QoS) como la capacidad que tiene un sistema de asegurar, con un grado de fiabilidad preestablecido, que se cumplan los requisitos de tráfico, en términos de perfil y ancho de banda, para un flujo de información dado.

1.3. Estándar WLAN 802.11a

La norma IEEE 802.11 es un estándar en continua evolución, por lo que ha sufrido varias modificaciones y extensiones a lo largo de su corta vida, y es por ello que aún hoy en día van apareciendo nuevas especificaciones. Este estándar no especifica una tecnología o implementación concretas, sino simplemente el nivel físico y el subnivel de control de acceso al medio (MAC), siguiendo la arquitectura de sistemas abiertos OSI/ISO.

802.11a: La revisión 802.11a al estándar original fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 GHz y utiliza

52 subportadoras por multiplexación por división de frecuencias ortogonal (OFDM, por sus siglas en inglés) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s.La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

1.4. Sistemas autónomos

Según Goitia (2003), un sistema autónomo (SA) será la subred que es administrada por una autoridad común, que tiene un protocolo de ruteo homogéneo mediante el cual intercambia información en toda la subred y que posee una política común para el intercambio de tráfico con otras redes o sistemas autónomos. En Internet se dan, al menos, dos niveles jerárquicos de ruteo, el que realiza dentro de un sistema autónomo y el que se efectúa entre sistemas autónomos.

Habitualmente, el SA es visto como una única entidad. Cada SA tiene un número identificador de 16 bits, que se le asigna mediante un Registro de Internet (como RIPE, ARIN, o APNIC), o un proveedor de servicios en el caso de los SA privados. Así, se consigue dividir el mundo en distintas administraciones, con la capacidad de tener una gran red dividida en redes más pequeñas y manipulables. Existen casos de que se junten varios SA, cada uno de estas asociaciones utilizará un router de gama alta que llamaremos router fronterizo, cuya función principal es intercambiar tráfico e información de rutas con los distintos routers fronterizos. Así, un concepto importante de comprender es el tráfico de tránsito, que no es más que todo tráfico que entra en un SA con un origen y destino distinto al SA local.

1.5. Protocolo de Enrutamiento de Pasarela Frontero: BGP

Goitia (2003), menciona que dentro de un solo SA, el protocolo de enrutamiento recomendado en Internet es el OSPF (aunque no es el único en uso). Entre los SA se usa un protocolo diferente, el BGP (Border Gateway Protocol o protocolo de pasarela frontera). Se requiere un protocolo diferente entre los SA, ya que las metas de un protocolo de pasarela interior y un protocolo de pasarela exterior no son iguales.

Es por eso que Stallings (2004) explica que el protocolo de pasarela de frontera (BGP) se desarrolló para su uso en conjunción con interconexiones en redes que empleen la arquitectura de protocolo TCP/IP, aunque los conceptos son aplicables a cualquier interconexión de redes. El protocolo de pasarela frontera se ha convertido en el protocolo de dispositivo de enrutamiento exterior preferido para Internet, diseñado para permitir la cooperación en el intercambio de información de enrutamiento entre dispositivos de enrutamiento de diferentes sistemas autónomos (SA), llamado pasarelas en el estándar.

2. Metodología utilizada

Para determinar cómo influye el protocolo Ipv6 con QoS en Sistemas Autónomos conectados por Enlace Inalámbrico a 5.7 Ghz, en esta investigación se siguió la metodología de Bisquerra (2000) que se describe a través de las siguientes fases:

Fase I: Recopilación de información

Para el desarrollo de la investigación se recopiló información muy importante referente a los mecanismos, estructuras y configuración de calidad de servicio para cada protocolo IP, redes de área local inalámbrica, comandos de configuración de enrutadores, entre otros, utilizando los dos protocolos en comparación, Ipv6 e Ipv4,

configuración de puntos de acceso y las características del protocolo Ipv6. Además de éstos, se tuvo la necesidad de buscar y conocer software de monitoreo de red a fin de escoger el que mejor se adaptaba a la investigación. Así, entonces, fueron estudiados por medio de búsquedas en Internet, consultas de tesis, guías, revistas, libros, entre otras.

*Fase II: Diseño y desarrollo de topologías y/o ambientes de pruebas de la re*d

En ésta se llevó a cabo la conexión total de los equipos pasivos y activos a través del diseño de una red WAN inalámbrica y nodos móviles. La topología implementada se muestra en la figura No. 1 y debido a que el modelo de enrutadores CISCO 1721 sólo disponen de una interfaz Ethernet, y para este entorno de trabajo se requería un mínimo de dos interfaces Ethernet (Una para el Access Point y el otro para la Antena Ubiquiti), se tuvo que agregar un Switch CISCO 2924 en cada extremo y utilizar VLAN (Virtual LAN en inglés) para imitar que los enrutadores CISCO tuvieran más de dos puertos Ethernet.

Luego, se procedió a conectar físicamente todas las interfaces Ethernet entre el AP, Switch y el enrutador mediante el cable UTP (Cat 5) para simular un Sistema Autónomo (SA). Así mismo, se hizo un procedimiento similar en el otro extremo para crear otro Sistema Autónomo. Posteriormente, se configuraron dos Antenas (AP Ubiquiti) en cada uno extremo de los dos Sistemas Autónomos creando un Enlace Inalámbrico a 5.7 Ghz. Seguidamente, se configuraron los dos APs de cada SA para formar dos redes inalámbricas en los extremos. Una vez finalizado esto, se inició la configuración de los distintos protocolos requeridos en este ambiente de pruebas, tales como RIPv2/RIPng, OSPF, BGP con IPv4 / IPv6.

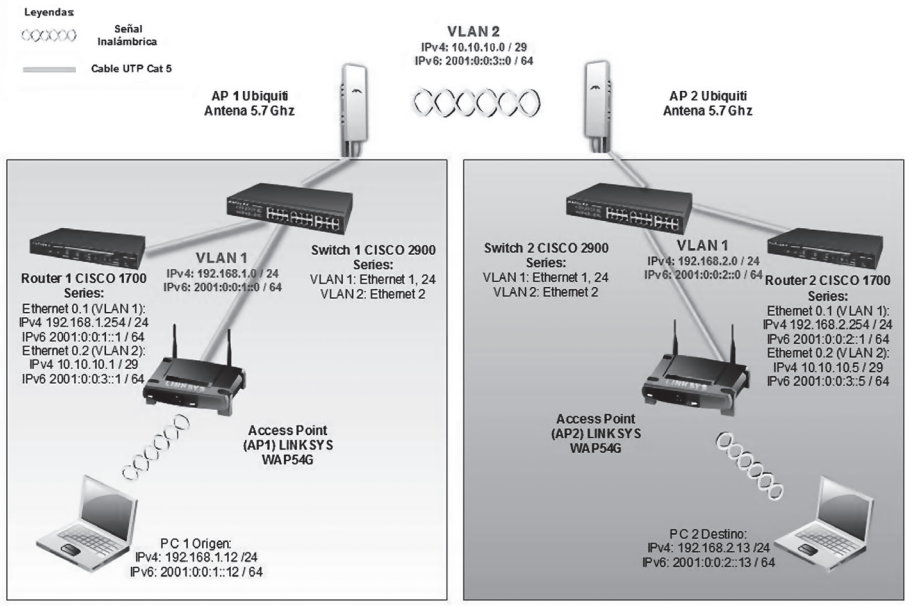

FIGURA 1: Topología y/o ambiente de pruebas
Fuente: Autores (2012)

La comunicación y configuración con los enrutadores y switches CISCO se estableció por medio de un cable de consola a través de la interfaz de línea de comando de un programa de Terminal (Hyper Terminal). Finalmente, se procedió a configurar las PCs en cada extremo de los SA asignándoles direcciones IPv4 e IPv6 a través de la interfaz de red inalámbrica de Windows.

Fase III: Pruebas de medición y recopilación de información de las mismas

Para conseguir un análisis representativo de la QoS en cada protocolo fue necesario disponer de un número óptimo de pruebas realizadas; por este motivo se hicieron de tres (3) repeticiones de cada prueba para garantizar datos más confiables (Montgomery, 2004). Asimismo, los valores reflejados en las tablas de los parámetros (indicadores) estudiados se refieren a su valor promedio. En otras palabras, se promedian los resultados de las tres mediciones realizadas.

Dichas pruebas fueron establecidas en base a la variación del porcentaje de prioridad del ancho de banda que le fue asignado a cada uno de los tres tipos de tráfico (Video, Dato y Voz) a ser enviados, junto con variación de congestionamiento de tráfico de la red, para evaluar cómo se comportaba QoS en ambos protocolos y con distintos niveles de congestionamiento y estableciendo varios puntos de comparación entre los mismos.

Los datos fueron recopilados mediante software de Generación de Tráfico Distribuido DITG (versión 2.6.1d), Wireshark (versión 1.4.4), VideoLAN e IPERF. Del mismo se recopilaron parámetros de medición para establecer el comportamiento de una red, en base al tráfico que se generó; por consiguiente, estos datos fueron almacenados, clasificados y ordenados de manera adecuada, distinguiendo entre cada prueba definida.

Se detectó el ancho de banda disponible desde una PC de un extremo a otra PC del otro extremo, arrojando como resultado óptimo 16.9Mbits/sec.Una vez conocido el ancho de banda disponible en el ambiente, y sabiendo que la QoS funcionaba sólo en caso de congestionamiento, se diseñaron tres tipos de Tráfico que se describen de la siguiente manera:

- Tráfico Datos: Este flujo de tráfico simula la transmisión de tráfico UDP, en las cuales se enviaron paquetes de tamaño 540 bytes, tamaño por defecto del programa DITG para representar una transmisión constante de datos.

- Tráfico Voz: Este flujo de tráfico también fue de UDP, en la cual se enviaron paquetes de tamaño 144 bytes, en el cual se utilizó el códec G.711 de flujo de voz con la técnica de codificación VAD (Propuesta por DITG).

- Tráfico Video: Este flujo de tráfico fue de RTP (Real Time Protocol, siglas en inglés), pero estos paquetes son de tamaño 1390

bytes para IPv6 y 1370 bytes para IPv4, estos valores fueron generados automáticamente por el VideoLAN y capturados por el Wireshark.

En base a estos tres tipos de tráficos antes mencionados, se crearon los siguientes parámetros de pruebas de tráfico a criterio del investigador para colapsar el ancho de banda disponible en este ambiente de red:

1. Tráfico Bajo:
    1.1. Datos: Se enviaron 200 paquetes por segundo durante 60 segundos, para un total de 12000 paquetes.
    1.2. Voz: Se enviaron 100 paquetes por segundo durante 60 segundos, para un total de 6000 paquetes.
    1.3. Video: Se enviaron 25874 paquetes.

2. Tráfico Medio:
    2.1. Datos: Se enviaron 2000 paquetes por segundo durante 60 segundos, para un total de 120000 paquetes.
    2.2. Voz: Se enviaron 500 paquetes por segundo durante 60 segundos, para un total de 30000 paquetes.
    2.3. Video: Se enviaron 25874 paquetes.

3. Tráfico Alto:
    3.1. Datos: Se enviaron 4000 paquetes por segundo durante 60 segundos, para un total de 240000 paquetes.
    3.2. Voz: Se enviaron 1000 paquetes por segundo durante 60 segundos, para un total de 60000 paquetes.
    3.3. Video: Se enviaron 25874 paquetes.

Cabe destacar que se transmitió el mismo video en los diferentes tipos de tráfico por no contarse con el software para enviar un segmento de video, pero se ajustó el tráfico de datos y voz según cada ambiente de prueba, tal como se especifica en la siguiente sección. Este criterio se establece dado que buscó forzar el funcionamiento de la QoS para cada ambiente.

Ambientes de prueba

Basado en lo anterior, se puede decir que en esta investigación se usaron varios ambientes de pruebas, variando los parámetros de prueba de tráfico antes descritos y las prioridades que se le daba a cada tipo de tráfico (individual) a través de políticas de calidad de servicio en el enrutador. Dichos ambientes contemplaron el uso de IPv4 e IPv6 por separado, con y sin QoS, quedando establecidos de la siguiente manera:

a. Condiciones de la red en IPv4 /IPv6 sin QoS enviando:
- Tráfico Bajo
- Tráfico Medio
- Tráfico Alto

b. Condiciones de la red en IPv4 / IPv6, con Calidad de Servicio y 55% del ancho de banda para Datos, 10% para el Video y 10% para la Voz, con envío de:
- Tráfico Bajo
- Tráfico Medio
- Tráfico Alto

c. Condiciones de la red en IPv4 / IPv6, con Calidad de Servicio y 10% del ancho de banda para Datos, 55% para el Video y 10% para la Voz, con envío de:
- Tráfico Bajo
- Tráfico Medio
- Tráfico Alto

d. Condiciones de la red en IPv4 / IPv6, con Calidad de Servicio y 10% del ancho de banda para Datos, 10% para el Video y 55% para la Voz, con envío de:
- Tráfico Bajo
- Tráfico Medio
- Tráfico Alto

Fase IV: Análisis comparativo, teórico y estadístico

En esta fase, se realizó un estudio comparativo entre el protocolo actual (IPv4) y el protocolo en estudio (IPv6), ya que a la fecha es el único punto de comparación, lo cual permite establecer conclusiones más ajustadas a la realidad. Seguidamente, se realizó una sustentación teórica de los resultados obtenidos y finalmente, se realizó un análisis estadístico. Para tales efectos, se trabajó con el software estadístico SPSS versión 15, utilizando la distribución Fisher y el procedimiento ANOVA. El modelo estadístico utilizado fue el siguiente: la variable independiente está conformada por el Protocolo IP (IPv4 e IPv6), y las variables dependientes pertenecen al conjunto relativo al rendimiento de la red (% de Paq. Perdidos, Delay, Bitrate).

El modelo estadístico utilizado es: $yij = \mu + \alpha i - \varepsilon ij$

$i=1,\ldots,n \qquad j=1,\ldots,m$

Donde:

n es el número de repeticiones y m el número de casos
y = var dependiente: % de Paq. Perdidos, Delay, Bitrate
μ = media del caso
α = var independiente: los dos protocolos (IPv4 e IPv6)
εij = error experimental

3. Resultados obtenidos

Los resultados obtenidos se resumen en tres (3) tablas (gráficos) categorizadas por Indicadores de QoS:

- Porcentaje de Paquetes Perdidos:

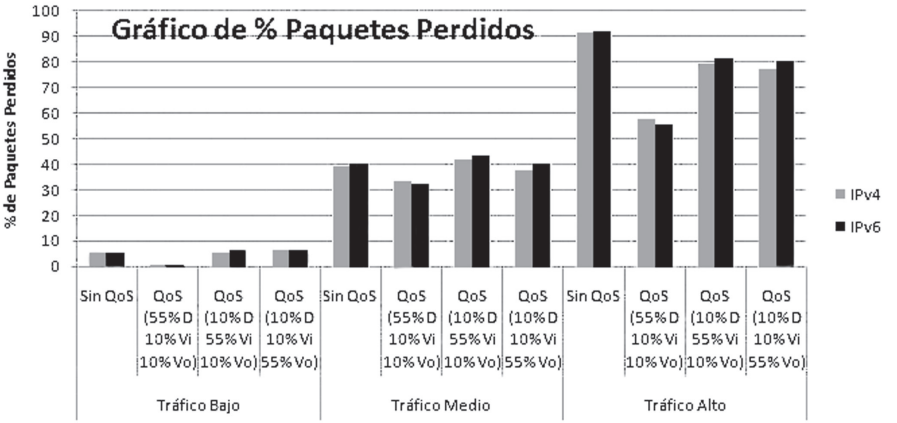

Gráfico N° 1: Gráfico de Porcentaje de Paquetes Perdidos.
Fuente: Autores (2012).

En términos generales, IPv4 tuvo mejor comportamiento que IPv6 aunque no fue con amplio margen, según la visualización del gráfico. Sin embargo, en los ambientes con implementación de QoS y en los cuales donde la mayor prioridad de ancho de banda se da al tráfico de DATOS, se pudo apreciar una pequeña mejora de IPv6 con respecto a IPv4.

- Delay (Latencia):

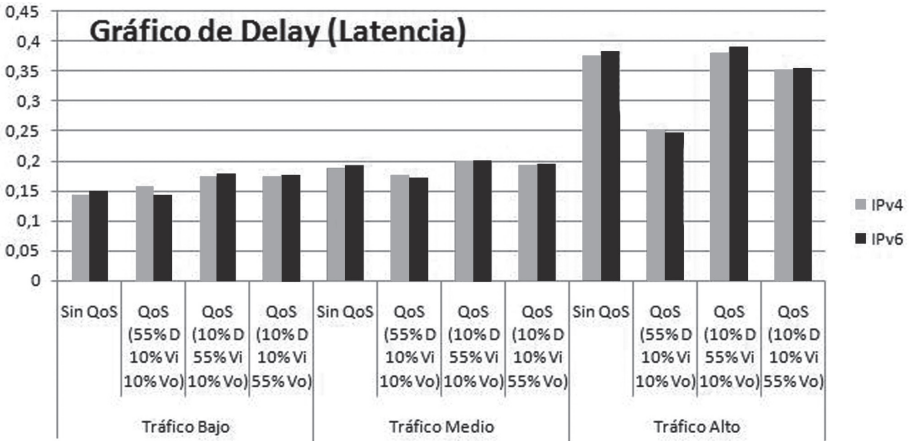

Gráfico N° 2: Gráfico de Delay (Latencia).
Fuente: Autores (2012).

En esta categoría, se pudo apreciar que IPv4 funcionó mejor que el nuevo protocolo IPv6. Con la excepción de los ambientes de QoS con mayor prioridad de ancho de banda para tráfico de DATOS, en los cuales el IPv6 salió victorioso frente al IPv4 con un margen mínimo.

- Bitrate:

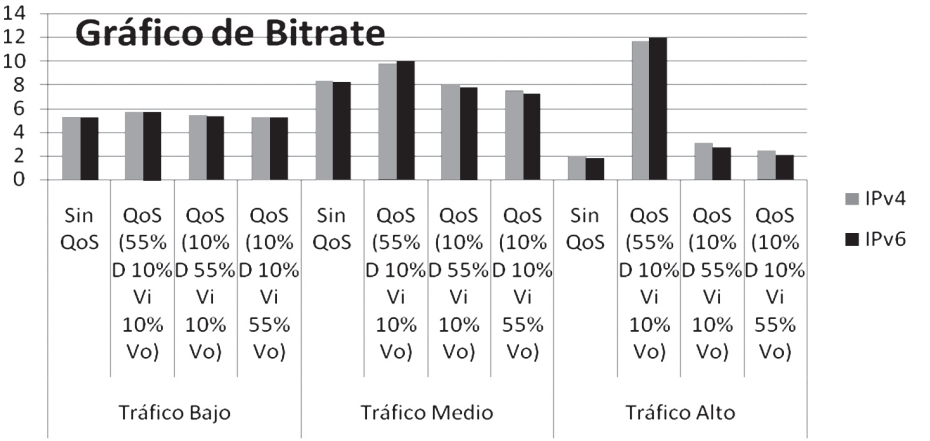

Gráfico N° 3: Gráfico del Bitrate.
Fuente: Autores (2012).

En este renglón, el IPv6 tuvo un comportamiento inferior comparado con el IPv4, ya que en la mayoría de los ambientes de pruebas fue igual o inferior. Pero, en los casos de ambientes con QoS y la mayor prioridad de ancho de banda en el tráfico de DATOS, el IPv6 fue mejor que el IPv4 aunque fue por una mínima diferencia.

3.1 Sustentación teórica de los resultados

En líneas generales, para estas pruebas se evidencia que IPv4 tuvo un mejor comportamiento que IPv6, aún cuando las diferencias fueron mínimas. Asimismo, la relación entre los cuatros indicadores medidos no muestra tendencias anormales. Es decir, se demuestra que mientras mayor es la latencia y el número de paquetes perdidos, menor es el bitrate (situación mayormente notable en la congestión); tal y como lo especifica García (2002), cuando describe

que al ir aumentando la congestión de una red, se activan mecanismos de anticongestión que generan disminución en el bitrate.

Según Odom (2004), la latencia también se ve afectada por un retardo de la señal en los medios, como así también por el retardo añadido por el procesamiento de las señales mediante hubs y repetidores.

Asímismo, se comprueba que esta pérdida se da porque la energía de la señal radiada se expande en función de la distancia desde el transmisor (Flickenger, 2006).

La pérdida también puede producirse cuando los nódulos congestionados de la red dejan caer los paquetes. Algunos protocolos de redes, como TCP, brindan protección de caída de paquetes al retransmitir los paquetes que pueden haber caído o que pueden haber sido corrompidos por la red. A medida que la red se congestiona más, caen más paquetes y hay más retransmisiones de tipo TCP (CNX Anixter, 2011: s/p).

Con respecto al número de paquetes perdidos, y debido a que las transmisiones realizadas estuvieron basadas en el protocolo UDP, el cual no está orientado a conexión, la pérdida de paquetes se produce por descartes de paquetes que no llegan a tiempo al receptor, permitiendo una degradación de la comunicación (menor bitrate) (Harrington, 2003).

4. Resultados del análisis estadístico

A continuación se analizan estadísticamente los resultados obtenidos a partir de los ambientes y las pruebas descritas:

- *Porcentaje (%) de Paquetes Perdidos:*

En todos los ambientes a realizar, se pudo apreciar que el F arrojado por ANOVA es mucho menor que el Ftab (7,71) y además la

significancia (Sig) asociada en la tabla ANOVA también es mucho mayor que el coeficiente de significancia (0,05). Por lo que se pudo afirmar que no hubo diferencias significativas entre IPv4 e IPv6 en este indicador.

- Delay (Latencia):

Al igual que el indicador anterior, se pudo notar que en todos los ambientes a realizar, el F arrojado por ANOVA es mucho menor que el Ftab (7,71) y además la significancia (Sig) asociada en la tabla ANOVA también es mucho mayor que el coeficiente de significancia (0,05). Por lo que se pudo afirmar que no hubo diferencias significativas entre IPv4 e IPv6 en esta categoría.

- Bitrate:

En este indicador se pudo observar un comportamiento equivalente a todos los indicadores anteriores, por lo que se puede afirmar que no hubo diferencias significativas entre IPv4 e IPv6 en este contorno.

Conclusiones

Cuando se establecen políticas de calidad de servicio donde la mayor prioridad es para tráficos que no son de tiempo real, IPv6 tiende a comportarse mejor que IPv4 aún cuando no es significativo estadísticamente. Asimismo, el uso de una cabecera más grande en IPv6, influye en el aumento de los retardos y disminución del bitrate, debido al tiempo de procesamiento de los paquetes en los dispositivos activos como enrutadores, conmutadores y puntos de acceso.

Por otra parte, la utilización del protocolo IPv6 en ambientes de producción con QoS similares a los utilizados en esta investigación, no influye significativamente en el desempeño de la red respecto a entornos IPv4 con las mismas características usadas. A pesar de que

IPv6 presenta en general un menor desempeño frente a IPv4, esta diferencia puede considerarse no significativa, IPv6 aún está en su etapa de madurez, ya que IPv6 es un protocolo que fue construido en base a la experiencia obtenida con IPv4. Por lo tanto, puede concluirse que su uso no altera de manera significativa el desempeño de Sistemas Autónomos conectados por enlaces inalámbricos a 5.7 GHz.

Por último, el hecho de utilizar enlaces de 5.7 GHz genera una pérdida de paquetes superior a otros enlaces de otras frecuencias y enlaces cableados, debido al factor distancia, donde la pérdida de espacio libre puede aumentar, ya que la potencia de la señal tiende a disminuir. Por tanto, el estudio de las condiciones de los enlaces inalámbricos entre sistemas autónomos, es un factor determinante dada la envergadura de los sistemas a interconectar.

Referencias

Álvarez S. (2005). *Estudio y configuración de calidad de servicio para protocolos ipv4 e ipv6 en una red de fibra óptica WDM*. Universidad Politécnica Federico Santa Maria, Chile. Disponible en: http://www.scielo.cl/pdf/rfacing/v13n3/art15.pdf. (Página consultada el 12 de Mayo de 2009).

Bagnulo, Marcelo (2004). *¿Por qué IPv6?* [On-Line]. Dirección URL: http://lacnic.net/documentos/lacnicvi/why-IPv6-lacnicVI.pdf (Página consultada el 12 de Mayo de 2009).

Bisquerra, R. (2000). *Manual de orientación y tutoría***.** Barcelona. Praxis, 271-293.

Certain A. (2009). *Calidad de Servicio (QoS)*. [En Línea]: http://www.alfredcertain.com/?p=9. (Página consultada el 12 de Mayo de 2009).

Cisco Systems (2012). *Border Gateway Protocol (BGP).*[On-Line]. Dirección:URL: http://www.cisco.com/en/US/tech/tk365/tk80/tsd_technology_support_sub-protocol_home.html. (Página consultada el 25 de enero de 2012).

CNX Anixter (2011). *La importancia de la Calidad de Servicio (QoS) - Parte II***.** Revista en Línea: CNX Anixter, Año 2011 - Nº 132, 06 de Junio de 2011. [On-Line]. Dirección URL: http://www.anixtersoluciones.com/latam/cl/informacion_general/2078/la_importancia_de_la_calidad_de_servicio_qos___parte_ii_es.htm (Página consultada el 22 de Junio de 2011).

Díaz Miguel A., Morales César O., García S. Pedro (2007). *Despegando con Movilidad IPv6 (MIPv6).* [On-Line]. Dirección URL: http://www.ist-enable.eu/open/enable_pu_paper_consulintel_despegando_con_MIPv6_AUI_v1_5.pdf (Página consultada el 12 de Mayo de 2009).

Fabero, Juan Carlos (2008). *Tecnologías Avanzadas de Redes y Telecomunicaciones*. [On-Line]. Dirección URL: http://www.fdi.ucm.es/profesor/jcfabero/Asuncion/bgp.pdf (Página consultada el 13 de Mayo de 2009).

Fernández Alcántara, Azael (2007). *Direcciones IPv4 ¿recurso de Internet en agotamiento?* [On-Line]. Dirección URL: http://www.enterate.unam.mx/Articulos/2007/junio/art1.html (Página consultada el 8 de Junio de 2009).

Flickenger Rob (2006). *Creative Commons*. *Redes Inalámbricas en los Países en Desarrollo.* Editorial Limehouse Book Sprint Team.

García, J. (2002). *Redes de Comunicación: conceptos fundamentales y arquitecturas*. Madrid. Editorial: MC Graw Hill-Madrid.

Goitia, Maria Julieta (2003). *Protocolos de Enrutamiento Un Simulador Didáctico***.** Universidad Nacional del Nordeste, Facultad de Ciencias Exactas, Licenciatura en Sistemas, Argentina.

Harrington Donna L. (2003). *Shooting Trouble with IP***.** [On-Line]. Dirección URL: http://www.ciscopress.com/articles/article.asp?p=98156&seqNum=2

Millán R. (2012). *Qué ha pasado con IPv6?* [En línea]. Disponible en: http://www.ramonmillan.com/documentos/estadoipv6.pdf. (Página consultada el 25 de enero de 2012).

Montgomery D. (2004). *Diseño y Análisis de Experimentos*. Segunda Edición. Editorial Limusa Wiley.

Odom Wendell (2004). *Networking First-Step: How to Build a Local (Network) Roadway*. [On-Line]. Dirección URL: http://www.ciscopress.com/articles/article.asp?p=174105&seqNum=2

Stallings, William (2004). *Comunicaciones y Redes de Computadores*. Séptima Edición. Madrid. España. McGraw-Hill Internacional, S.A.