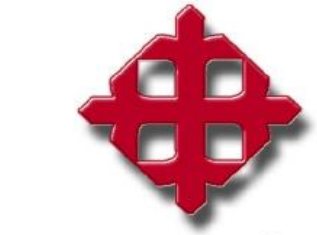


UNIVERSIDAD CATOLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

TESIS FINAL

Previa a la obtención del grado de

MAGÍSTER EN TELECOMUNICACIONES

TEMA: Enfoque comparativo entre IPv4 e IPv6 de la QoS en Redes Inalámbricas

Elaborado por: Ing. Judith Gálvez Soto

Tutor: MSc. Juan García Pérez

Guayaquil, Octubre de 2012

UNIVERSIDAD CATOLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

CERTIFICACIÓN

Certificamos que el trabajo fue realizado en su totalidad por Magister Judith María Gálvez Soto, como requerimiento parcial para la obtención del Grado Académico de Magister en Telecomunicaciones.

Guayaquil, a los 30 días del mes de octubre año 2012

DIRECTOR DE TESIS

_____

MSc. Juan García Pérez

REVISORES:

_____

Ing. Edwin Palacios Meléndez, MSc.

_____

Ing. Néstor Zamora Cedeño, MSc.

DIRECTOR DEL PROGRAMA

_____

Ing. Manuel Romero Paz, MSc.

UNIVERSIDAD CATOLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

DECLARACIÓN DE RESPONSABILIDAD

YO, Judith María Gálvez Soto

DECLARO QUE:

La tesis “Enfoque comparativo entre IPv4 e IPv6 de la QoS en Redes Inalámbricas”, previa a la obtención del grado Académico de Magister, ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico de la tesis del Grado Académico en mención.

Guayaquil, a los 30 días del mes de octubre año 2012

EL AUTOR

_____

Ing. Judith María Gálvez Soto

UNIVERSIDAD CATOLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

AUTORIZACIÓN

Yo, Judith María Gálvez Soto

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la Institución de la Tesis de Maestría titulada: “Enfoque comparativo entre IPv4 e IPv6 de la QoS en Redes Inalámbricas”, cuyo contenido, ideas y criterios son de exclusiva responsabilidad y total autoría.

Guayaquil, a los 30 días del mes de octubre año 2012

EL AUTOR

_____

Ing. Judith María Gálvez Soto

AGRADECIMIENTO

A Dios, por ser la luz que ilumina mi camino.

A mis padres, a mi esposo y a mis hijos, por su incondicional amor y apoyo, lo que me ha permitido lograr mis metas.

A mi director de tesis MSc. Juan Pérez, por el apoyo, orientación y motivación brindada en el desarrollo de este trabajo.

DEDICATORIA

Dedico este trabajo de tesis a mis padres, a mi esposo, a mis hijos y a mi hermana. En especial a mi querida madre, María Angélica, que aunque ya no me acompaña físicamente, fue siempre mi eterna amiga, ejemplo de perseverancia y superación, su amor y sus consejos me han mostrado el camino correcto a seguir.

Índice General

Índice de Figuras

Índice de Figuras

RESUMEN

Brindar Calidad de Servicio (QoS) en redes inalámbricas con tecnología IPv4 en tiempo real se presenta como un problema a resolver. Esta versión del protocolo IP en redes inalámbricas entrega características como retardo, *jitter,* pérdida de paquetes, requerimiento de ancho de banda, etc. que impactan en el rendimiento y Calidad de Servicio (QoS) que ofrecen al usuario. El protocolo IPv6 es una alternativa para resolver las desventajas que representa el uso de IPv4.

En el Capítulo 1 se exponen los aspectos teóricos para poder abordar el tema.

En el Capítulo 2 se resumen los conceptos y características principales de las redes inalámbricas. Se determina también la importancia, prioridad y requerimientos de las aplicaciones actuales para implementar Calidad de Servicio (QoS) en este tipo de redes.

En el Capítulo 3 se presenta las características de los protocolo IPv4 e TPv6.

En el Capítulo 4 se describen procesos, con la información obtenida se compara los resultados obtenidos en cada caso determinando la Calidad de Servicio (QoS) que ofrecen.

Finalmente se termina con las conclusiones y recomendaciones realizadas al comparar la Calidad de Servicio (QoS) que ofrecen los protocolos IPv4 e IPv6 en redes inalámbricas.

Palabras claves: redes inalámbricas, IPv4, IPv6, Calidad de Servicio (QoS)

ABSTRACT

Provide Quality of Service (QoS) in wireless networks with IPv4 technology in real time is presented as a problem to solve. This version of the IP protocol in wireless networks delivery features such as delay, jitter, packet loss, requirement of bandwidth, etc. that have an impact on the performance and quality of service (QoS) that offer the user. The IPv6 protocol is an alternative to solve the disadvantages that represents the use of IPv4.

In Chapter 1 presents the theoretical aspects in order to address the issue.

In Chapter 2 summarizes the key features and concepts of wireless networks. It also determines the importance, priority and requirements of the current applications to implement Quality of Service (QoS) in this type of network.

Chapter 3 presents the characteristics of the IPv4 protocol and TPv6.

Chapter 4 describes processes, the information obtained is compared the results obtained in each case determine the Quality of Service (QoS) they provide.

Finally it ends with the conclusions and recommendations made to compare the Quality of Service (QoS) offered by IPv4 and IPv6 protocols in wireless networks.

Keywords: wireless networks, IPv4, IPv6, Quality of Service (QoS)

CAPÍTULO 1 DESCRIPCIÓN Y ASPECTOS TEÓRICOS

1.1. Introducción.

En la actualidad, los sistemas de comunicaciones han cambiado la manera en que opera la sociedad, facilitando el compartir cualquier tipo de información de una manera rápida y eficaz, lo que ha supuesto una revolución muy importante en el mundo de las Telecomunicaciones.

La mayoría de los enlaces transportan datos sobre protocolos TCP/IP, proporcionando cada vez más aplicaciones, que necesitan determinadas características para que puedan funcionar correctamente. Se trata de lograr que las redes de computadoras así como los servicios ofrecidos a los usuarios sean eficientes y eficaces, por lo que se requiere un nivel de calidad, siendo necesario implementar modelos para satisfacer la demanda de Calidad de Servicios *(*QoS).

1.2. Antecedentes.

De acuerdo a Holt, A. (2010), las redes inalámbricas basadas en el estándar IEEE *(Institute of Electrical and ElectronicsEngineers)* 802.11, se popularizaron en los últimos tiempos, siendo innumerables las oportunidades que este tipo de redes puede proporcionar a sus usuarios. Debido a las muchas aplicaciones que hacen uso de éstas redes brindando una baja eficiencia por sus características de funcionamiento, hace que en el presente se esté dando una gran importancia a las técnicas de Calidad de Servicio (QoS*)* en redes inalámbricas. Para responder a esta deficiencia la IEEE desarrolla el estándar 802.11e que permite brindar Calidad de Servicio (QoS) a redes inalámbricas.

El concepto de Calidad de Servicio (QoS) puede variar dependiendo del autor. De acuerdo a la ISO/IEC DIS 13236, es un conjunto de cualidades relacionadas con la provisión de un servicio hacia un usuario. Según León, M. (2002), la Calidad de Servicio (QoS*)* se puede definir como el conjunto de calidades relacionadas con los servicios que deben percibir los usuarios. Otros investigadores definen la Calidad de Servicio *(*QoS*),*

como la capacidad para proporcionar aseguramiento del recurso y diferenciación del servicio en una red.

En relación al tema de tesis, existen algunas investigaciones que se considerarán como base para este tema, una de ellas es el estudio de los modelos propuestos para ofrecer Calidad de Servicio *(*QoS*).* Otra investigación que analiza los Servicios Diferenciales que ofrece IP por medio de los campos ToS y TC presentando cómo aplicar Calidad de Servicio (QoS*)* en los *hosts* y los *routers.*

Las nuevas aplicaciones como *VoIP, e-commerce* y videoconferencia son sensibles al desempeño de la red y hacen que la capacidad de las redes de proporcionar Calidad de Servicio (QoS) sea cada vez más importante. Las redes de IP actuales proporcionan un envío de tráfico de mejor esfuerzo, por lo tanto no ofrece ningún tipo de garantías de Calidad de Servicio (QoS). Existen servicios como la voz con rigurosos requisitos de retardo y variación del retardo (*jitter)*, que hace necesario añadir funcionalidad a las IP para que las redes basadas en este protocolo sean capaces de soportar este tipo de servicios.

Hoy en día los usuarios de servicios de Internet pueden ser tanto humanos como programas de aplicación, buscadores, multimedia, telefonía entre otros. Dado que las redes fueron creadas en primera instancia para transportar de forma óptima y segura el tráfico de datos pero no en tiempo real, la Calidad de Servicio (QoS) se implementa en las redes buscando no perder el contenido ni la secuencia de los datos. Aplicar eficientemente Calidad de Servicio (QoS) en redes inalámbricas brinda la capacidad de asegurar el sistema utilizado. Sin embargo, en el presente las aplicaciones son diferentes y los requerimientos que tiene cada usuario también son diferentes.

1.3. Justificación del Problema.

El crecimiento tecnológico va de la mano con el crecimiento y evolución de las aplicaciones. Con el correr del tiempo las redes de datos requieren más disponibilidad, tornándose crítico para una red pública o privada.

Pequeños cambios en el uso de la red pueden causar alto impacto en la misma, impacto al que se debe de considerar como un impacto negativo, por ejemplo la saturación de un enlace o utilizar recursos asignados para otra aplicación más prioritaria, hace que aumente el costo de operación de la red y como consecuencia una degradación de servicio. Nuevas aplicaciones como *VoIP*, videoconferencia, son sensibles al desempeño de la red, provocando que la capacidad de las redes para proporcionar Calidad de Servicio (QoS) sea cada vez más importante.

En la evolución hacia una red de servicios múltiples uno de los principales objetivos es optimizar la red respondiendo de forma eficiente a inconvenientes, como la pérdida de paquetes, retardos, variaciones en la entrega del tráfico de voz, congestión, etc. Considerando todos éstos escenarios, es necesario plantear condiciones de solución para aumentar y satisfacer los requisitos de Calidad de Servicio (QoS) en sistemas basados en IP.

Las redes inalámbricas son una realidad que proporciona un servicio de cierta calidad en determinadas condiciones, como por ejemplo con baja carga de tráfico. Sin embargo, añadir movilidad trae consigo nuevos retos relacionados a la Calidad de Servicio (QoS). Es necesario considerar que la transmisión por medios inalámbricos enfrenta a complicaciones como la interferencia, pérdida de paquetes, etc. Sería una tarea muy sencilla dar Calidad de Servicio (QoS) si las redes nunca se congestionaran, para ello habría que sobredimensionar todos los enlaces, situación que no siempre es posible o deseable, por lo que es preciso tener mecanismos que permitan cumplir con los requisitos de Calidad de Servicio (QoS*)* en redes inalámbricas.

Este estudio comparativo será realizado para alcanzar los objetivos propuestos, tratando de identificar las debilidades y eficiencias que pueden proporcionar las dos versiones de IP, que se tratan en este documento, en cuanto al ofrecimiento de Calidad de Servicio (QoS) en redes inalámbricas, también conocidas como redes *Wi-Fi*. Documento que está también orientado a identificar los elementos y características

que se reconocerán como propuestas para satisfacer la Calidad de Servicio (QoS) requerida en la actualidad en este tipo de redes.

Para entender mejor la problemática, se debe tener presente también que los requerimientos de calidad varían dependiendo de los usuarios y de los servicios solicitados.

1.4 Definición de Problema

1.4.1 Problema

Los protocolos de internet IPv4 e IPv6 funcionan a través de cualquier medio de transmisión, es por esto que surge la necesidad de garantizar la Calidad de Servicio (QoS) en redes inalámbricas para cumplir de manera eficiente con los requerimientos de los usuarios.

1.5 Objetivos

El crecimiento tecnológico va de la mano con el crecimiento y la evolución de las aplicaciones. Conforme pasa el tiempo las redes inalámbricas requieren mayor disponibilidad, por ello se describe el objetivo general y los objetivos específicos.

1.5.1 Objetivo General.

Analizar técnicas de Calidad de Servicio (QoS*)* en redes inalámbricas con protocolo IPv4 e IPv6 aplicadas en investigaciones realizadas, con el propósito de observar los beneficios obtenidos en el rendimiento de la red.

1.5.2 Objetivos Específicos.

- Obtener y procesar contenidos relevantes sobre la Calidad de Servicio (QoS) que ofrecen IPv4 e IPv6 en redes inalámbricas, para poder utilizarlos de una manera eficiente en el presente trabajo.
- Identificar y describir los mecanismos que se utilizan para brindar Calidad de Servicio (QoS) en redes inalámbricas.
- Observar, analizar y evaluar la información obtenida de pruebas de simulación realizadas, que permita determinar las deficiencias y fortalezas

mediante la comparación de los resultados obtenidos al aplicar Calidad de Servicio (QoS*)* en redes inalámbricas con protocolo IPv4 e IPv6.

1.6 Hipótesis o Idea a Defender.

El uso del protocolo IPv6 en redes inalámbricas permitirá mejorar la provisión de Calidad de Servicio (QoS) a los usuarios.

1.7 Metodología de Investigación.

La metodología utilizada en el presente trabajo de investigación está en base al método científico, para lo cual se realiza la revisión de literatura relacionada con la temática que es utilizada en el marco teórico. Los criterios manejados en el proceso de búsqueda de documentos y artículos se basaron en proyectos de investigación relacionados al tema propuesto bajo el esquema cuasi experimental, debido a que se enfoca en el análisis de casos particulares y en ambientes virtuales, utilizando herramientas de simulación de redes con el fin de obtener los datos que serán estudiados para determinar las deficiencias y fortalezas de las tecnologías utilizadas. En esta etapa se muestra de manera virtual los mecanismos que ofrece el estándar 802.11e que hacen posible que una red inalámbrica pueda proporcionar Calidad de Servicio (QoS).

Para poder evaluar la Calidad de Servicio en redes inalámbricas utilizando protocolos IPv4 e IPv6, es necesario realizar los siguientes pasos:

1. Consultar contenidos relevantes en relación a la Calidad de Servicio en redes inalámbricas, protocolos IPv4 e IPv6.
2. Describir los mecanismos introducidos en el protocolo 802.11e para proporcionar Calidad de Servicio (QoS).
3. Observar el comportamiento de las redes inalámbricas al integrar las herramientas que proveen los protocolos IPv4 e IPv6, a través de la especificación 802.11e, mediante el análisis de pruebas de simulación realizadas por otros autores, para poder controlar los parámetros de Calidad de Servicio (QoS).
4. Analizar la información para determinar las deficiencias y fortalezas mediante la comparación de los resultados obtenidos.

CAPÍTULO 2 REDES INALÁMBRICAS Y CALIDAD DE SERVICIO (QoS)

2.1 Introducción

Para realizar las conexiones entre dispositivos inalámbricos con una red LAN (ver Figura 2.1), existe una serie de dispositivos que cumplen esa función y trabajan bajo un estándar común, el IEEE 802.11 (también conocido como WiFi o WLAN). Este estándar sirve para el manejo de video en redes, ya que para enviar la señal de video, esa señal es digitalizada previamente. Existen otros estándares y otras tecnologías patentadas, sin embargo, la ventaja de utilizar los estándares inalámbricos 802.11 es que trabaja en bandas de frecuencia que no necesitan licencia, de manera que no implican ningún costo asociado a la configuración y al funcionamiento de la red, (Legal, 2011)

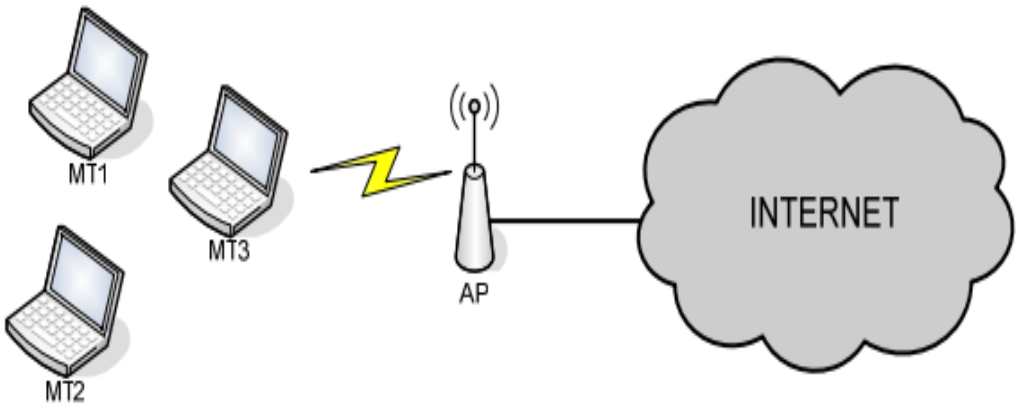


Figura 2.1: Esquema de red inalámbrica
Fuente: Andreu, F. (2006). *Redes WLAN. Fundamentos y aplicaciones de seguridad.*

Las redes inalámbricas se encuentran en un periodo de gran expansión, debido principalmente a su bajo costo, su facilidad a la hora de desplegarse, y a la libertad de movimiento que otorgan a las estaciones dentro de su área de cobertura, convirtiéndose en una solución muy común para proporcionar acceso a Internet. Otro factor muy importante ha sido la aparición del principal mecanismo usado a nivel MAC (*Medium Access Control*) para las redes inalámbricas definido por el estándar IEEE 802.11, ratificado en julio de 1997 con su posterior revisión en 1999,

y sus enmiendas. De acuerdo a (Pellejero, Andreu, & Lesta, 2006), es una red inalámbrica que usa la transmisión por radio en la banda de 2.4GHz., o infrarroja, con velocidades de transmisión de 1Mbps y 2Mbps, dependiendo de la distancia entre el punto de acceso y la estación inalámbrica y de las condiciones de utilización del canal.

Dentro de la familia IEEE 802.11 a los estándares inalámbricos de capa física y de subnivel MAC, les acompañan una serie de extensiones de estándares, cuyo principal objetivo es la incorporación de nuevas funcionalidades a los estándares base, como evolución y optimización de los mismos. En la Tabla 1 se resumen los estándares y sus funcionalidades.

Tabla 2.1: Estándares físicos y de optimización

Estándares IEEE 802.11	Capa del modele OSI en el que se aplica	Descripción
a	Física	Capa física con velocidades de hasta 54 Mbps operando en la banda de 5 GHz
b	Física	Capa física con velocidades de hasta 11 Mbps operando en la banda de 2,4 GHz
c	MAC	Operaciones de bridging (puente)
d	Física	Dominios internacionales
e	MAC	Modificación de la capa MAC para proveer Calidad de Servicio (QoS)
f	Ambas	Interoperabilidad entre puntos de acceso
g	Física	Capa física con velocidades de hasta 54 Mbps operando en la banda de 2,4 GHz
h	Ambas	Coordinación con los estándares Hiper LAN2 europeos
i	MAC	Estándar para dotar a las redes de seguridad
j	Ambas	Estándar específico para regular las bandas de frecuencia japonesas de 4,5 y 5 GHz
k	Ambas	Mejora del estándar original para permitir la gestión de recursos radio
m	Ambas	Mantenimiento de estándares previos
n	Ambas	Capa física con velocidades de hasta 100 Mbps
p	MAC	Modificación de la capa MAC para permitir el hanf-off a velocidades vehiculares
r	MAC	Modificación de la capa MAC para permitir roaming rápido
s	Ambas	Estándar para las redes Mesh

Fuente: Andreu, F. (2006). *Redes WLAN. Fundamentos y aplicaciones de seguridad.*

La gran acogida de las redes inalámbricas en la actualidad y la integración de los servicios de voz, video y datos sobre una misma infraestructura, ha generado la necesidad de proporcionar un tratamiento

diferente al tráfico de voz y video, mediante la aplicación de técnicas que aseguren una determinada Calidad de Servicio (QoS).

2.1.1 Funcionamiento de una red inalámbrica

Detectar el alcance, la localización de una red cableada es una tarea fácil de realizar. La señal de la red cableada tiene el mismo alcance que los cables, a diferencia de una red inalámbrica en que las señales no son guiadas por ningún cable y su alcance no está delimitado, lo que aumenta la complejidad cuando se tienen redes inalámbricas superpuestas. Es necesario asignar un nombre a la red que se conoce como SSID (*Service Set Identifier*), conocido como el *beacon,* son tramas que llevan información con las distintas características de la red (velocidad de transferencia, seguridad, etc.). Para utilizar el usuario una red inalámbrica específica debe de indicar el nombre de la red a la que quiere conectarse. Como seguridad se puede ocultar la red no enviando el SSID en las tramas.

Como los datos de una red inalámbrica flotan en el aire, para los hackers es fácil interceptar las señales que atraviesan una zona determinada, que cuenta con redes de este tipo, (Parsons & Oja, 2008), por lo que codificar los datos transmitidos brinda seguridad ante intrusos.

La codificación inalámbrica original fue llamada WEP (*Wired Privacy Equivalency,* Privacidad equivalente a conexión con cable). Este algoritmo presentó muchas fallas en su funcionamiento lo que obligó a los ingenieros de la IEEE a desarrollar un nuevo mecanismo de seguridad. Una segunda versión de WEP emplea codificación más resistente, pero tiene varios defectos que los hackers aprovechan con facilidad. WPA resuelve algunas de las debilidades de WEP, apareciendo luego WEP2, que ofrece una mayor seguridad al cambiar las cables de codificación e implementar revisiones más rigurosas de la integridad de los mensajes. Todos los dispositivos de una red deben de usar el mismo tipo de codificación. Los dispositivos inalámbricos fabricados después de marzo de 2006 deben soportar WEP2. Una clave de red inalámbrica es la base

para desordenar y reorganizar los datos transmitidos entre los dispositivos inalámbricos.

El estándar IEEE 802.11 define dos funciones de acceso al medio a nivel MAC. La primera de ellas recibe el nombre de DCF (*Distributed Coordination Function*) y utiliza un mecanismo de acceso al medio distribuido basado en CSMA/CA (*Carrier Sense Multiple Access with a Collisions*). La segunda de las funciones recibe el nombre de PCF (*Point Coordination Function*), y utiliza la anterior como base para su funcionamiento. PCF es opcional y usa un mecanismo de *polling* que requiere de un nodo central llamado PC (*Point Coordinator*) que lo coordine.

2.1.2 Evolución de las redes inalámbricas

Al ser la comunicación no cableada para una transmisión inalámbrica, en sus inicios creaba restricción en cuanto a zona de disponibilidad, considerándose como soluciones costosas para entornos muy limitados. Sin embargo, en la actualidad, las redes inalámbricas representan una solución tecnológica de comunicaciones que debe responder a cinco áreas claves: el estándar, la regulación, la tecnología, los servicios, y las posibilidades económicas.

2.2 Protocolo 802.11e

EEE 802.11e fue ratificado en diciembre del 2005, (Andreu, 2006), es una propuesta que define los mecanismos utilizados en una red inalámbrica para proporcionar Calidad de Servicio (QoS) a aplicaciones en tiempo real como voz y video. Su objetivo es corregir los problemas que presentaba el estándar 802.11 al momento de ofrecer Calidad de Servicio (QoS*)* a los diferentes tipos de tráficos de red.

Calidad de Servicio *(*QoS) es la denominación común que se le da a los mecanismos de Calidad de Servicio aplicados en el ámbito de las redes de datos. Éstos permiten manipular características específicas del tráfico en la red, de manera que se satisfagan las necesidades de servicio de ciertas aplicaciones y usuarios. Calidad de Servicio (QoS) brinda

capacidad a una red para ofrecer prioridad a determinados tipos de tráficos, independientemente de la tecnología que la red utiliza, generalmente se aplica a nivel de la capa 3-4.

La finalidad es proporcionar clases de servicio con niveles gestionados de Calidad de Servicio (QoS), mecanismos que son indispensables cuando se ofrecen servicios de tiempo real como VoIP, videoconferencia, video *streaming*, radio por Internet, entre otras aplicaciones de datos, voz y video.

En este nuevo estándar se hace una distinción entre aquellas estaciones que no utilizan los servicios QoS, que se denominan nQSTA, y aquellas que si lo utilizan, llamadas QSTA.

2.2.1 Antecedentes y provisión del protocolo 802.11e.

Las redes inalámbricas atraen cada vez más el interés de las empresas y de las personas en general, por lo que la interconexión de una red inalámbrica a la red de una empresa requiere de mucha seguridad de acceso en los extremos de la red. Cualquier persona con una tarjeta de red inalámbrica podría conectarse a cualquier empresa que se encuentre en el radio de sus nodos inalámbricos.

Debido a la gran aceptación del protocolo 802.11 y el uso de aplicaciones en tiempo real sobre dichas redes, ha presentado la necesidad de contar con una herramienta que permita proporcionar garantías de servicio a las aplicaciones. Ratificado en diciembre del 2005, el objetivo del estándar 802.11e es proporcionar Calidad de Servicio (QoS) en redes WLAN, cuenta con mecanismos en el nivel MAC de la capa de enlace que permiten proporcionar diferentes tipos de servicio a aplicaciones que comparten el mismo medio inalámbrico, como datos, voz y video, de acuerdo a (Pellejero, Andreu, & Lesta, 2006).

La Calidad de Servicio (QoS) permite que los administradores de una red puedan asignarle a un determinado tráfico prioridad sobre otro, para garantizar que un mínimo nivel de servicio le sea provisto. Debido al desarrollo de aplicaciones como VoIP, videoconferencia, etc., la

necesidad de implementar técnicas de Calidad de Servicio (QoS) es evidente. Aplicaciones en tiempo real como voz y video, son sensitivas a retardo de la red. Si a los paquetes que conforman una comunicación de voz o video les toma demasiado tiempo llegar al destino, el resultado se presentará distorsionado.

Situaciones en las que son convenientes proveer Calidad de Servicio (QoS), para brindar un servicio más acorde al tipo de tráfico.

- Para responder a cambios en los flujos del tráfico de red.
- Para maximizar el uso de la infraestructura de la red.
- Para priorizar ciertas aplicaciones de nivel crítico
- Para brindar mejor desempeño a las aplicaciones sensitivas al retardo

2.2.2 Modos de acceso en 802.11e

El protocolo MAC del estándar IEEE 802.11 no provee ninguna forma de diferenciar los distintos tipos de tráficos. Todos son tratados en forma equitativa.

El estándar 802.11e define un conjunto de mejoras a la capa MAC del estándar 802.11 para proveer Calidad de Servicio (QoS).

Para proporcionar soporte a la Calidad de Servicio (QoS) en IEEE 802.11e se introduce una nueva función de coordinación llamada función de coordinación híbrida (HCF – *Hybrid Cocrdination Function*) la cual se emplea para el conjunto de servicios básicos con soporte de QoS (QBSS). La función HCF define dos nuevos mecanismos de acceso al canal:

- Acceso a canal distribuido mejorado (EDCA – *Enhanced Distributed Channel Access)* que consiste en una función de acceso al canal basada en contienda, funciona de manera concurrente junto con el segundo modo de operación que sigue,
- Acceso a canal controlado HCF (HCCA – HCF *Controlled Channel Access*) que se basa en un mecanismo de sondeo controlado por

el coordinador híbrido. En la figura 2.2 se presenta la manera cómo modifica el estándar 802.11e al estándar original.

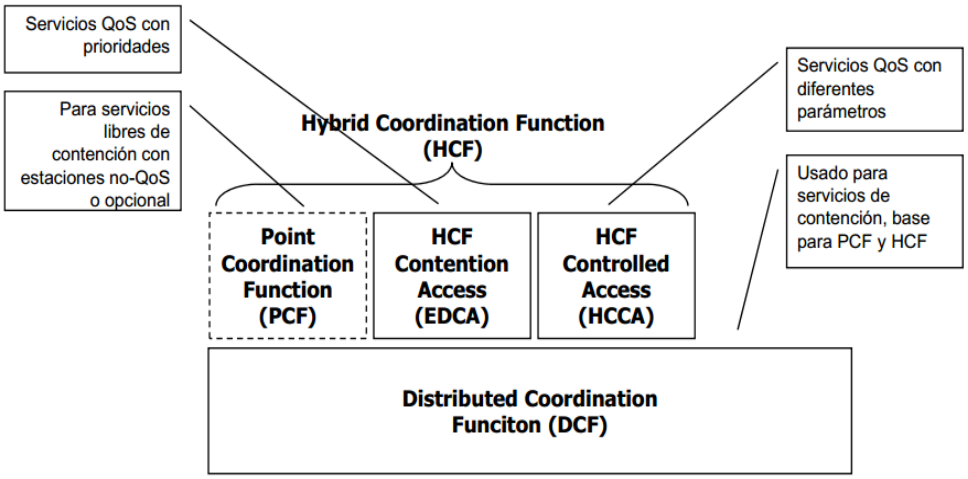


Figura 2.2: Modelo 802.11e

Fuente: Banchs, A. & Vollero, L. (24 de agosto de 2005). *Computer Networks*.

Ambas funciones de acceso mejoran o extienden la funcionalidad de los métodos de acceso originales (DCF y PCF). La primera función de acceso, EDCA, fue diseñada para soportar la priorización de tráficos, tal como hace *DiffServ,* mientras que *HCCA* soporta tráfico parametrizado, de la misma forma que *IntServ*.

a) EDCA (Acceso al canal de forma distribuida)

Al ser aprobado el estándar 802.11e la Alianza WiFi generó una especificación interna llamada WMM (WiFi Multimedia adoptando únicamente el mecanismo EDCA con el propósito de facilitar la interoperabilidad y garantizar la Calidad de Servicio (QoS) entre diferentes proveedores de equipos, según el tipo de tráfico que exista en la red, tratando de forma preferencial a las aplicaciones con restricciones en el tiempo.

EDCA es una extensión en varios aspectos para mejorar el mecanismo de acceso DCF y provee acceso con prioridad al medio inalámbrico.

Cada estación implementa hasta cuatro categorías de acceso (AC) independientes, cada una de ellas está asociada a un determinado tipo de

tráfico. El nombre que tiene cada AC determina la aplicación que debe ocupar la misma. Voz (VO), video (VI), *best effort* (BE) y *background* (BK). Si durante la ejecución del *backoff* se produce una colisión interna entre dos AC's de la misma estación (llamada colisión virtual), la cola con más prioridad transmitiría la trama al medio físico, mientras que la otra cola se comportaría como si hubiese sufrido una colisión.

El proceso de *backoff* también se ve modificado, por la introducción de unos parámetros (diferentes para cada AC) que afectan al comportamiento del mismo. En la Figura 2.3 se presenta la definición de estos parámetros.

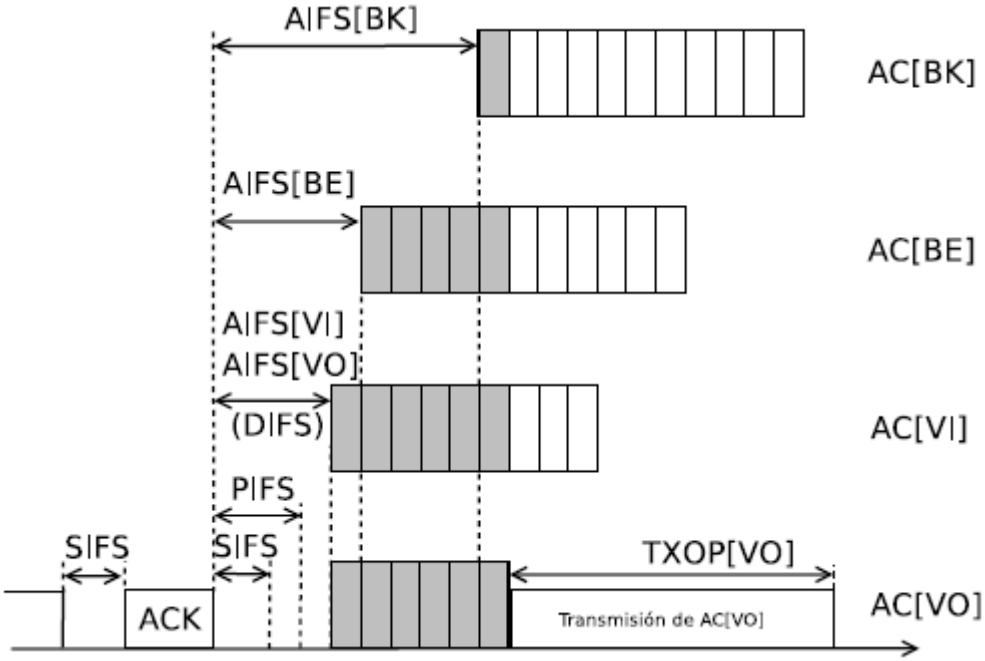


Figura 2.3: Parámetros del modo EDCA

Fuente: Banchs, A. & Vollero, L. (24 de agosto de 2005). *Computer Networks*.

TXOP (*Transmission Oportunity*): Una vez que una estación ha conseguido acceder al medio, tiene derecho a utilizar el canal durante un tiempo menor o igual al TXOP (teniendo en cuenta las confirmaciones). Esto permite que se puedan transmitir varias tramas durante la misma ranura de tiempo, existiendo la posibilidad de realizar un confirmación por cada trama. Si el valor de este parámetro es cero supone que la estación utilizará el canal el tiempo necesario para transmitir una única trama (como en DCF). Si el tiempo necesario para la transmisión de una trama

superase el valor indicado por este parámetro, la trama debe ser fragmentada.

CW (*Contention Window)*: El funcionamiento del retroceso exponencial binario es muy similar al mecanismo DCF, aunque hay que considerar que tanto el valor de *CWmin* como el de *CWmax* puede ser diferente para cada clase de tráfico.

AIFS (*Arbitration InterFrame Space*): En el modo EDCA, el tiempo que debe esperar una estación hasta disminuir dicho contador es diferente para cada cola de tráfico.

EDCA proporciona acceso diferenciado DCF al medio inalámbrico para ocho clases de tráfico. En la Figura 2.4 se observa el modelo de referencia de EDCA.

Cada estación tiene cuatro colas o ACs (Categorías de Acceso), para poder implementar las ocho clases de tráfico.

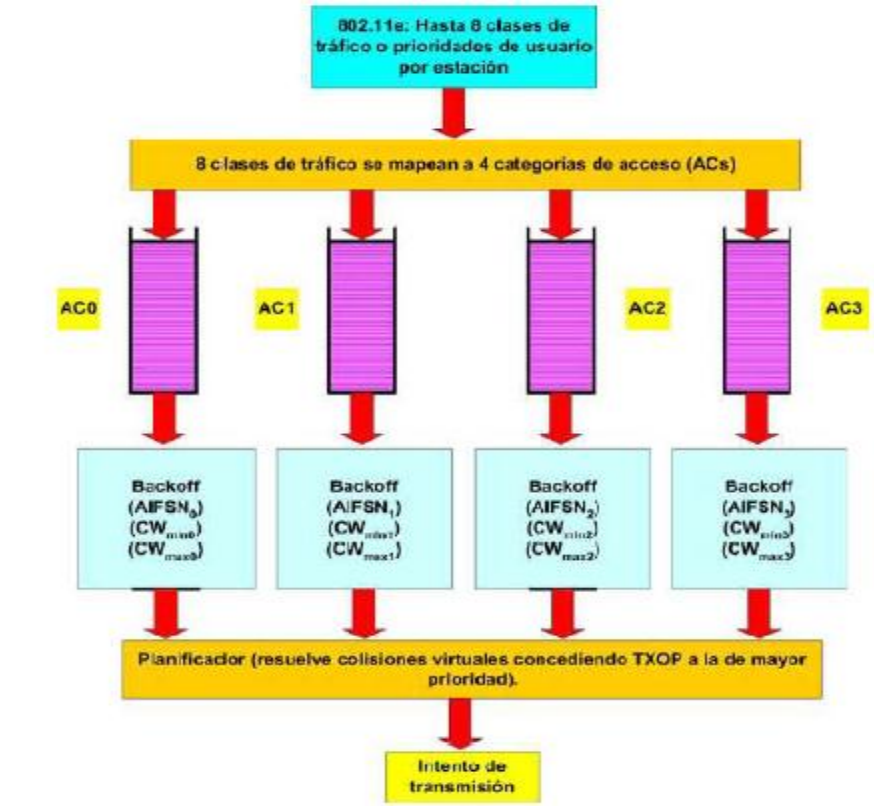


Figura 2.4: Categorías de Acceso en el mecanismo de acceso EDCA

Fuente: Zhu, C. (2011). *Streaming Media Architectures, Techniques and Applicatios*

En el mecanismo de acceso EDCA cada estación (QSTA, QoS *Station),* tiene cuatro colas de transmisión o categorías de acceso (*AC, Access Category),* que se comportan como estaciones virtuales. Las cuatro ACs son AC_VO (para tráfico de voz, AC_VI (para tráfico de ideo), AC_BE (para tráfico *Best Effort)* y AC_BK (para tráfico de *background)*. De esta manera, al contrario que en DCF donde todo el tráfico comparte una cola común, en EDCA cada tipo de tráfico se encola en su AC correspondiente. Ver Tabla 2.2.

Tabla 2.2: Mapeo de Prioridad de usuario a Categoría de Acceso

Prioridad	Prioridad 802.1D	Descripción 802.1D	Categoría de Acceso 802.11e	Descripción 802.11e
Menor	1	Background	AC_BK	Best Effort
...	2	-	AC_BK	Best Effort
...	0	Best Effort	AC_BE	Best Effort
...	3	Excellent Effort	AC_BE	Prueba Video
...	4	Carga Controlada	AC_VI	Video
...	5	Video	AC_VI	Video
...	6	Voz, Video	AC_VO	Voz
Mayor	7	Señalización Red	AC_VO	Voz

Fuente: Zhu, C. (2011). *Streaming Media Architectures, Techniques and Applicatios.*

Cada categoría de acceso dispone de su propia cola de transmisión caracterizada por unos determinados parámetros. La priorización entre las diferentes categorías se consigue configurando adecuadamente los parámetros de cada cola de acceso.

En la Figura 2.5 se presenta un esquema de funcionamiento del sistema de categorías de acceso. Los parámetros de mayor interés son los siguientes:

Número de Espacio Arbitrario entre Tramas (*AIFSN – Arbitrary Inter-Frame Space Number*), corresponde con el intervalo mínimo desde que el medio físico se detecta como vacío hasta que se comienza la transmisión.

Ventana de Contienda (*CW – Contention Window),* un número aleatorio se escoge en este rango para lanzar el mecanismo de espera (*backoff)*.

Límite de Oportunidad de Transmisión (TXOP *limit*), es la duración máxima durante la cual una QSTA puede transmitir tras haber obtenido el

TXOP.

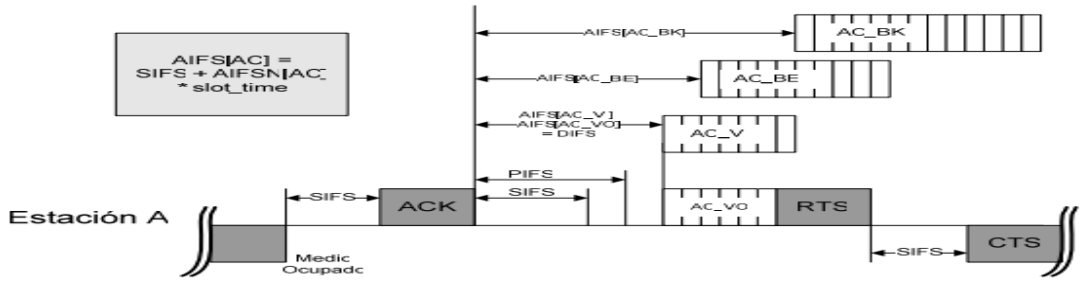


Figura 2.5: Modelo de funcionamiento de capa MAC 802.11e

Fuente: Zhu, C. (2011). *Streaming Media Architectures, Techniques and Applicatios*

Cuando los datos llegan al punto de acceso de servicio de información MAC (SAPMAC), la capa MAC de 802.11e se encarga de clasificar adecuadamente los datos, y envía la MSDU a la cola correspondiente. Entonces los bloques de información (MSDU) de las diferentes colas (AC) compiten internamente por el EDCA-TXOP.

El algoritmo de contienda interno calcula la espera (*backoff)* independientemente para cada cola (AC), según los parámetros descritos: AIFSN, CW, y un número aleatorio. El mecanismo de espera es similar al de DCF, y la cola con el menor *backoff* ganará la competición interna.

La cola (AC) vencedora competiría externamente por el acceso al medio inalámbrico. El algoritmo de contienda externo no se ha modificado significativamente comparado con DCF, excepto que en DCF el *backoff* y tiempos de espera eran fijos para un medio físico concreto, mientras que en 802.11e estos son variables, y se configuran adecuadamente según la cola (AC) correspondiente.

A través de un ajuste adecuado de los parámetros de las colas (AC), el rendimiento del tráfico de diferentes colas puede ser ajustado, y se puede lograr la priorización de tráfico. Esto requiere un punto de coordinación central (QAP) para mantener un conjunto común de parámetros en las colas y garantizar así un acceso justo entre las diferentes estaciones que componen la red (QBSS). De igual forma, para lograr ajustar la asimetría existente entre el tráfico de subida (QSTA a QAP) y de bajada (QAP a

QSTA), un conjunto separado de parámetros EDCA se define exclusivamente para el QAP.

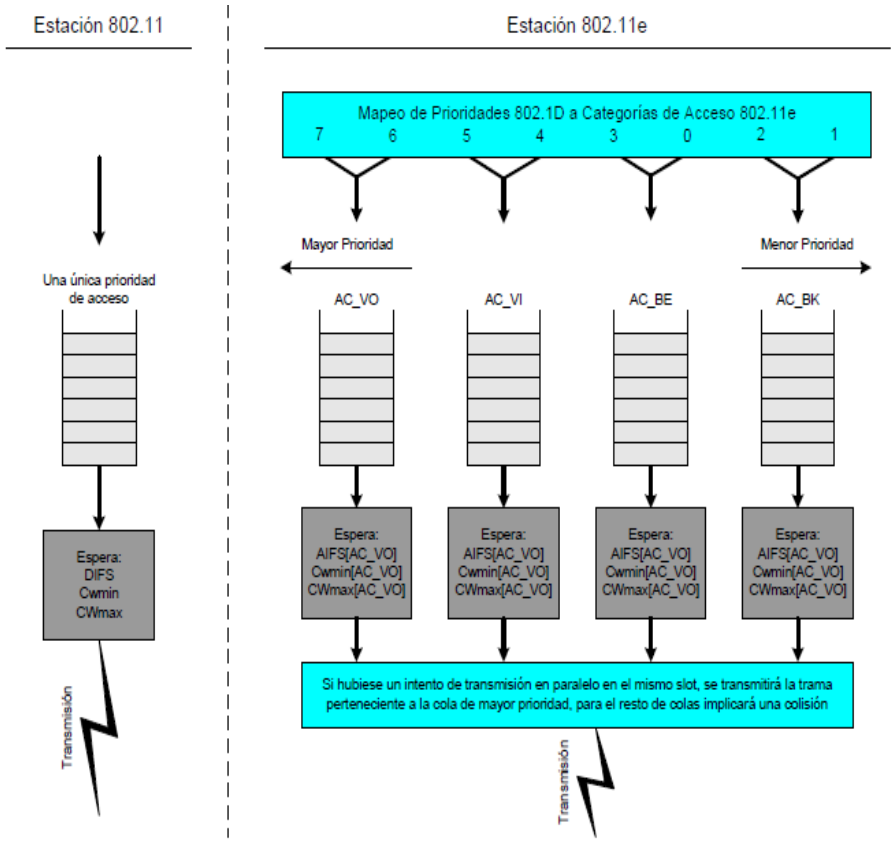


Figura 2.6: Comparación de mapeo de prioridades entre 802.11 y 802.11e

Fuente: Zhu, C. (2011). *Streaming Media Architectures, Techniques and Applicatios.* British Library.

Acceso al canal de forma coordinada HCCA

HCCA (HCF Controlled Channel Access), es un mecanismo de *polling* opcional, evolución del mecanismo PCF del estándar 802.11, en el que el punto de acceso controla todas las transmisiones desde y hacia las estaciones inalámbricas.

En este método existe una funcionalidad provista por un *Hybrid Coordinator* (HC, Coordinador Híbrido), generalmente ubicado en el *access point,* que permite al mecanismo HCCA la provisión de QoS parametrizada. El HC tiene una prioridad mayor para el acceso que las estaciones inalámbricas, algo necesario para poder asignar las oportunidades de transmisión a las estaciones en los períodos con o sin contención. Una QSTA, de acuerdo a sus requisitos, solicita TXOPs al

HC, tanto para sus propias transmisiones como para aquellas desde el QAP hacia ellas mismas. El coordinador híbrido, que normalmente se ubica en el QAP, o bien acepta o bien rechaza la petición basándose en los parámetros soportados por la QSTA.

El HCCA, cada QSTA puede establecer hasta ocho flujos de tráfico (*TS, Traffic Stream),* que se caracterizan por las Especificaciones de Tráfico (*TSPEC, Traffic Specification*) negociadas entre la QSTA y el QAP. Las TSPECs incluyen un conjunto de parámetros, la mayoría opcionales, que se utilizan para describir el tráfico y sus requisitos.

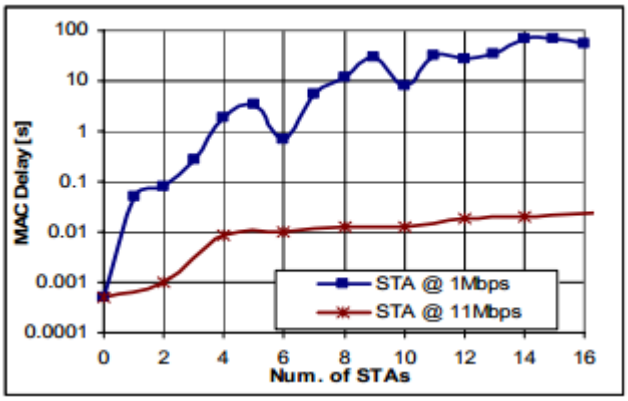
Los Campos principales de la TSPEC de un TS:

- Tasa de datos media (*R_i, Mean Data Rate)*
- Tamaño de la unidad de datos nominal del servicio (N_i, *Nominal Service Data Unit (SDU) Size)*
- Tamaño máximo de SDU, (M_i, *Maximum SDU Size)*
- La tasa mínima de la capa física (T_i, *Minimum* PHY *Rate)*
- Cota de retardo (D_i, *Delay Bound)*
- Intervalo máximo de servicio (MSI_i, *Maximum Service Interval)*

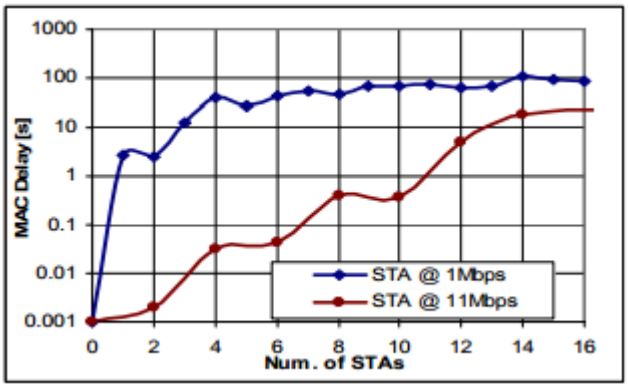
2.2.3. Limitaciones y mejoras del protocolo 802.11e.

Las mejoras propuestas en el estándar IEEE 802.11e soluciona los problemas de QoS del acceso de DCF. En consecuencia la Calidad de Servicio puede ser garantizada en un sistema homogéneo, o sea un sistema compuesto sólo por estaciones 802.11e en un entorno mixto con las estaciones con estándar 802.11 y 802.11e, puede provocar la reaparición de las limitaciones de Calidad de Servicio (QoS).

Dependiendo de la capa física que se adopte para el tráfico DCF los recursos a utilizar varían mucho y resultan con diferentes valores de retardo para el tráfico EDCA, como se muestra en la siguiente Figura 2.7.



a) Voz



b) Video

Figura 2.7: Retardo de las estaciones EDCA en función de número de estaciones DCF a) voz, b) video. Fuente: Majkonoski, J., & Casadovall, F. (s.f.). *Calidad de servicio en WLAN considerando un escenario mixto 8002.11e y 802.11b*.

Los nodos con estándar 802.11e sólo pueden empezar a transmitir en el caso de que la duración de la transmisión no sobrepase el inicio de la siguiente transmisión de la trama de *beacon.* En consecuencia puede entregarse un intervalo de tiempo, T_{free}, justo antes del inicio de la trama de *beacon* durante el cual solamente los nodos 802.11 podr.an competir por el acceso al medio.

Además de proveer las funcionalidades de EDCA y HCCA, el estándar 802.11e contiene otras mejoras en la capa MAC, así se tiene: a) ráfaga Libre de Contención (*Contention Free Burst - CFB*), b) Protocolo de Enlace directo (*Direct Link Protocol - DLP*), c) Nuevas reglas de acuse de recibo (*New Acknowledgement Rules)* y d) *Piggybackin.*

2.2.4 Provisión de QoS en redes inalámbricas

El servicio que ofrecen las redes inalámbricas es de tipo *best effort*, lo que hace que la velocidad real de la red sea baja. Proporcionar QoS en un canal inalámbrico es una tarea difícil de cumplir, puesto que este único canal tiene que ser compartido por los usuarios de la red, con una baja tasa de transmisión efectiva, no permitiendo distinguir cuáles son las aplicaciones que requieren de QoS de las que no. Tres son las herramientas que se consideran para proporcionar QoS: Diferenciación de recursos, configuración de la diferenciación de recursos y regulación.

a) Diferenciación de recursos: Aplicaciones diferentes requieren mecanismos diferentes.
b) Configuración de la diferenciación de recursos: Proporcionan configuración de los diferentes mecanismos en función de sus requerimientos.
c) Regulación: Supervisan el acceso a la red inalámbrica así como el comportamiento de los usuarios.

2.2.5 Calidad de Servicio (QoS) en redes inalámbricas

Hoy en día el IEEE 802.11 es el estándar más utilizado, lo que ha redefinido el significado de estar conectado. Sin embargo, dicho estándar no proporciona soporte de QoS para las aplicaciones multimedia. Esto ha llevado, debido al gran crecimiento de este tipo de redes, a que surjan nuevas organizaciones y grupos de trabajo que se encarguen de proponer estándares, definir nuevas tecnologías, que permitan diseñar un mecanismo que proporcione buenos niveles de QoS a estas aplicaciones.

Calidad de Servicio *(*QoS, *Quality of Service*) es un término usado para definir la capacidad de una red para proveer diferentes niveles de servicio a los distintos tipos de tráfico. Permite que los administradores de una red puedan asignarle a un determinado tráfico prioridad sobre otro y, de esta forma, garantizar que un mínimo nivel de servicio le será provisto.

Para comprender de mejor manera lo que es Calidad de Servicio, se cita una definición presentada por el TR-058 del DSL *Forum,* "Calidad de Servicio o QoS se refiere a la naturaleza de la provisión del servicio de entrega de tráfico diferenciado, que viene descrito por parámetros como ancho de banda obtenido, retardo de paquetes, y tasas de pérdida de paquetes."

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

Los requerimientos de calidad varían dependiendo de los usuarios y los servicios solicitados. En las redes IP la entrega de los paquetes se puede llevar minutos o eventualmente horas, como es el caso de la obtención de un archivo. Al navegar en la web o al solicitar acceso a una base de datos remota, la tolerancia podrá ser de segundos pero no de minutos. En aplicaciones demandantes tales como sesiones de chat o voz y video en tiempo real, sólo se toleran retardos de fracciones de segundos para satisfacer los requerimientos humanos, y algo también muy importante es el orden de llegada de los paquetes. Debido al desarrollo de estos nuevos tipos de aplicaciones (*streaming,* Voz sobre IP, videoconferencia, etc.), la necesidad de implementar técnicas de calidad de servicio se ha vuelto más evidente, enfocándose en su provisión.

El objetivo es evitar que la congestión de determinados nodos de la red afecte a algunas aplicaciones que requieren un determinado caudal o retardo, por ejemplo aplicaciones como video-vigilancia-IP.

Según Lloret, 2008, la Calidad de Servicio (QoS) desde la perspectiva del usuario, se basa en la percepción del servicio recibido, que se puede definir como:

- Disponibilidad de contenidos.
- Elección, facilidad de acceso e indexación del contenido disponible.
- Calidad del video y del audio.

- Resolución de audio y video.
- Interfaz de usuario.
- Paleta de colores, navegación, diseño.
- Descripción de programa, clasificación de género, actualización de programación hasta el último minuto.
- Entre otros servicios.

2.2.5.1 Factores que afectan la calidad de servicio

El administrador de la red al aplicar técnicas de Calidad de Servicio (QoS), puede tener control sobre los diferentes parámetros que definen las características de un tráfico en particular, y que pueden representar los principales problemas en cuanto a QoS en redes inalámbricas, entre los que se encuentran el *delay* (latencia), *jitter* (variación en el retardo), *packet loss* (pérdida de paquetes) y *bandwidth* (ancho de banda). A continuación se definen cada uno de ellos:

• *Delay (retardo o latencia):* es la cantidad de tiempo que tarda un paquete en alcanzar el destino después de ser transmitido desde el emisor. Este periodo de tiempo es conocido como “retardo de fin a fin” (*end-to-end delay*).

El retardo no es un problema específico de las redes no orientadas a conexión, es un problema general de las redes de telecomunicación.

• *Jitter*: se define como la diferencia entre el tiempo que llega un paquete y el tiempo en que se cree llegará el paquete, es la variación en el retardo, causada por congestión de red, pérdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino. Por ejemplo, si un paquete tiene 100 milisegundos de latencia y el siguiente paquete tiene una latencia de 130 milisegundos, entonces el *jitter* es de 30 milisegundos.

El *jitter* es un efecto de las redes de datos no orientadas a la conexión y basadas en la conmutación de paquetes. Como la información se divide en paquetes, cada paquete puede seguir una ruta diferente para llegar al destino.

• *Packet Loss (pérdida de paquetes)*: indica la cantidad máxima de paquetes que puede perder una red. Ésta no puede garantizar que todos los paquetes alcanzarán su destino. En determinados picos de carga, los paquetes serán eliminados por los *routers.*

• *Bandwidth (*ancho de banda*):* Es la cantidad de información o de datos que se envían a través de una conexión de red en un período de tiempo determinado. Los distintos tipos de aplicaciones compiten por el limitado ancho de banda. La falta de ancho de banda puede causar retardo, pérdida de paquetes y pobre performance para las aplicaciones.

Si una red estuviese vacía el tráfico de una aplicación debería conseguir cumplir con todos los parámetros anteriores, obtendría el *bandwidth* necesario, no perdería paquetes y tampoco sufriría *delay* ni *jitter.* Pero la realidad es diferente. Existen varias aplicaciones usando la red al mismo tiempo y por lo tanto, compitiendo por los recursos disponibles.

De los anteriores términos el más difícil de comprender es el *Jitter*, es por esto que a continuación se muestra la figura 2.8, para ayudar a entender su significado. Los paquetes A y B llegan al destino cada 50 milisegundos pero el paquete C tarda 90 milisegundos, 40 milisegundos más de retardo que los dos paquetes anteriores lo que provoca un *jitter* de 40 milisegundos.

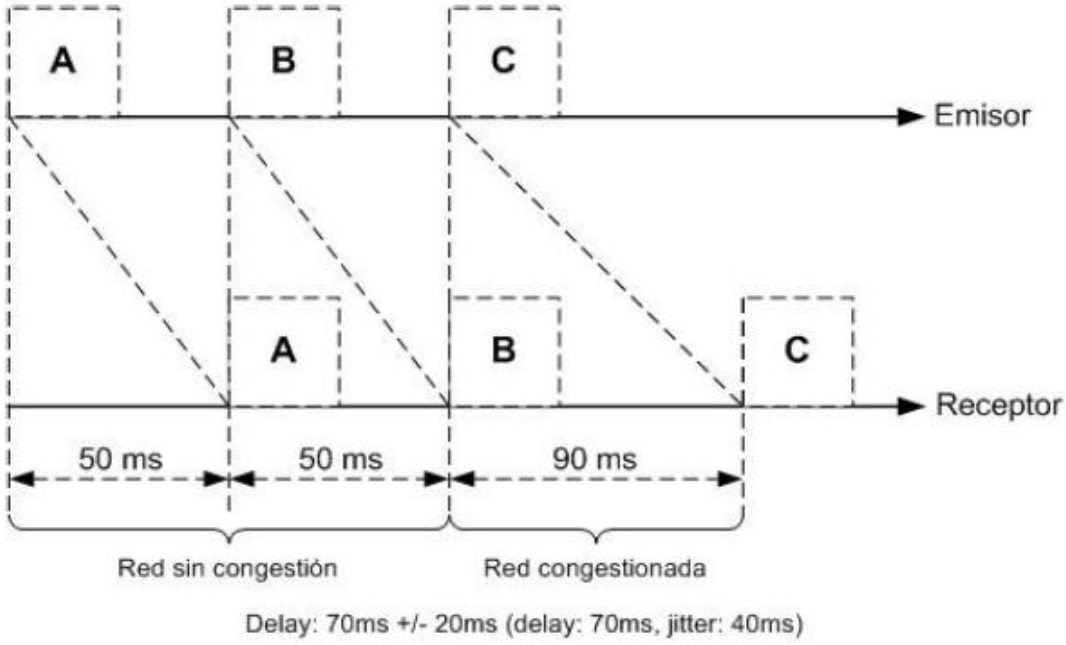


Figura 2.8: Jitter

Fuente: Zhu, C. (2011). *Streaming Media Architectures, Techniques and Applicatios.* British Library.

Con este contexto, el grupo de trabajo (*Working Group)* 802.11 ha aprobado un nuevo estándar, denominado 802.11e, que extiende dicho mecanismo para suministrar Calidad de Servicio (QoS*).* Este nuevo estándar se basa en una serie de parámetros a configurar, tema aún pendiente de ser resuelto pues si bien se proporcionan unos valores recomendados para dichos parámetros, estos valores son estáticos por lo que su idoneidad no está garantizada.

CAPÍTULO 3: PROTOCOLO DE INTERNET IPv4 e IP

Internet es una Red Global Púbica que utiliza el conjunto de protocolos TCP/IP, permite la comunicación instantánea de datos por todo el mundo entre cualquier persona, en cualquier lugar y en cualquier momento.

Internet ha dejado de ser una herramienta exclusivamente de comunicación patrocinada por el gobierno, ahora se presenta en un ambiente de comunicación de carácter comercial y que presta servicios.

En la Figura 3.1 se presenta la conexión de una red física a otra por medio de un computador que recibe el nombre de *router.* La suma de redes físicas distintas forma la red Internet.

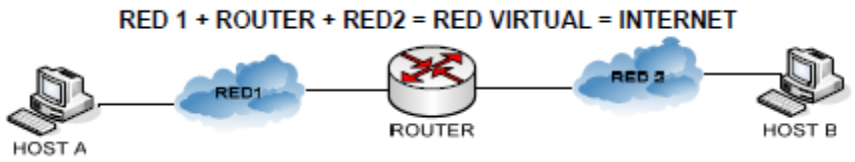


Figura 3.1: Conexión de una red física
Fuente: Curriculum CCNA, Cisco V3.1

En la Figura 3.2 se presenta la conexión de tres redes físicas conectadas mediante dos *routers.* Los *routers* tienen la opción de guardar una lista de todos los computadores y de todas las rutas y son los dispositivos que tienen la tarea de tomar complejas decisiones para permitir que todos los usuarios de todas las redes puedan comunicarse entre sí, enviando los paquetes de datos en base a la lista de referencia, este envío se basa en la dirección IP del computador de destino.

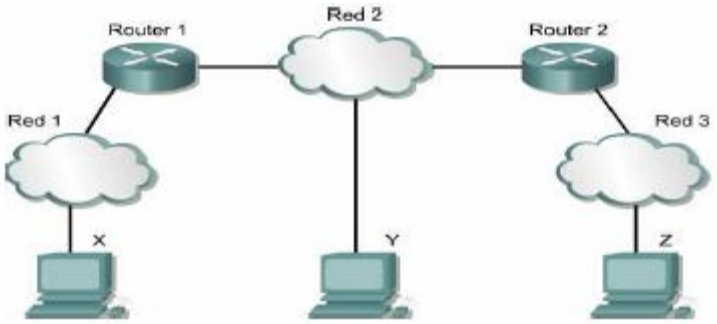


Figura 3.2: Conexión de una red física con dos *routers*
Fuente: Curriculum CCNA, Cisco V3.1

El TCP/IP es la base del Internet, es compatible con cualquier sistema operativo y con cualquier tipo de hardware, sirve para enlazar computadoras que pueden utilizar iguales o diferentes sistemas operativos, (Gil, Pomares, Candelas, 2010). Hay que considerar que en Internet se encuentran conectados ordenadores de clases muy diferentes, con hardware y software incompatibles en muchos casos.

TCP/IP es una familia de protocolos que proporcionan una comunicación entre nodos extremo a extremo. TCP proporciona los servicios a nivel de transporte e IP a nivel de red. TCP utiliza al IP para establecer comunicaciones fiables entre subredes de datos.

El protocolo IP es no orientado a conexión y no asegura la entrega de todos los datagrama de un mensaje. El protocolo TCP, que utiliza los servicios del IP, incluye los procedimientos necesarios para asegurar la transferencia de datos en forma correcta y ordenada (orientado a conexión), con lo que en conjunto, resultan adecuado para la transmisión segura de datos. (Moya, 2005)

La IETF (*Internet Engineering Task Force* – Grupo de Trabajo sobre Ingeniería de Internet) es una organización que establece reglamentos para transferir información a través de la red. A continuación se presenta algunos de los modelos que proponen para satisfacer la demanda de Calidad de Servicio (QoS) en las redes IP.

- *Int Serv (Integrated Services* – Servicios Integrales)
- *Diff – Serv (Differentiated Services* - Servicios Diferenciales)

- MPLS (*Multi Protocol Label Switching* – Multiprotocolo de Conmutación de Etiquetas)
- Ingeniería de Tráfico
- *Constrain – Based Routing* (Ruteo Basado en Restricciones)
- SBM (*Subset Bandwith Management* – Administración del Ancho de Banda de la Subred)

De acuerdo a los requerimientos de los usuarios, el administrador de redes puede disponer de las herramientas que proporcionan estos mecanismos.

Actualmente se están utilizando dos versiones del protocolo de Internet, la versión IPv4 y la versión IPv6.

3.1 Protocolo IPv4

IPv4 es la cuarta versión del protocolo *Internet Protocol* (IP), y la primera en ser implementada a gran escala, es el elemento común en la Internet de hoy. El actual y más popular protocolo de red es IPv4.

3.1.1 Características de IPv4

El protocolo de Internet IPv4, es un protocolo que se ubica en la capa 3 del modelo ISO/OSI y su función es entregar paquetes desde un nodo de origen a uno de destino, basado en la dirección escrita en cada paquete.

El protocolo de Internet versión 4 (IPV4) ha sido el principal protagonista del desarrollo y expansión de Internet en los últimos años. Sucesos como el aumento exponencial del número de equipos, a lo que hay que agregar indicadores como una mayor generación de tráfico y un elevado número de enlaces, han expuesto los problemas existentes actualmente. Todo lo anteriormente anotado, obliga a desarrollar nuevos servicios de telecomunicaciones que garantice una Calidad de Servicio (QoS) que permita sustentar las nuevas necesidades.

Hasta ahora para las conexiones a Internet, se utilizó el protocolo IPv4, el cual permite solo un número determinado de direcciones IP, que son la base para la conexión a la red. IPv4 tiene un espacio de direcciones 32 bits, es decir 2^{32} (4.294.967.296), agrupados en cuatro grupos de 8 bits,

por lo que el conjunto global va de la dirección 0.0.0.0 a la dirección 255.255.255.255; lo que en realidad es menos por las diferentes direcciones restringidas, debido a que las direcciones se asignan en bloques o subredes; o sea, se agrupan, se asigna a una empresa, a una institución, y todas ellas se consideran ya ocupadas, se usen o no. El direccionamiento IPv4 está casi agotado, lo que traería como consecuencia que el crecimiento en Internet se pararía, al no poder incorporarse nuevas máquinas a la Red.

Una de las primeras soluciones al problema de direccionamiento en IPv4 fue conocido como SIPP *(Simple IP Plus*), donde simplemente se aumentaba el tamaño de las direcciones IP a 64bits y se mejoraban ciertos aspectos de IPv4, como lo eran mejores estrategias de enrutamiento. SIPP era lo más cercano a lo que la Internet necesitaría después de unas modificaciones. Las direcciones pasaron de 64bits a 128 y se le asignó el nombre de IPv6 (IPv5 ya había sido asignado a otro protocolo, conocido como ST-2, que servía para soporte nativo de ATM en Internet). IPv6 ofrece un espacio de 2128 (340.282.366.920.938.463.463.374.607.431.768.211.456), IPv6 se presenta como un protocolo que soluciona o mejora las dificultades o problemas que tiene IPv4, (Mathon, 2004)

3.1.1.1 Cabecera de IPv4

El encabezamiento de IPv4 se compone de 20 octetos de información de control y organizados en extensión como se lo muestra en la Figura 3.3.

Figura 3.3: Encabezado IPv4 dividido en segmentos de 32 bits

Fuente: Boquera, M. C. (2003). *Servivios Avanzados de Telecomunicación.*

Cada campo proporciona la siguiente información:

Versión: (4 bits) define la versión actual del protocolo que es 4.

Cabecera (4 bits, *Internet Header Lenght*) este campo mide el largo del encabezado en segmentos de 32 bits. Todos los campos en IPv4 son fijos a excepción del campo de opciones.

Largo total: (16 bits) proporciona el largo del datagrama medido en octetos incluyendo el encabezado y el área de datos. Restando el IHL del Largo total se puede obtener el largo del encabezado.

Tipo de Servicio (TOS): este campo especifica cómo debe ser manejado el datagrama al pasar por los *routers.* Sus 8 bits se dividen como lo muestra la figura 3.4.

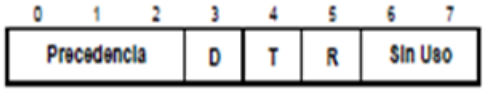


Figura 3.4: Subdivisión del campo tipo de servicio

Fuente: Boquera, M. C. (2003). *Servivios Avanzados de Telecomunicación.*

Los bits de *Precedencia* especifican la importancia relativa del datagrama, permitiendo al originador determinar diferentes prioridades a cada datagrama. Las 8 combinaciones posibles van desde la etiqueta de rutina (000) hasta “control de red” (111).

Los bits D, T, R, especifican el tipo de transporte que el datagrama desea. Cuando D=1 se requiere un bajo retraso mientras que D=0 requiere un retraso normal. Con T=1 se requiere un rendimiento (*throughput)* alto y con R=1 se requiere una alta confiabilidad. Es de entenderse que colocar los bits en un estatus determinado no garantiza que el parámetro requerido será cumplido a cabalidad. El transporte de información a través de Internet está restringido por un sin fin de factores que están, muchas veces, fuera del alcance del emisor de la información. Los bits 6 y 7 están reservados para usos futuros y su valor es cero por definición.

Los siguientes 32 bits del encabezado se encargan de manejar los procesos de fragmentación de datagramas

Identificador: (16 bits) contiene un número entero único que identifica al datagrama. Se debe recordar que cuando un *router* fragmenta un datagrama, este copia la mayoría de los campos del encabezado del datagrama en cada fragmento. El "identificador" debe ser copiado también. Su propósito principal es permitir al destinatario conocer cuál de los fragmentos que va recibiendo pertenece a cuál datagrama.

***Desplazamiento de fragmentación*:** (13 bits) este campo especifica el número de bits (offset) del datagrama original, medidos en unidades de 8 octetos, que están siendo acarreado por un fragmento determinado, empezando con un "offset" de cero. Para reensamblar el datagrama, el destinatario debe obtener todos los fragmentos, empezando con el que tenga el número cero hasta el fragmento con el offset más alto.

Banderas: (3 bits) estos bits se utilizan como controles para indicar de qué manera debe ser manejada la fragmentación. El bit 0 está reservado y se coloca en 0. El bit1 = 1 indica que el datagrama no se debe fragmentar y el bit1 = 0 indica que el datagrama puede ser fragmentado. Finalmente, el bit 2 = 0 indica que es el último fragmento, con su valor en 1, se asume que existen más fragmentos por llegar.

(TTL) Tiempo de vida: (8 bits) este campo especifica el tiempo, en segundos, que el datagrama puede permanecer viajando en Internet. Digamos que es el tiempo de supervivencia que tiene un datagrama dentro de Internet. Ya que es difícil medir con exactitud el tiempo el proceso real que siguen los *routers* es el de disminuir en uno el TTL cada vez que procesan el encabezado de un datagrama. En los casos de alta congestión, los *routers* pueden introducir largos retardos, pero para compensar esta situación, el *router* graba en memoria la hora a la cuál llega el datagrama y disminuye el campo TTL por el número de segundos que el datagrama permaneció dentro del *router* esperando por el servicio.

Protocolo: (8 bits) el valor del campo especifica cuál protocolo de alto nivel fue usado para crear la información que es llevada en área de DATOS del datagrama, es decir, especifican el formato del área de

DATOS. El mapeo entre el número y nombre de las aplicaciones es administrado por autoridades centrales con objeto de garantizar acuerdos dentro del Internet global.

***Checksum* de Encabezado:** (16 bits) este asegura la integridad en los valores del encabezado. El *checksum* se forma tratando el encabezado como una secuencia de enteros de 16 bits, sumándolos todos juntos utilizando el complemento a uno aritmético. Finalmente se toma el complemento a uno del resultado. Este *checksum* solo aplica a los bits del encabezado y no a los bits del área de datos.

Los campos **Dirección de Origen** y **Dirección de Destino** contienen las direcciones de 32 bits del emisor y del destinatario deseado respectivamente. Durante todo el trayecto del datagrama estos campos nunca modifican su valor.

Opciones IP: el campo de opciones no es requerido para todos los datagramas, su uso está más extendido para pruebas en la red y la eliminación de errores. Aún así, representa una parte integral del protocolo IP. Sus características incluyen funciones como el enrutamiento de datagramas sobre rutas predeterminadas, seguridad, identificación de los *routers* por donde viajó el datagrama, monitoreo de la manera en la que se está realizando el enrutamiento y situaciones similares.

3.1.1.2 QoS en IPv4

En IPv4 se utiliza el campo ToS (*Type of Service* – tipo de Servicio) para aplicar Calidad de Servicio (QoS).

En IPV4 la transmisión de bloques de datos llamados datagramas, tiene un cierto formato de encabezado que contiene cuatro puntos clave para proporcionar un servicio: tipo de servicio, tiempo de vida, opciones y suma de verificación. Entre ellos el que brinda la calidad de servicio es tipo de servicio.

3.1.1.3 Tipo de servicio de IPv4

El campo Tipo de Servicio (ToS) se utiliza para la aplicación de Calidad de Servicio (QoS), en el datagrama IPv4 este campo tiene una longitud de 8 bits, y se encuentra subdividido en 6 sub-campos, como se muestra en la Figura 3.5. Los tres bits del sub-campo Precedencia determinan la importancia o prioridad del datagrama y los ToS (*Type of Service*-Tipo de Servicio) deseado. Los valores de Precedencia definidos para IP que pueden aparecer en este sub-campo se muestran en la Tabla 1, estos valores permiten indicar al emisor la importancia del datagrama. Los siguientes 4 bits en donde D significa Retardo, T Desempeño, R integridad y C costo, tienen una interpretación que se presenta en la Tabla 3.1 Y 3.2, que se debe de tomar en cuenta en cada una de las pasarelas.

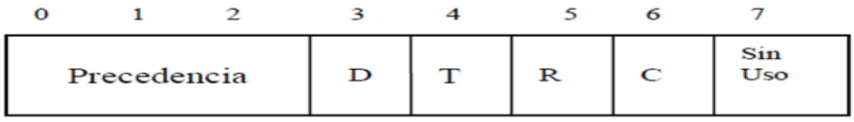


Figura 3.5: Sub-campos del campo Tipo de Servicio.
Fuente: Boquera, M. C. (2003). *Servivios Avanzados de Telecomunicación.*

Los bits D, T, R y C especifican el tipo de transporte deseado para el datagrama. Los bits: D, T y R, son los que definen, es decir desde el bit 3 al 5 de la fig. 1, e incluye el bit 6 al sub-campo de Sin Uso.

Una de las razones para colocar los cuatro bits: D, T, R y C, es la de minimizar el costo monetario en el envío de los datagramas.

Cuando el bit D se encuentra activo solicita un procesamiento con mínimo retardo, el bit T solicita un máximo desempeño, el bit R solicita una máxima confiabilidad, y el bit C un mínimo costo monetario.

Cuando estos bits se encuentran inactivos se está especificando un trato normal para el datagrama.

Los valores de los bits no pueden ser utilizados simultáneamente, de hecho los algoritmos de ToS eligen el “mejor” de ellos cuando existe más

de un bit activo, por lo tanto, la recomendación es utilizar sólo uno de estos bits.

Tabla 3.1: Nivel de precedencia IP

Valor de Precedencia IP	Nombre descriptivo
000	Normal o Rutinario
001	Prioritario
010	Inmediato
011	Urgente
100	Muy urgente
101	ECP (Emergency Call Processing) /Critico
110	Control entre redes
111	Control de red

Fuente: Boquera, M. C. (2003). *Servivios Avanzados de Telecomunicación*

Tabla 3.2: Bits del 3 al 6 del campo ToS

D	T	R	C	INTERPRETACION
1	0	0	0	Solicita un procesamiento con mínimo retardo
0	1	0	0	Solicita máximo desempeño
0	0	1	0	Solicita máxima confiabilidad
0	0	0	1	Solicita mínimo costo monetario
0	0	0	0	Especifica un trato normal para el datagrama

Fuente: Boquera, M. C. (2003). *Servivios Avanzados de Telecomunicación.* Madrid: Díaz de Santos S.A.

3.2 Protocolo IPv6

Durante años se han buscado nuevas formas de proporcionar calidad en las redes de computadoras. Sin embargo, a comienzo de los años 90 la IETF (*Internet Engineering Task Force* – Grupo Especial sobre Ingeniería de Internet) anunció la creación de los grupos de trabajo de "IP de próxima generación" *("IP Next Generation")* o (IPng) ya que se predijo que el agotamiento de IPV4 se daría entre el 2010 y el 2017. El límite en el número de direcciones de red admisibles restringe el crecimiento de Internet y su uso, especialmente en países densamente poblados.

La discusión técnica, el desarrollo e introducción de IPv6 no se ha realizado controversia. Incluso el diseño ha sido criticado por la falta de interoperabilidad con IPv4 y otros aspectos. Incidentalmente, IPng no pudo usar la versión número 5 como sucesor de IPv4, ya que ésta había

sido asignada a un protocolo experimental orientado al flujo de *streaming* que intentaba soportar voz, video y audio. Finalmente IPV6 se considera completamente testeado y disponible para producción desde 1999. La versión final de IPv6 está ya aprobada como estándar, y este estándar es considerado altamente estable y apropiado para un ambiente de producción, pero su adopción ha sido frenada por la Traducción de Direcciones de Red (NAT), que alivia parcialmente el problema de la falta de direcciones de IP. Algunas aplicaciones P2P, Voz sobre IP (VoIP), juegos multiusuarios, encuentran dificultades en su uso debido al NAT, que además termina con la idea de que todos pueden conectarse con todos.

Servicios como las conferencias multimedia o el comercio electrónico, exigen requisitos de Calidad de Servicio (QoS), difícilmente cubiertos por IPv4, todo ello ha conducido a la definición del protocolo IPv6

Actualmente el protocolo IPv6 es soportado por la mayoría de los sistemas operativos.

3.2.1 Características de IPv6

El protocolo IPv6 se presenta como la solución para muchas de las limitaciones de direccionamientos existentes en IPv4, pasando de 32 a 128 bits (cuadriplica la dirección), un tamaño que permitiría unas 1040 direcciones por cada persona del planeta.

IPv6 implementa soluciones más eficientes para ofrecer Calidad de Servicio (QoS) y Seguridad. Las ventajas y características que ofrece IPv6 entre las más importantes son:

- Arquitectura jerárquica de direcciones
- Convivencia con IPv4
- Autoconfiguración de equipos
- Computación móvil
- Seguridad e integridad de datos

- Calidad de Servicios, QoS
- Soporte de audio y video, permite establecer rutas de alta calidad
- Nueva etiqueta de flujo para identificar paquetes de un mismo flujo
- No se usa *chesksum*, ni fragmentación, ni reensamblado
- Nueva versión de ICMP y desaparición del IGMP
- Soporte a tráfico multimedia en tiempo real
- Aplicaciones *multicast y anycast*
- Mecanismos de transición gradual de IPv4 a IPv6

Tabla 3.3: Resumen de características de IPv6

Direccionamiento:	Direcciones de 128 bits asignadas jerárquicamente
Encaminamiento:	Jerárquico. Agregación de rutas
Prestaciones:	Cabecera simple alineada a 64 bits
Versatilidad:	Formato flexible de opciones. Extensibilidad mejorada
Multimedia:	Identificador de flujos
Multicast:	Obligatorio, control de ámbitos
Seguridad:	Soporte autentificación/cifrado obligatorio (IPSec)
Autoconfiguración:	3 métodos PnP
Movilidad:	Mejora de la eficiencia y seguridad

Fuente: 6SOS. (2004). *El protocolo IPv6*.

En IPv6 se utilizan los campos TC (*Traffic Control* – Control de Tráfico) y el campo Etiqueta de Flujo.

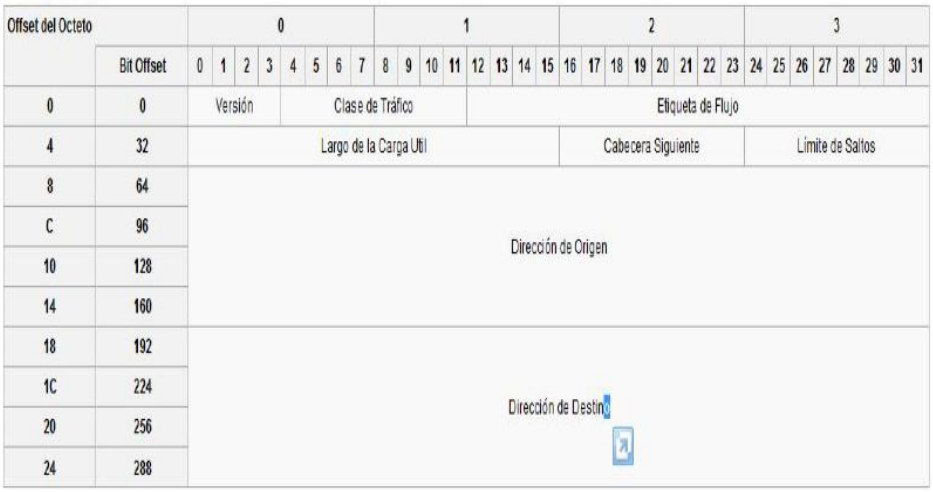


Figura 3.6: Estructura de un paquete de IPv6
Fuente: "www.implementacionipv6.utfsm"

Ventajas

- No hay limitación en el número de opciones.
- Mejora de prestaciones debido a la ordenación de cabeceras.
- Cabeceras procesadas por *routers.*
- Cabeceras procesadas en destino.
- Definición precisa del comportamiento frente a opciones desconocidas.

Para aplicar Calidad de Servicio (QoS*)* en las versiones 4 y 6 de IP se utilizan los campos de sus encabezados.

Se incluyen opciones que facilitan el tratamiento de los flujos de información. Un flujo se define como una secuencia de paquetes enviados desde un origen particular a un destino particular y para el cual el origen desea un tratamiento especial por parte de los dispositivos de encaminamiento. Desde el punto de vista del origen un flujo está constituido por una secuencia de paquetes generados por una misma aplicación y que requieren los mismos servicios. Desde el punto de vista de los dispositivos de encaminamiento, un flujo es una secuencia de paquetes que comparten una serie de exigencias en el tratamiento que se les debe suministrar (asignación de recursos, seguridad, etc.).

Una aplicación puede generar varios flujos, cada uno de ellos con diferentes requisitos (por ejemplo en una videoconferencia, se tiene un

flujo de audio y otro de video). Para identificar los paquetes pertenecientes a un mismo flujo, estos incorporan una etiqueta de flujo en la cabecera.

Para incrementar la eficiencia del procesado de los paquetes en los dispositivos de encaminamiento, se ha asignado a la cabecera una longitud fija y el número de sus campos se ha reducido. Las funciones de carácter suplementario se introducen en unas cabeceras separadas opcionales, denominadas cabeceras de extensión, que en la mayoría de los casos no necesitan ser examinadas ni procesadas por los dispositivos de encaminamiento. Sólo se permite la fragmentación de los paquetes por parte de la fuente, pero no por los dispositivos de encaminamiento, con lo que se incrementa su velocidad de operación.

3.2.2 Cabecera IPv6

A manera de comparación con el encabezado de IPv4, el datagrama (o paquete) de IPv6 es llevado hasta las redes locales de manera muy parecida a como lo hace IPv4.

Sin embargo, el encabezado de IPv6 consta de el encabezado base, cabecera principal o cabecera IPv6, seguida de las cabeceras de extensión opcionales (Figura 3.7) y por último de la carga útil, que contiene una unidad de datos del protocolo del nivel superior (por ejemplo del protocolo de transporte). La parte opcional, puede ser incluida o no como parte del paquete IPv6, dependiendo del tipo de aplicación que se desee transmitir. Con o sin el encabezado, el tamaño original del *Frame* de la red local debe ser respetado como en IPv4.

Figura 3.7: Formato del encabezado de IPv6

Fuente: 6SOS. (2004). *El protocolo IPv6*.

El encabezado base de IPv6 que se presenta en la Figura 3.8 consta de 40 octetos de información, con ocho campos y dos direcciones. Comparado con el encabezado IPv4 que consta de 20 octetos divididos en 10 campos, dos direcciones y un bloque de opciones. Aunque tiene una longitud superior a la cabecera de IPv4, el número de campos es menor (tiene un costo de procesamiento menor), el incremento de longitud responde a la mayor cantidad de octetos que ocupan las direcciones.

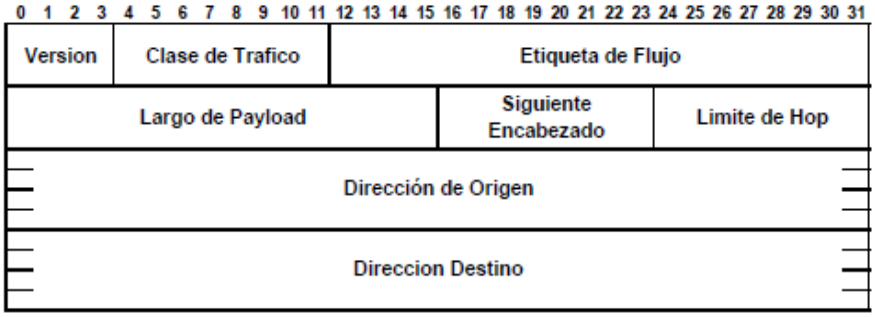


Figura 3.8: Encabezado base de IPv6

Fuente: Zhu, C. (2011). *Streaming Media Architectures, Techniques and Applicatios.* British Library.

Campo de Versión: (4 bits)

Simplemente identifica la versión del protocolo. Para IPv6 debe ser por supuesto igual a 6.

Cabe mencionar que este es el único campo consistente en función y posición con respecto a IPv4. Al estar al inicio del paquete permite una rápida identificación y envío del paquete para su apropiado procesamiento, ya sea IPv4 o IPv6.

Campo de Clase de Tráfico: (8 bits)

Su función es la de proporcionar la información a los *routers* intermedios o a los Hosts para identificar y distinguir las diferentes clases o prioridades de paquetes IPv6. Este campo sustituye al llamado Tipo de Servicio en IPv4 y su función se conoce como “servicios diferenciados”. El RFC 2474 y el 2475 discuten el concepto de servicios diferenciados, dividiéndolos en dos categorías: una que trata con el envío de paquetes en sí mismo y otra que trata con las políticas que determinan los parámetros usados en la

ruta de envío de los paquetes. Los acuerdos a los que se llegue para el uso de este campo deben tener carácter de estándares debido a su alcance global. Hasta el momento no existe una recomendación específica de los valores que debe tomar este campo para sus diferentes aplicaciones, pero los RFCs definen algunos criterios generales que deben seguirse para la implementación de códigos específicos en este campo. Las guías generales más importantes para el uso de este campo se describen a continuación:

La estructura del campo de Clase de Tráfico debe contener 6 bits para utilizarse como código de identificación de una aplicación o servicio diferenciado, lo cual proporciona 64 posibles combinaciones para 64 diferentes opciones de servicio. Los últimos dos bits quedan reservados para usos futuros y se colocan con valor de cero.

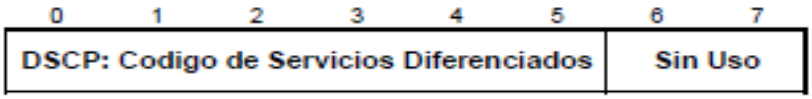


Figura 3.9: Estructura del campo de Clase de Tráfico

Fuente: Zhu, C. (2011). *Streaming Media Architectures, Techniques and Applicatios.* British Library.

Etiqueta de Flujo: (20 bits)

Este campo puede ser utilizado para realizar un manejo especial de ciertos paquetes, como lo serían los que requieren soporte para servicios en tiempo real. Todos los paquetes que pertenezcan al mismo “flujo” de información deberán llevar las mismas direcciones origen y destino, así como la misma etiquete de flujo. Un ejemplo de estos flujos sería el audio o el video. Si no se requiere ningún tratamiento especial para el manejo de los datos, la etiquete de flujo debe ser colocada con solo ceros. Al igual que el campo de clase de tráfico, la etiqueta de flujo se encuentra bajo experimentación y no se tiene un estándar definido y su uso puede cambiar a medida que madure la tecnología. El RFC 1809 proporciona los detalles de las últimas investigaciones para el uso de este campo.

Largo de *Payload*: (16 bits)

Este campo mide el largo, en número de octetos, de la carga útil o "*payload"* del paquete, es decir, la información que no pertenece a los encabezados. Entonces el largo total máximo para el *payload* de IPv6 es de 65,535 octetos. La utilización de "*Jumbo payloads*" mayores a 65K también es permitida en IPv6 pero su interpretación es manejada por los encabezados opcionales.

Encabezado Siguiente: (8 bits)

Se encarga de identificar el tipo de encabezado que sigue inmediatamente al encabezado IPv6. Los valores utilizados para la identificación son los mismos que los usados en el campo de protocolo de IPv4. Por ejemplo TCP se representa con el valor 6, UDP con el 17 etc.

Límite de *Hops:* (8 bits)

Equipara la función del campo TTL en IPv4. Su valor se disminuye en una unidad cada vez que pasa por el procesamiento de un nodo. Si el campo llega a cero, el paquete se la opción de ser medido tanto en segundos como en número de nodos o *hops* que atraviesa, pero en IPv6 la opción de medición de tiempo no está disponible.

Direcciones Origen y Destino: (128 bits)

Como en IPv4, estos campos se encargan de dar una identificación única a los nodos origen y destino de la información, solo que ahora su largo es 4 veces más grande en tamaño y millones de veces mayor en capacidad de direccionamiento.

Extensiones del Encabezado IPv6

El diseño de IPv6 simplifica al encabezado de IPv4 colocando muchos de los actuales campos en la parte del encabezado opcional. De esta manera no es necesario procesar siempre todas las opciones, lo cual permite una reducción en el "*overhead*" del paquete. Así, el paquete IPv6 puede contener una o varias extensiones. El orden en que se deben colocar las extensiones está sugerido en el RFC 2460 y se ilustra en la Figura 3.10.

Figura 3.10: Extensiones del encabezado IPv6

Fuente: Ahuatzin, G. (s.f.). *Desarrollo de un esquema de traducción de direcciones IPv6-IPv4-IPv6*.

Encabezado Hop by Hop y Opciones IPv6:

Este campo lleva información que debe ser examinada por todos los nodos a través del *path* de entrega del paquete. La presencia de este encabezado se identifica cuando el campo “Encabezado Siguiente” del encabezado base de IPv6 contiene solo ceros. El formato para la parte de ”opciones” de este encabezado y del Encabezado de Opciones Destino, también tiene su propio formato como se puede ver en la Figura 3.11.

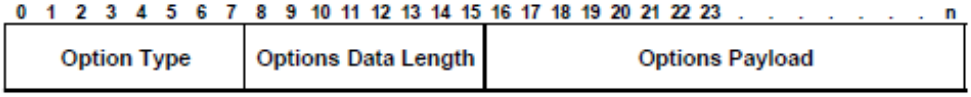


Figura 3.11 Formato de las opciones IPv6

Fuente: Ahuatzin, G. (s.f.). *Desarrollo de un esquema de traducción de direcciones IPv6-IPv4-IPv6*.

Encabezado de Destino

Este lleva información opcional que debe ser examinada solo por el nodo destino del paquete. Esta opción se identifica en el campo “*Next Header*” del encabezado base de IPv6 por el código 60. Las opciones definidas hasta el momento son: Pad1, utilizada para insertar un octeto de *padding*

dentro del área de opciones del encabezado y PadN, utilizada para insertar dos o más octetos dentro del área de opciones del encabezado.

Encabezado de Ruteo

Para un emisor, IPv6 retiene la habilidad de especificar una ruta definida que debe seguir el paquete enviado. A diferencia de IPv4, esta funcionalidad es entregada por los encabezados opcionales, en este caso, el de ruteo. El formato se muestra en la Figura 3.12.

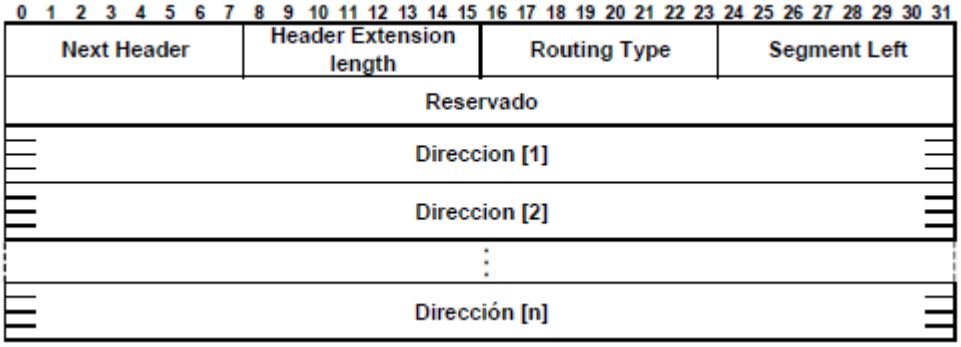


Figura 3.12: Formato de encabezado de ruteo (Tipo 0)

Fuente: Ahuatzin, G. (s.f.). *Desarrollo de un esquema de traducción de direcciones IPv6-IPv4-IPv6*.

El campo *Next Header y Next Header Length* funcionan de la mima manera que con las opciones anteriores, el campo *Routing Type* especifica una variante específica del encabezado. A la fecha la variante definida se conoce como *Routing type* 0, la cual indica una lista ordenada de las direcciones que deben ser “visitadas” hasta la entrega final del paquete en su destino (un buen ejemplo del uso de este encabezado de ruteo se encuentra en el RFC 2460). El campo *Segments Left* indica el número de nodos que faltan por ser visitados antes de llegar al destino final.

Encabezado de Fragmentación:

Como en IPv4, IPv6 hace los arreglos necesarios para que el paquete se fragmente y sea reensamblado en su destino final, de acuerdo al tamaño del paquete y al tamaño del *Maximum Transmisión Unit* (MTU) de las redes por donde debe pasar. Pero IPv6 hace un cambio en el procedimiento con respecto a IPv4. La fragmentación IPv6 se restringe al

emisor original. Antes de enviar tráfico, el nodo emisor debe realizar un *Path MTU Discovery* para identificar el MTU más pequeño a lo largo del *path* hasta el destino. Así, IPv6 fragmenta el datagrama original de manera que cada fragmento sea de un tamaño menor al más pequeño de los MTUs a lo largo del *path* de transmisión. El formato del encabezado se muestra en la Figura 3.13. Teóricamente, el uso de fragmentación "*end to end*" está motivado porque permite reducir el *overhead* y hacer más rápido el ruteo gracias a la reducción en el procesamiento necesario para manejar la fragmentación.

Sin embargo, las rutas de IPv6 no pueden cambiar de manera tan fácil como lo hacen en IPv4, lo cual introduce una limitante importante para la concepción del actual Internet.

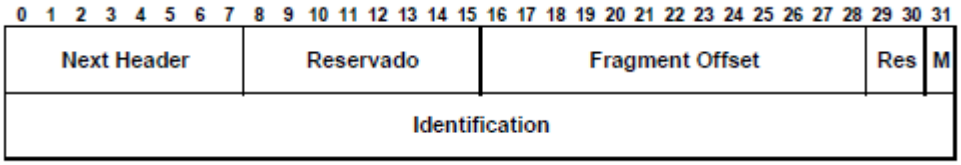


Figura 3.13: Formato del encabezado de fragmentación.
Fuente: Ahuatzin, G. (s.f.). *Desarrollo de un esquema de traducción de direcciones IPv6-IPv4-IPv6*.

El campo de *Next header*, se maneja de la misma manera que con los encabezados anteriores. El campo reservado se inicializa con ceros y está destinado para usos futuros. El campo de *Fragment Offset* mide precisamente el tamaño del "*offset"* o distancia en el corrimiento en los bits, en unidades de 8 octetos, en relación con el inicio de la parte fragmentable del paquete original. El campo *Res* está también reservado para uso futuro y la bandea M se coloca en 1 para indicar si más fragmentos están por llegar y en 0 cuando el último fragmento ha arribado. El campo de *Identification* La parte fragmentable del paquete incluye el *payload* del paquete y el encabezado que preceden al de fragmentación, mientras que la parte no fragmentable se compone del encabezado base y los encabezados anteriores al de fragmentación.

Encabezado de Autenticación

Los siguientes encabezados están diseñados para proporcionar seguridad en la transmisión de información pero con la característica de que trabajan al nivel de capa 2, es decir, son independientes de las aplicaciones de alto nivel. El encabezado de Autenticación está diseñado para proveer integridad de los datos y autenticación de la fuente u origen de los datos. Su formato se muestra en la Figura 3.14. Aquí los campos de *Next Header y Reserved* trabajan de la misma manera que en los anteriores encabezados.

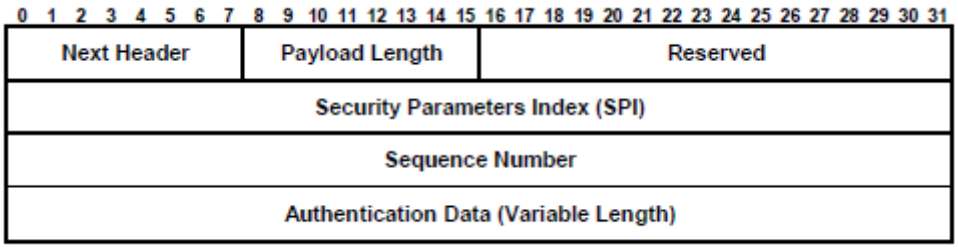


Figura 3.14: Encabezado de autenticación

Fuente: Rivasainz, A. (2006). *Impactos de implementación del protocolo IPv6 para el proveedor de servicios de telecomunicaciones*.

El campo de *Payload length* proporciona el tamaño del campo de autenticación en espacios de 32 bits, menos 2. El valor mínimo es 1 y se aplica cuando se tiene un algoritmo de autenticación “nulo” o inexistente. El campo SPI, es un valor arbitrario de 32 bits que identifica la *security association* (SA) para este datagrama, relativa a la dirección de IP destino que está contenida en el encabezado IP con el cual el encabezado de seguridad está asociado. Además está en relación también al protocolo utilizado. La *security association* es una simple conexión lógica con propósitos de seguridad. El campo de *Sequence Number* es un contador de 32 bits inicializado en cero y que se incrementa de manera monótona durante una transmisión segura. Finalmente, el campo de *Authentication Data* posee una tamaño variable en múltiplos de 32 bits que contiene el *Integrity Check Value (ICV),* el cual, puede ser utilizado como código de identificación y es donde se puede implementar el algoritmo de autenticación, que podría ser, por ejemplo, el intercambio de claves secretas.

Encabezado de Seguridad y Encapsulamiento del *Payload* (ESP)

Aunque el encabezado de autenticación puede proporcionar una fuente confiable y una información confiable, no puede evitar que la información sea leída de manera pasiva durante su trayecto. El encabezado de seguridad y encapsulamiento del *payload* está diseñado para proveer además de lo anterior, una limitada confidencialidad en el flujo de tráfico. Los servicios ofrecidos por este encabezado dependen de la "asociación de seguridad" establecida y de su implementación. Algunos de los campos de este encabezado son obligatorios mientras que otros son opcionales, como se muestra en el formato de la Figura 3.15.

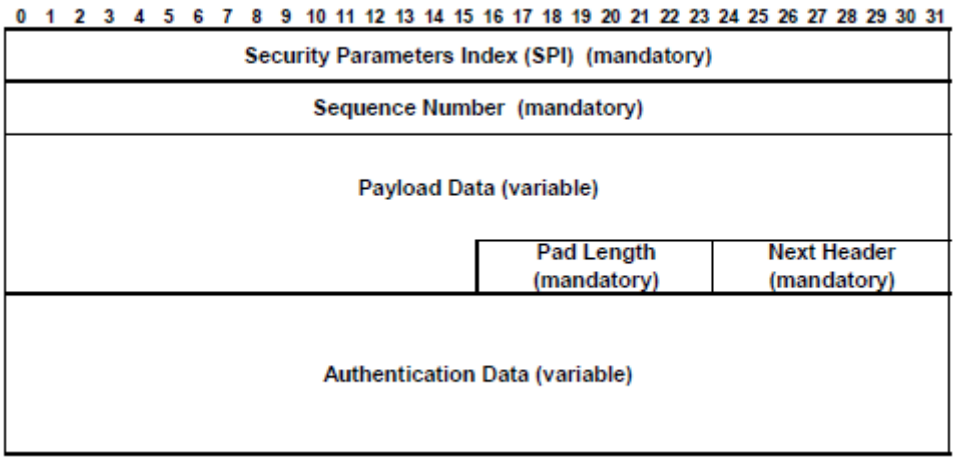


Figura 3.15: Encabezado de *encapsulating security payload (ESD)*

Fuente: Rivasainz, A. (2006). *Impactos de implementación del protocolo IPv6 para el proveedor de servicios de telecomunicaciones*.

Los campos SPI y *Sequense Number* se definen de la misma manera que en el encabezado de autenticación. El campo *Payload Data* contiene los datos descritos por el campo *Next Header*. El campo de *Padding* puede contener de 0 a 255 octetos de información. Su contenido depende de la implementación del algoritmo de seguridad deseado. El campo de *Pad Length* indica el número de octetos de información del campo que le precede. El campo *Next Header* de ocho bits, identifica al encabezado siguiente al encabezado ESP. Finalmente el *Autentication Data* es un campo de longitud variable que contiene el *Integrity check value (ICV.)*

Este valor se incluye solo si el servicio de *security association* ha sido seleccionado.

Los detalles de implementación de la función de seguridad, sus formatos, encriptación, etc. se pueden encontrar en los RFC's 2401, 2402, 2403, 2405,2406, 2411 entre otros.

Se espera ampliamente que IPv6 sea soportado en conjunto con IPv4 en un futuro cercano. Los nodos solo-IPv4 no son capaces de comunicarse directamente con los nodos IPv6, por lo que necesitan de la ayuda de un intermediario.

3.3 Mecanismos de transición a IPv6

El agotamiento de las direcciones IPv4 es una realidad. *El proceso de cambio a* IPv6 ya ha comenzado de una forma paulatina, nodo por nodo, sin un orden específico de actualización, haciendo que ambos protocolos tengan que convivir durante un largo tiempo. La integración y la coexistencia de IPv6 con IPv4 es un requisito para permitir la transición gradual. Migrar a IPv6 la Internet actual, que está basada en IPv4 se lo considera a través de un conjunto de mecanismos que pueden implementar los nodos IPv6 con el fin de ser compatibles con los nodos IPv4.

Se conocen 3 técnicas de transición: *Dual-Stack*, túneles y mecanismos de translación. Pueden ser usadas en combinación unas con otras.

3.3.1 Dual-Stack

Esta técnica más que un mecanismo de transición es un mecanismo de integración, que se conceptualiza en el modelo TCP/IP en donde cada host y *router* cuenta con un soporte completo para el protocolo IPv4 e IPv6. Cada nodo es configurado con ambos protocolos, por lo que pueden interactuar con nodos IPv4 usando mensajes IPv4 y con nodos IPv6 usando paquetes IPv6, sin necesidad de realizar costosos procesos de encapsulación o translación. Cada nodo de red tendrá dos direcciones de red una IPv4 y otra IPv6. Son llamados "nodo IPv4/IPv6".

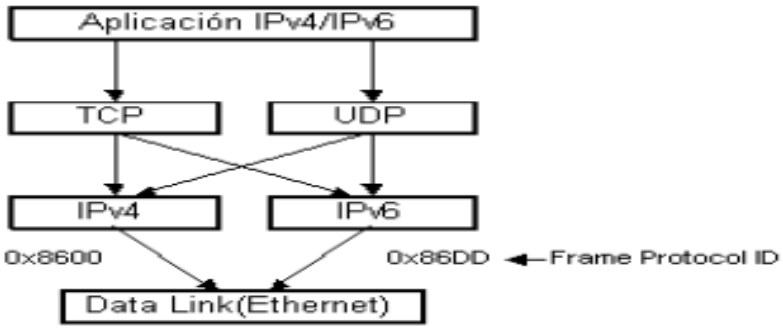


Figura 3.16: Nodo Dual-Stack

Fuente: Rivasainz, A. (2006). *Impactos de implementación del protocolo IPv6 para el proveedor de servicios de telecomunicaciones*.

El segundo mecanismo es conocido como tunelización.

3.3.2 Túneles

Esta técnica permite que dos *routers* IPv6 que están interconectados a través de *routers* IPv4, se comuniquen entre sí utilizando paquetes IPv6 a través del establecimiento de un túnel entre ambos. El conjunto de *routers* IPv4 intermedios pasan a ser parte del túnel. Permite que redes IPv6 aisladas se puedan comunicar sin necesidad de reemplazar la estructura de ruteo IPv4 entre ellas. Esta solución permite enviar paquetes IPv6 sobre una estructura IPv4. (Ternera, 2010).

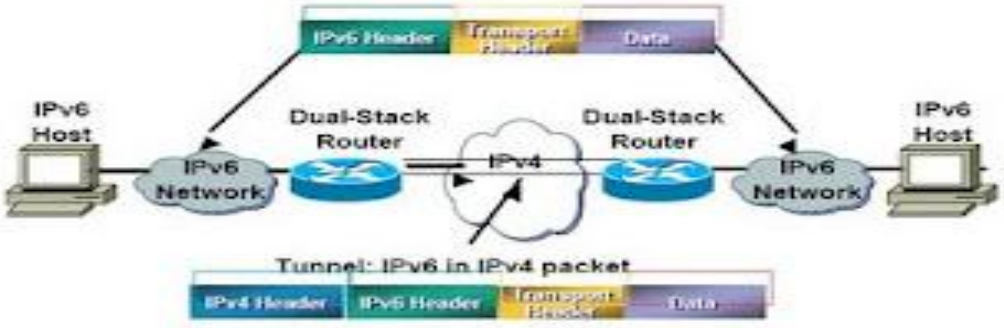


Figura 3.17: Túnel IPv6 en IPv4

Fuente: Rivasainz, A. (2006). *Impactos de implementación del protocolo IPv6 para el proveedor de servicios de telecomunicaciones*.

Los paquetes IPv6 son encapsulados por un *router dual stack* y enviados por una red IPv4. El *router* inicial del túnel le agrega una cabecera IPv4, en la cual las direcciones origen y destino son las correspondientes a las de inicio y fin del túnel. El *router* donde finaliza el túnel es el encargado de

desencapsular el paquete IPv6 (eliminando la cabecera IPv4) y retransmitirlo hacia el destino final. Los túneles pueden ser configurados o automáticos.

3.3.2.1 Túneles Configurados

La utilización de túneles en el *backbone* es la menos eficiente y permite una solución en el corto plazo que no escala. Ofrecer servicios IPv6 con túneles dentro de la red del proveedor vuelve complejos los diagnósticos, afecta la disponibilidad de los servicios IPv6 y dificulta la adecuada utilización de los recursos (enlaces y *routers*). En estos casos los túneles son configurados manualmente.

Esta clase de túneles punto-a-punto necesitan configuración manual por parte de los administradores de la red y el punto final del túnel es determinado por la información de configuración ingresada en el nodo que encapsula. Ambos extremos del túnel deben ser configurados. Todos los túneles manuales son bidireccionales. Por lo tanto, un nodo debe mantener información por cada túnel que se le configura. Estos túneles son creados, en general, para comunicar en forma permanente dos redes IPv6 aisladas usando la infraestructura de ruteo IPv4. Los dos extremos del túnel debe ser *dual-stack* y, aunque esos extremos pueden ser un host y un *router*, usualmente son dos *routers.*

Esta solución debe ser considerada como transitoria y no la implementación definitiva en la red.

La utilización de túneles manuales es denominada túneles configurados para diferenciarla de otras técnicas de túneles automáticos.

3.3.2.2 Túneles Automáticos

Los túneles automáticos permiten a los nodos enviar tráfico IPv6 por una red IPv4 sin tener que pre-configurar, manualmente, un túnel. Al utilizar direcciones IPv6 compatibles con IPv4, el nodo encapsulador puede determinar la dirección IPv4 del final del túnel automáticamente de la dirección IPv6, y por lo tanto, no se necesita configuración manual de los extremos del túnel que, obviamente, deben ser *dual-stack.*

En la Figura 3.18 se muestra como se forman estas direcciones, donde los últimos 32 bits corresponden a la dirección IPv4 del nodo destino.

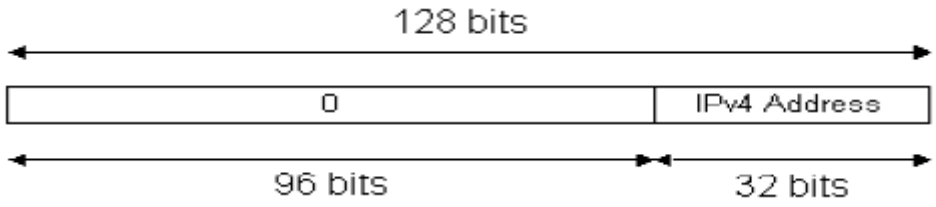


Figura 3.18: Estructura dirección IPv4-compatible IPv6
Fuente: Robles, M. *QoS en redes wireless con IPv6*

Una dirección IPv4-compatible es globalmente única siempre que la dirección IPv4 no pertenezca al espacio de direcciones privadas de IPv4.

En la Figura 3.19 se muestra como un *host* que soporta este tipo de direcciones, al enviar un mensaje a la dirección ::A319:021E, el nodo encapsulador determina la dirección IPv4, 163.25.2.30, automáticamente de la dirección IPv6.

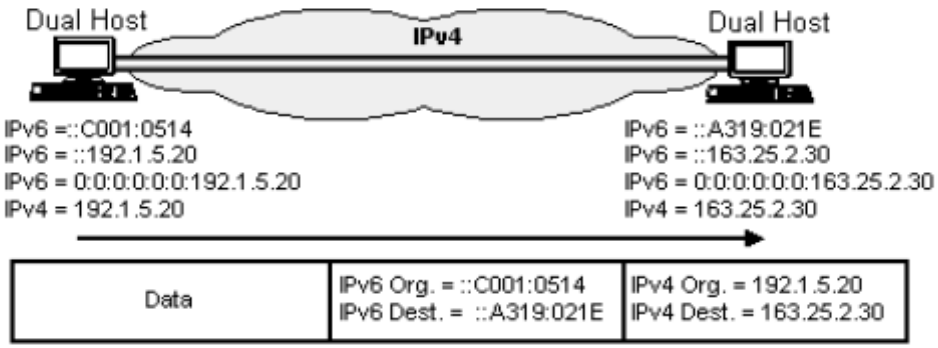


Figura 3.19: Túneles Automáticos
Fuente: Robles, M. *QoS en redes wireless con IPv6*

3.3.2.3 Túneles 6to4

Este método es un tipo de túnel automático *router-to-router*. Comienzan con un prefijo que se basa en un rango de direcciones reservado por la IANA: 2002::/16, y los siguientes 32 bits son ocupados por la dirección IPv4 del *router*. Esto permite construir un prefijo /48, con lo cual, una

organización dispone de los siguientes 16 bits para administrar localmente.

Para poder comunicarse por Internet, la dirección IPv4 debe ser única globalmente.

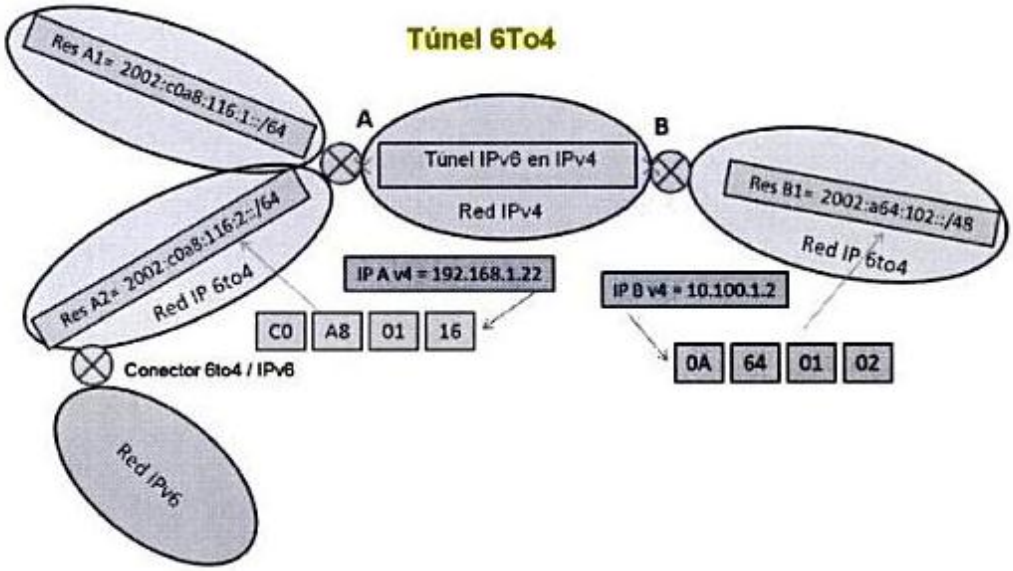


Figura 3.20: Túnel 6to4
Fuente: Robles, M. *QoS en redes wireless con IPv6*

Las interfaces de túnel simplemente tienen la necesidad de una dirección origen, ya que las direcciones de destino se obtienen automáticamente a partir del destino de un paquete: la dirección IPv4 de salida del túnel se utiliza para construir el número de red de destino. Cuando se enrutan varias redes, se utiliza un sufijo complementario para diferenciarlas, (Dordoigne, 2011).

Este tipo de túnel sólo permite relacionar redes 6to4. Si se quieren conectar redes IPv6, es necesario utilizar un conector específico (6to4/IPv6).

Un *router* utiliza la dirección IPv4 embebida en la dirección destino IPv6 para determinar el otro extremo del túnel.

Para establecer este tipo de túneles cada dominio IPv6 requiere un *router dual-stack* que automáticamente construya el túnel. Estos *routers r*eciben el nombre de *6to4 Relay Router*. Se recomienda que cada *router* tenga una sola dirección 6to4 asignada a su interface externa. Dentro del sitio se puede utilizar un protocolo de ruteo IPv6, fuera de éste se continúan utilizando los protocolos de ruteo IPv4. De esta forma, un número arbitrario de sitios 6to4 pueden comunicarse entre ellos sin necesidad de configurar túneles manuales.

Difieren de los túneles automáticos, explicados en el punto anterior, en que este método permite formar prefijos de red y direcciones para un único host (aunque se recomienda que sea utilizado para configurar prefijos), mientras que el anterior, únicamente permite formar direcciones asignables a un nodo en particular

3.3.2.4 Túnel 6over4

Está definido en RFC 2529, permite que nodos IPv6 aislados se conecten, en un mismo link, utilizando direcciones *multicast* IPv4 mediante túneles automáticos. El túnel establecido es como un link virtual entre los nodos 6over4 en una red IPv4. Las direcciones IPv4 *multicast* son usadas para ejecutar el proceso *Neighbor Discovery*. No ha tenido mucho éxito y su utilización se desaconseja.

3.3.2.5 Túnel Broker

En esta solución, un nodo *dual-stack*, ubicado en un red IPv4, se conecta a un servidor *web,* ingresa información de autenticidad y recibe un *script* que al ejecutarlo establece un túnel IPv6-en-IPv4 al servidor túnel *broker.* Éste puede ser visto como un ISP IPv6 virtual.

A diferencia de la solución 6to4, el Túnel *Broker* es adecuado para pequeños sitios IPv6 aislados o hosts IPv6 en una red IPv4 que quieren comunicarse con una red IPv6.

3.3.3 Mecanismo de translación

Para que un nodo en una red IPv6 se pueda comunicar con un nodo remoto en una red IPv4 debe usar los mecanismos de translación. Dentro

de estos, se encuentra NAT-PT, *Network Address Translation - Port Translation*, que realiza un mapeo de direcciones IPv6 en direcciones IPv4 modificando la cabecera de los paquetes. Este proceso es similar al NAT tradicional realizado entre direcciones públicas y privadas del protocolo IPv4.

3.4 Modelos de servicios.

Durante años se han buscado nuevas formas de proporcionar calidad en las redes de computadoras, por ello la IETF, ha propuesto modelos que ofrecen QoS en diferentes modalidades. Por este motivo se presentará conceptos, características, arquitecturas de los protocolos IPv4 e IPv6 para garantizar la QoS en las redes IP.

Las posibilidades de comunicación interactiva son incrementadas por las diferentes aplicaciones que se disponen, por lo que se cuenta con modelos que satisfacen los niveles de QoS dependiendo de la necesidad del usuario, teniendo que considerarse también parámetros como la latencia y el ancho de banda.

Actualmente se están utilizando dos versiones del protocolo de Internet, la versión IPv4 y la versión IPv6.

Para aplicar QoS en las versiones 4 y 6 de IP se utilizan los campos de sus encabezados.

Actualmente, Internet ofrece un servicio *best-effort*, sin garantía de QoS, por lo que es necesario contar con mecanismos con el fin de proporcionar un servicio adecuado.

3.4.1 Servicio de mejor esfuerzo

Éste es el nivel que proveen las redes IP y, por consiguiente, es el modelo que se utiliza en Internet. La red hará todo lo posible por enviar cada paquete hasta su destino, pero no da ninguna garantía de que eso suceda. Una aplicación puede enviar todos los datos que desee en cualquier momento sin solicitar permiso o notificar a la red. Determinadas aplicaciones, como FTP o HTTP, pueden utilizar este modelo sin mayores

inconvenientes, pero no es un modelo óptimo para otro tipo de aplicaciones.

Con la aparición de aplicaciones de multimedia con requisitos de tiempo real (videoconferencia, telefonía, etc.) este modelo no es válido, creándose la necesidad de dotar a las redes de Calidad de Servicio.

3.4.2 Servicios Integrados (*IntServ)*

IntServ, 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 para poder operar apropiadamente. Los routers que se encuentran a lo largo del camino, entre el origen y el destino, reservan los recursos de red necesarios antes de que la aplicación comience a operar. Estas reservaciones se mantienen hasta que la aplicación termina o hasta que el ancho de banda requerido por ésta sobrepase el límite reservado para dicha aplicación.

Cuando recibe una solicitud de recursos, la red ejecuta un proceso de control de admisión. Mediante este mecanismo, la red comprueba que está en condiciones de satisfacer los requerimientos solicitados. Si es así, se realiza la reserva de recursos en los *routers,* que se mantiene hasta que la aplicación termine la transmisión. En caso contrario, la reserva no se puede hacer y se rechaza la conexión.

El mecanismo para llevar a cabo el modelo *IntServ* es el RSVP (*Resource Reservation Protoco*, RFC 2205l) es el protocolo que puede ser usado por las aplicaciones para enviar los requerimientos de QoS del *router.*

El protocolo de Reserva de Recursos crea y mantiene un estado específico para cada flujo de información, tanto en los nodos finales, como en los nodos intermedios, por los que pasan las conexiones. La clave de RSVP es reservar recursos en cada nodo por donde transitarán los paquetes o flujos de datos.

Este método tiene la desventaja de que para cada flujo de información que lo requiera es necesario hacer una reserva de recursos en los

routers, lo que puede producir que, ante una gran demanda de servicios, un *router* no pueda satisfacer todos los pedidos. No es una solución escalable, por lo cual no es adecuada para grandes entornos como Internet.

3.4.3 Servicios Diferenciados *(DiffServ*)

Una manera de entregar Calidad de Servicio (QoS), es diferenciar entre el conjunto de paquetes que circulan por la red. Este modelo tiene como objeto tratar a los paquetes de manera diferente, tomando la decisión de cómo procesarlo de acuerdo al contenido del encabezado del paquete.

Los *routers* de borde son los encargados de marcar los paquetes que entran a la red. El procesamiento que reciban los paquetes dentro de la red depende de la clase en la que fueron ubicados.

El marcado consiste en modificar los primeros 6 bits del campo DS *(DiffServ)* llamado DSCP (*DiffServ Code Point).* DS suplanta las definiciones de los campos *Type of Service* de la cabecera IP y *Traffic Class* de IPv6. Cada uno de los posibles valores de DSCP puede significar una forma diferente de tratar los paquetes por parte de los *routers*. A cada una de las formas de tratar los paquetes se lo conoce como *Per-Hop Behavior (PHB).*

3.5 Herramientas de Calidad de Servicio (QoS)

Un paquete que entra en un *router* debe tener disponible las siguientes herramientas básicas para tener QoS.

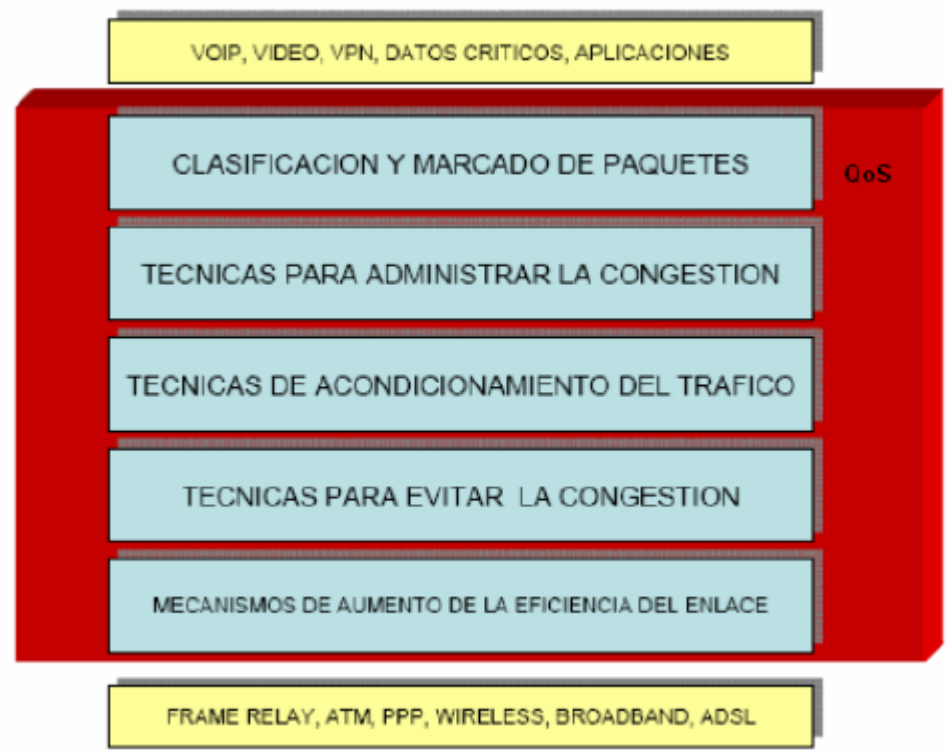


Figura 3.21: Herramientas básicas de diseño de QoS
Fuente: Robles, M. *QoS en redes wireless con IPv6*

3.5.1 Marcado y clasificación de paquetes

El marcado de paquetes es una forma de señalar paquetes con un identificador interno que más tarde se puede usar para el criterio de las reglas de filtrado y traducción. Esto permite diferenciar entre los diferentes tráficos y así poder brindar un servicio diferenciado.

El proceso debe efectuarse en la periferia (bordes) de la red de modo de contar lo antes posible con los criterios necesarios para preservar la calidad requerida.

Luego que el paquete se ha podido clasificar se le debe asignar algún atributo color o marca que permita su tratamiento posterior a partir de este parámetro marcado. Modifica el campo *DiffServ* (DS), que ocupa los primeros 6 bits del campo *Type of Service en IPv4 y Traffic Class* en IPv6.

Clasificación: el grupo o clase al que pertenecen cada uno de los paquetes depende del valor con el que fueron marcados. Cada uno de

esos agrupamientos recibirá un tratamiento diferente, de acuerdo a las políticas especifica dependiendo de la clase a la que pertenece.

3.5.1.1 Herramientas para el marcado y clasificación para la Calidad de Servicio (QoS).

Marcación basada en clases o clasificadores: Se aplica a nivel de los sistemas operativos de los dispositivos de red .Los mismos hacen un filtrado de los paquetes para identificar el tráfico a priorizar. En función de diversos criterios aplican condiciones por ejemplo asignando una marca DSCP o clasifican los paquetes interesantes para tratamiento de encolado. Finalmente aplican determinada política al vaciado de los buffers de salida en función de marcas recibidas o reclasificadas a los paquetes basada en información adicional a la dirección de destino IP, por Ejemplos: marcar todo el tráfico VoIP con DSCP *Expedited Forwarding* y el resto con default, sacar los paquetes DSCP EF con prioridad absoluta enviando solo paquetes de VoIP a la línea en caso de que haya tráfico VoIP y encolando el resto en otros buffers que hasta podrían llegar a desbordarse.

Tasa de acceso comprometida (*Committed Access Rate*) CAR: Esta herramienta permite el marcado, clasificación y/o el descarte de los paquetes que exceden ciertos umbrales configurables. La política CAR agresiva se aplica según lo especificado en un “contrato” con los usuarios de la red que posee al menos dos componentes, la velocidad bps y en tamaño de las ráfagas, si el tráfico que se recibe es conforme al “contrato” entonces es transmitido pero si se ha excedido del contrato CAR puede descartarlo directamente.

Ruteo basado en políticas: Esta herramienta permite a los nodos rutear ejemplo con el conocimiento de la topología del sistema se podría llegar a enrutar el tráfico no solo en base al destino IP sino por caminos específicos que garanticen una mayor calidad de servicio.

El ruteo basado en Políticas también tiene la posibilidad de marcar y puede estar basado en la métrica del ruteo, el origen de la información o

la interfaz que debe seguir el tráfico de esa clase. El ruteo basado en políticas puede marcar IP *Precedence,* grupos de Calidad de Servicio (QoS), o bits ToS.

3.5.2 Técnicas para el acondicionamiento del tráfico

Uno de los factores que afecta el retardo variable de los paquetes es la serialización y envío al siguiente nodo.

Si el largo de los paquetes no es analizado y acondicionado, las aplicaciones que utilicen paquetes de gran tamaño retrasan inevitablemente al resto de las aplicaciones. Los paquetes de voz y video no pueden sufrir retardos más allá de ciertos valores recomendables. Surge entonces la necesidad de controlar el envío de los paquetes al nodo siguiente de la red minimizando el retraso que provocan los paquetes “grandes”.

Los retardos introducidos en un nodo son función de la velocidad del enlace de salida y del tamaño del paquete.

3.5.3 Técnicas para la administración de la congestión

Los recursos limitados de los nodos (capacidad de *buffers* de entrada y salida, capacidad de procesamiento de paquetes por segundo) deben ser usados dando un tratamiento al tráfico en forma diferencial en función de la calidad de servicio asociada a cada uno.

Si se tuviera recursos ilimitados en los nodos (capacidad de buffer, ancho de banda de los enlaces y capacidad de procesamiento), no sería necesario establecer tratamientos diferenciados a los paquetes transmitidos. Pero como este escenario no es posible la administración de congestión se empieza a aplicar exclusivamente en el caso de congestión del nodo.

Las técnicas de administración consisten en el encolamiento según diferentes técnicas que de alguna manera ordenan los paquetes recibidos para situarlos en diferentes colas de salida. Esto genera en cada nodo

una selección del orden y cantidad de bytes que se tomarán de cada cola para transmitir hacia el siguiente nodo.

Las diferentes técnicas son conocidas por el nombre del proceso de ordenamientos de cola y cada uno de los algoritmos de encolado apunta a resolver un tipo específico de problema, afectando con ello el desempeño de la red.

Las técnicas más conocidas de encolamiento son:

Primero en entrar primero en salir FIFO: *First In First Out.*
• Encolamiento prioritario PQ: *Priority Queuing.*
• Encolamiento de despacho CQ: *Custom Queuing*.
• Encolamiento limpio ponderado WFQ*: Weighted Fair Queuing*.
• Encolamiento limpio ponderado basado en clases CBWFQ: *Class Based Weighted Fair Queuing.*
• Encolamiento prioritario / Encolamiento limpio ponderado PQ/WFQ.
• Encolamiento de bajo Retardo LLQ: *Low Latency Queuing*.

3.5.4 Técnicas para evitar la congestión

Estas técnicas monitorean la carga de tráfico en un esfuerzo por anticiparse y evitar posibles congestiones. El método consiste básicamente en descartar paquetes antes de que se tenga una congestión del tráfico. Existen dos formas de descartar el tráfico *Tail Drop* donde no se configura ni controla ningún aspecto y *Random Early Detection (*RED, WRED y FRED) que selectivamente (en algunos casos) descartan de forma preventiva paquetes para evitar la congestión.

Descarte de cola (*Tail Drop*): Es la respuesta por defecto de todo sistema, cuando la cola de salida se completa, todos los paquetes que intentan entrar en la parte final de la cola (*tail*) son descartados hasta que se elimina la congestión.

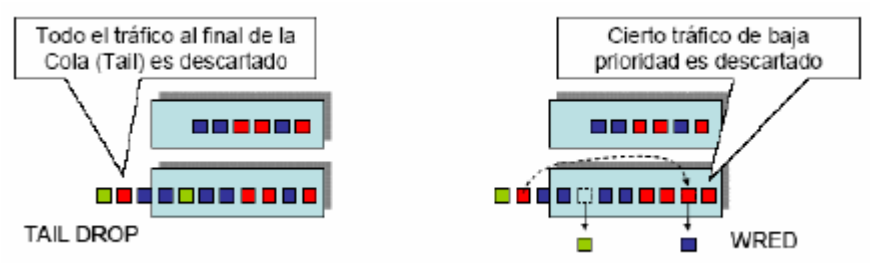


Figura 3.22: Descarte de paquetes TAIL DROP

Fuente: **"**www.implementacionipv6.utfsm"

Detección aleatoria temprana (*Random Early Detection*) RED: Procede a un descarte de paquetes al azar bajo ciertas condiciones de tráfico con la finalidad de evitar una congestión. RED no toma en cuenta el tipo de tráfico que descarta, por si sola, no brindaría ningún beneficio al tráfico prioritario de paquetes de voz puesto que si llegara a descartar paquetes de voz estaría afectando negativamente la calidad de la misma.

Por tanto se requiere identificar que paquetes serán candidatos al descarte y cuáles no, esta selección se logra mediante una variante llamada WRED.

Detección aleatoria temprana ponderada (*Weighted Random Early Detection*) WRED: asocia la probabilidad de descarte al tipo de tráfico, evitando entonces que se descarten paquetes de voz. WRED combina RED con precedencia IP y DSCP logrando descartar paquetes en forma selectiva.

Detección aleatoria temprana basada en flujos (*Flow Based Random Early Detection)* FRED: Es otra técnica de descarte que clasifica los paquetes en función de los flujos (en función del origen destino, puertos TCP etc.). De esta forma da un tratamiento en relación con el flujo del tráfico.

• Flujos no adaptativos, no responden a la congestión (UDP).
• Flujos robustos que en promedio tienen una velocidad uniforme y reducen su velocidad en respuesta a la congestión.

Debido al comportamiento del descarte de paquetes en FRED, todos los flujos son susceptibles de ser descartados.

FRED determina en realidad que flujos están monopolizando el uso de recursos y los penaliza más fuertemente. FRED mantiene una cuenta del número de flujos activos que existen en una interfaz de salida. Dado el número de flujos y el tamaño total del buffer disponible, FRED determina el número de buffers disponibles por flujo.

3.5.5 Mecanismos de aumento de la eficiencia del Enlace

Las razones para vigilar y mejorar la eficiencia del enlace se deben a:

• Controlar el ancho de banda necesario en ciertos casos.

Ejemplo: si un enlace PVC *Frame Relay* dispone de un ancho de banda en el sitio central de 2 Mbps pero de sólo 128 Kbps en el extremo, entonces se debe restringir el tráfico por dicho PVC desde el sitio central a solo 128 Kbps de modo de no saturar el sistema del sitio receptor. Esto implica aplicar una política de tráfico que debe restringir la velocidad de uso a valores que están por debajo del ancho de banda disponible en la interfaz.

• Regular el flujo del tráfico

Ejemplo: optimizar el envío de los paquetes sensibles al *jitter* y retardo, de modo que se pueda obtener una velocidad de recepción sincrónica regular de los mismos, acorde a las condiciones de diseño de un códec y no beneficiar al tráfico de ráfagas.

Combinado con el manejo de prioridad de colas, los mecanismos de aumento de la eficiencia del enlace (*traffic shaping*) brindan niveles aceptables de calidad de servicio en ambientes sujetos a políticas de descarte de paquetes en los nodos de tránsito.

CAPÍTULO 4 ANÁLISIS COMPARATIVO DE LA CALIDAD DE SERVCIO (QoS) QUE OFRECE IPv4 e IPv6

La norma 802.11, constituye en la actualidad la tecnología más extendida como red de acceso inalámbrica, por las ventajas que ofrece. Sin embargo, éstas redes tienen que enfrentar constantemente muchos desafíos, entre los que tenemos: mejorar su desempeño para requerimientos específicos, teniendo que brindar a la vez privacidad, seguridad para aplicaciones administrativas, financieras, de gestión, optimizar el tamaño de tramas en función de las condiciones del canal, favorecer la movilidad, lo que representa un área muy activa en lo que a investigación y desarrollo compete. Con el fin de adaptarse a estos requerimientos, ya que el protocolo original 802.11 no soporta Calidad de Servicio (QoS), aparecen nuevos estándares o modificaciones a lo ya existente, orientado a favorecer el desempeño de las diferentes redes, particularmente de aquellas que soportan Calidad de Servicio (QoS), donde se presentan nuevas características De todo esto se deduce la necesidad de integrar las herramientas que toda ésta tecnología ofrece.

4.1 Análisis de requerimientos de las aplicaciones

La integración de servicios de voz, video y datos sobre una misma infraestructura, tópicos analizados en el capítulo uno, ha generado la necesidad de tener que brindar servicios de prioridad explícita y un servicio de ancho de banda garantizado para el tráfico de señalización, para cumplir con la Calidad de Servicio (QoS). Por ejemplo de acuerdo a Cisco, para VoIP, la calidad de voz directamente se ve afectada por la pérdida de paquetes, el *jitter* y la latencia. La pérdida de paquetes causa el recorte de voz o saltos en la comunicación, La latencia puede causar la degradación de la calidad de la voz si es excesiva, haciendo incómodo mantener una conversación. Para tener una calidad alta, la pérdida de paquetes no debe ser superior al 1 por ciento, y la latencia no debe ser mayor a 150 ms y el *jitter* debe ser menor a 30 ms. Para obtener Calidad de Servicio para video, hay que considerar los dos principales tipos de tráfico que existen son: videoconferencia y *streaming* de video, para

marcar Calidad de Servicio (QoS) el exceso de tráfico de la videoconferencia puede ser marcado por un filtro de control, la pérdida de paquete no debe ser mayor al uno por ciento y la latencia de una vía no debe ser mayor de 150 ms. Cuando se utiliza cisco se debe garantizar el ancho de banda mínimo para el tamaño de la sesión de video conferencia, más el 20 por ciento.

Con el fin de reconocer y comparar las características de Calidad de Servicio (QoS) que ofrecen la versión 4 y 6 de IP, se realiza el análisis comparativo de diferentes proyectos realizados.

Según Robles, M. 2008, en su trabajo de tesis, la tecnología IPv4 tal como se la ha concebido no ofrece ningún tipo de garantías de Calidad de Servicios (QoS). Servicio como el telefónico, presenta exigentes requisitos de retardo y variación del retardo (*jitter*), convirtiendo en un problema la provisión de Calidad de Servicio (QoS) en este tipo de redes móviles, con una tendencia cada vez mayor de movilidad y de transmisión de datos. Se tiene la necesidad de integrar las herramientas provistas por IPv6 con las suministradas en las redes inalámbricas, a través de la especificación IEEE 802.11e, para brindar Calidad de Servicio (QoS).

La propuesta en su tesis es la de proveer Calidad de Servicio en redes inalámbricas usando el campo *Flow Label* que se encuentra en la cabecera de los paquetes IPv6. Este campo puede contener distintos valores que serán mapeados en alguna de las cuatro colas que se encuentran definidas en el estándar 802.11e. M. Robles, 2008, explica que el campo *Flow Label* de un tamaño de 20 bits, se encuentra especificado en el documento original de IPv6 pero su utilización no está determinada en una forma concreta. Al quedar su definición, en cierta forma abierta, es posible modificarlo para plantear nuevas alternativas en la manera de utilizarlo. Para cumplir su objetivo muestra un ejemplo. A partir de una topología de red determinada se realizan dos simulaciones, utilizando el simulador NS-2 versión 2.28. en la primera simulación no se aplica Calidad de Servicio (QoS) y la segunda sí la tiene. Luego, los resultados de ambas simulaciones son comparados.

Como primer ejemplo se realizará la prueba utilizando una red de tipo ad-hoc, formada por 6 nodos móviles, que generan cinco conexiones, cada una genera igual cantidad de tráfico por segundo. Ver Tabla 4.1.

Tabla 4.1: Definición de tráficos

Tráfico	Origen	Destino	Inicio(seg.)	Prioridad
Tráfico_0	3	0	40	2
Tráfico_1	4	1	0	3
Tráfico_2	5	2	30	1
Tráfico_3	1	3	20	2
Tráfico_4	2	4	10	0

Fuente: Robles, M. *QoS en redes wireless con IPv6*

En la Figura 4.1, se muestra el resultado obtenido al no aplicar ningún parámetro de Calidad de Servicio. Se presentan cuatro tráficos, el primero se inicia en el instante 0 de la simulación, los otros tres cada 10 segundos. El ancho de banda al final se comparte de manera similar entre todos los tráficos. A medida que se van agregando nuevas conexiones se observa que el rendimiento se va degradando.

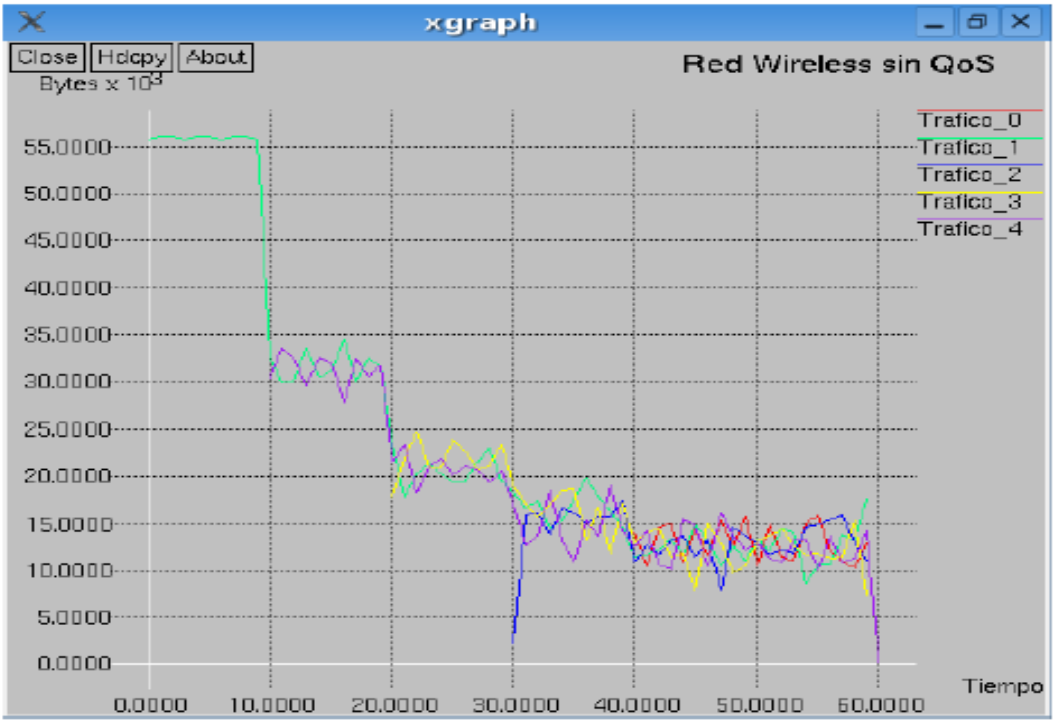


Figura 4.1: Simulación sin Calidad de Servicio

Fuente: Robles, M. *QoS en redes wireless con IPv6*

En la Figura 4.2 se muestra el resultado de ejecutar el mismo script ejecutado en el caso anterior, con la diferencia de que cuenta con técnicas de Calidad de Servicio, o sea IEEE 802.11e. En el tiempo 0 se inicia el tráfico _1 con prioridad 3 (menor prioridad), utiliza 556 Kbytes/s, hasta que a los 10 segundos se inicia la siguiente conexión, que tiene la máxima prioridad, o sea prioridad 0, lo que le permite obtener el mayor ancho de banda durante toda la simulación. En el tiempo 20, con prioridad 2 se inicia el Tráfico_3. Mientras el Tráfico_4 mantiene su tasa de transferencia. El Tráfico_1 va disminuyendo su rendimiento debido al Tráfico_3. El Tráfico_4 es el que más ancho de banda consume, de los 56 Kbytes/s con que parte, disminuye aproximadamente 10 Kbytes/s entre los 30 y 40 segundos.

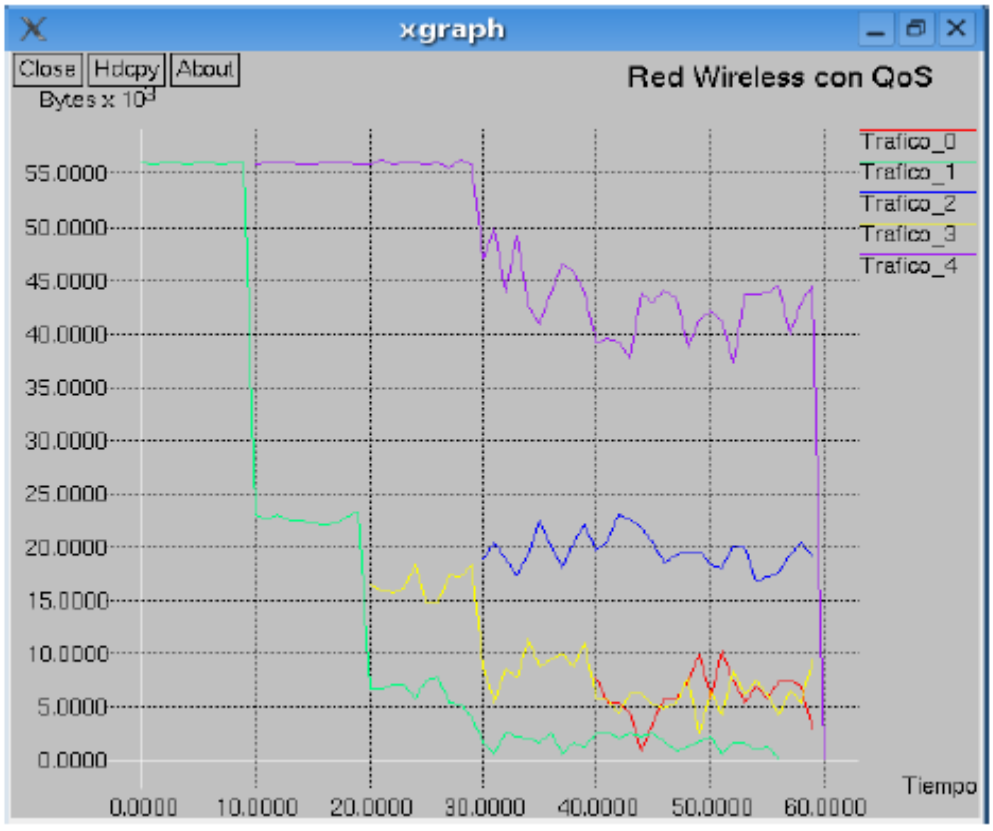


Figura 4.2: Resultado de la simulación con Calidad de Servicio

Fuente: Robles, M. *QoS en redes wireless con IPv6*

D. López, 2011, en su proyecto “Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6”, realiza pruebas para comprobar la comunicación VoIP en un entorno *Dual Stack*, pruebas que

servirán en este estudio para analizar los resultados obtenidos de la simulación de llamadas usando protocolo IPv4 e IPv6 en cuanto a los parámetros que determinan la QoS brindado por redes inalámbricas, para este objetivo realiza llamadas entre las extensiones SIP registradas en un mismo servidor y extensiones registras en un servidor diferente. Para ello, captura los paquetes RTF transmitidos utilizando la herramienta *Wireshart,* obteniendo gráficas correspondientes al flujo de paquetes y *jitter* generado entre las llamadas.

Para comparar IPv4 e IPv6 en cuanto a la QoS que ofrece cada una, se considera los resultados obtenidos en las pruebas realizadas en cuanto al tiempo de transmisión, el *jitter* generado y el retardo promedio entre paquetes, para ello se realizan 20 llamadas en total, de las cuales 10 utilizan IPv4 y 10 llamadas utilizan IPv6, capturando para ambas llamadas IPv4 e IPv6 la misma cantidad de paquetes.

En la Tabla 4.2 se muestra el número de paquetes capturados en cada una de las llamadas.

Tabla 4.2: Número de paquetes capturados en cada llamada VoIP

N.de llamada	N. de paquetes a capturar
1	7760
2	9524
3	14927
4	24448
5	33833
6	36890
7	45317
8	48679
9	54299
10	64321

Fuente: López, D. (2011). *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6.* Oaxaca.

En la Figura 4.3 se muestran las llamadas completas o exitosas con direccionamiento IPv6

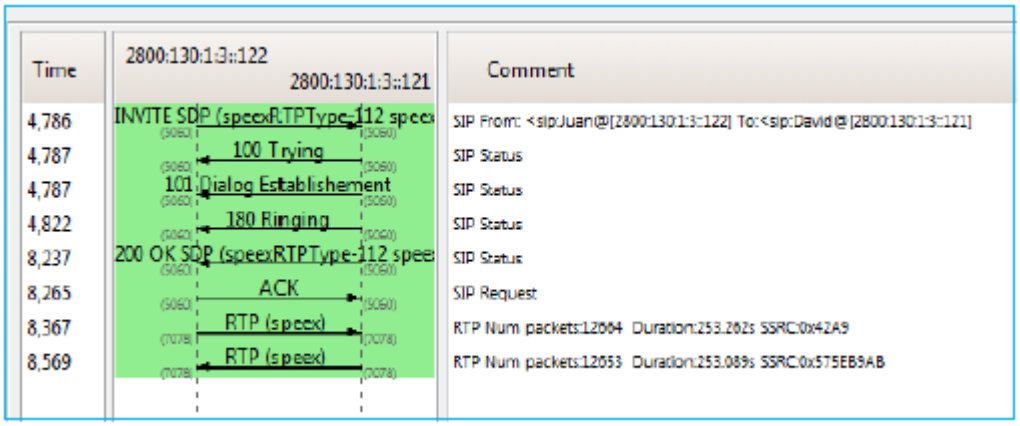


Figura 4.3: Sesión establecida entre clientes SIP mediante IPv6

Fuente: López, D. (2011). *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6.* Oaxaca.

En la Figura 4.4 se describe de manera detallada algunos parámetros del flujo RTP de los paquetes VoIP capturados. Se puede observar el número de paquetes t la secuencia de estos en la transmisión de voz. Se observa también el *jitter* máximo obtenido y el promedio generado durante la llamada, el Max delta que significa la diferencia máxima entre la llegada de un paquete y el siguiente, el total de paquetes transmitidos, el porcentaje de paquetes perdidos, el status o estado en cada secuencia, que en este caso es OK en cada una, indicando que todos los paquetes fueron entregados correctamente, o sea que no hubo pérdida de paquetes.

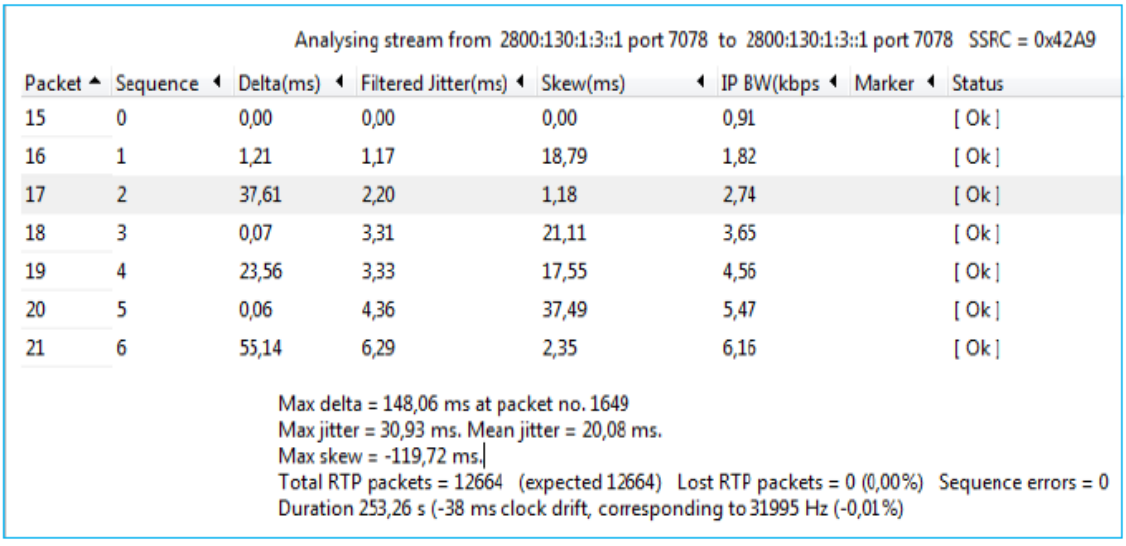


Figura 4.4: Flujo de paquetes RTP en una llamada entre extensiones IPv6

Fuente: López, D. (2011). *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6.* Oaxaca.

En la Figura 4.5 se presenta gráficamente los datos del *jitter* promedio y el *jitter* máximo.

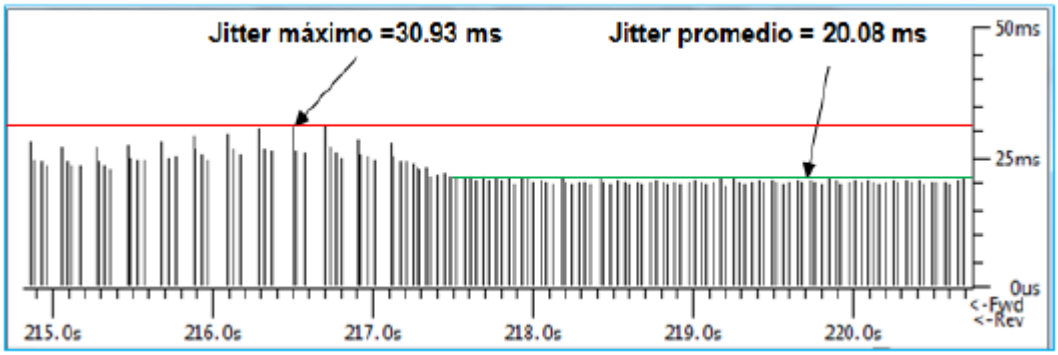


Figura 4.*5: Jitter* máximo y promedio generado en una llamada entre extensiones IPv6
Fuente: López, D. (2011). *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6.* Oaxaca.

La Figura 4.5 además señala el valor máximo de *jitter* generado que es de 30.93ms, se produce entre el intervalo de 216.0s 217.0s. Luego se mantiene con un valor promedio de 20.08 ms.

En la Figura 4.6 se observa el retardo máximo entre la llegada de un paquete y el siguiente.

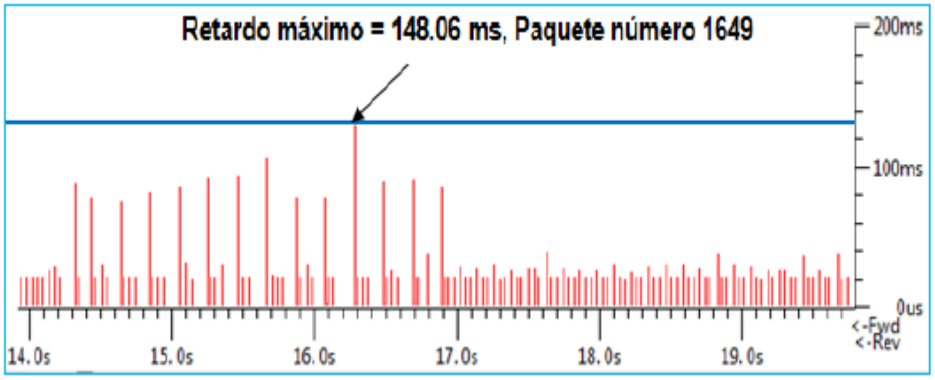


Figura 4.6: Retardo máximo generado en una llamada entre extensiones IPv6.
Fuente: López, D. (2011). *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6.* Oaxaca.

En las Figuras 4.7 y 4.8 se observa el tráfico generado por el cliente que realiza la llamada y el cliente que la recibe, relacionando los paquetes entregados y recibidos con relación al tiempo, observándose que el tráfico en ambas figuras es similar, debido a que la pérdida de paquetes fue de 0%, por lo que el flujo es similar.

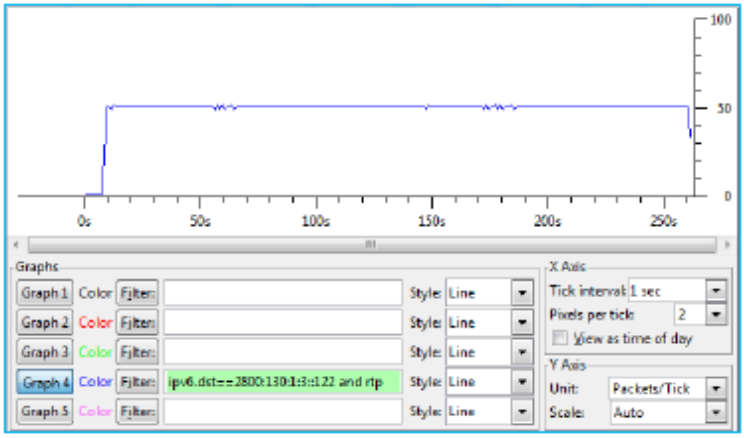


Figura 4.7: Tráfico RTP generado por el cliente SIP que inicia la llamada

Fuente: López, D. (2011). *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6.*

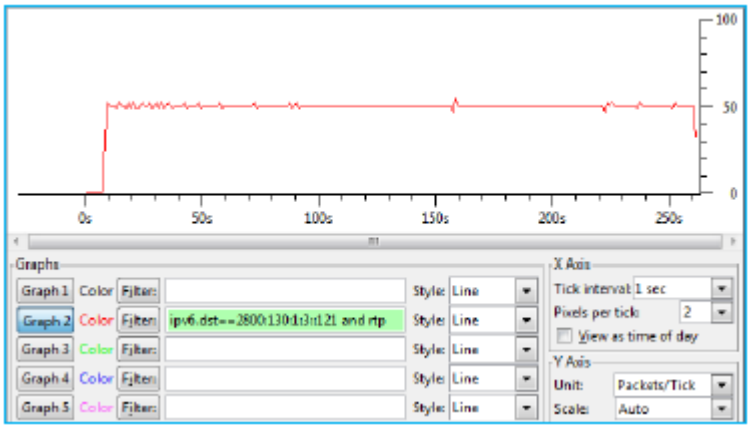


Figura 4.8: Tráfico RTP generado por el cliente SIP que recibe la llamada

Fuente: López, D. (2011) *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6*

Llamadas realizadas entre extensiones IPv6

De igual manera se realizó la sesión de llamada entre dos extensiones IPv4.

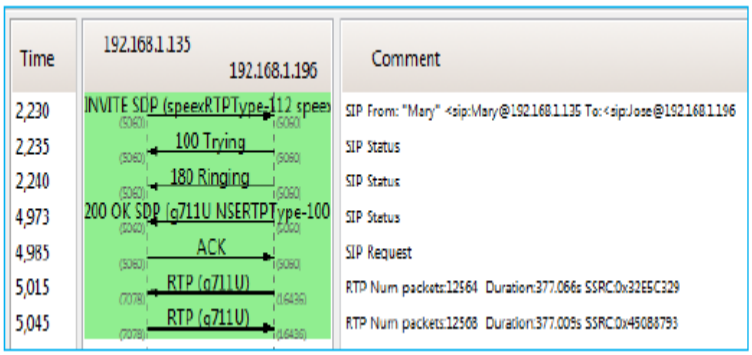


Figura 4.9: Sesión establecida entre clientes SIP usando IPv4

Fuente: López, D. *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6*

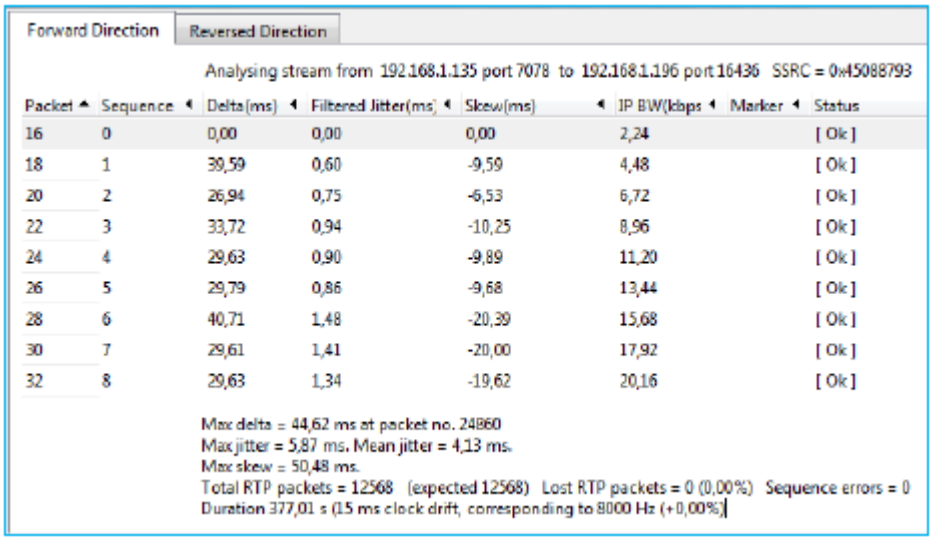


Figura 4.10: Flujo de paquetes RTP en una llamada entre extensiones IPv6

Fuente: López, D. *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6*

En las Figuras 4.9 y 4.10 se observa que las llamadas entre extensiones IPv4 son exitosas, así como el detalle del flujo RTP generado al establecerse la llamada, con los parámetros allí indicados.

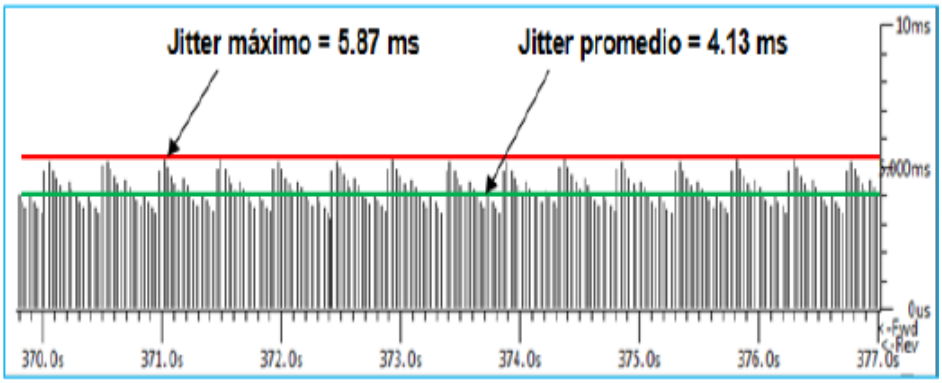


Figura 4.11: *Jitter* máximo y promedio generado en una llamada entre extensiones IPv4

Fuente: López, D. *Implementación de protocolos de señalización* VoIP *sobre un entorno de red IPv6*

En la Figura 4.11 se observa que el *jitter* máximo es de 5.87 ms, no teniendo un intervalo definido, el *jitter* promedio es de 4.13 ms. La calidad de la voz no es afectada debido a que el valor del *jitter* máximo es menor en comparación al *jitter* obtenido con IPv6.

En la siguiente Figura 4.12 se observa el retardo máximo entre la llegada de un paquete y el siguiente.

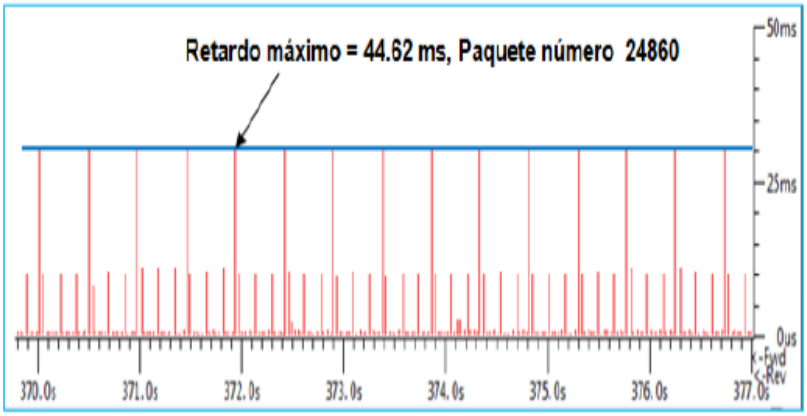


Figura 4.12: Retardo máximo generado en una llamada entre extensiones IPv4

Fuente: López, D. *Implementación de protocolos de señalización* VoIP *sobre un entorno de red IPv6*

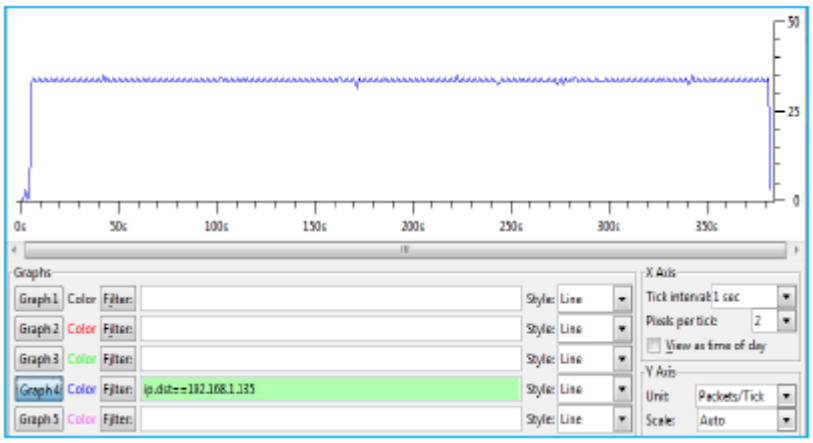


Figura 4.13: Tráfico RTP generado por el cliente SIP que inicia la llamada

Fuente: López, D. *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6*

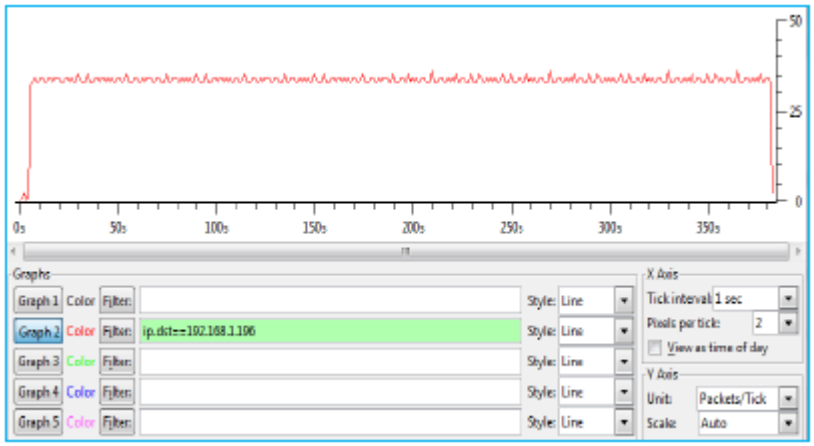


Figura 4.14: Tráfico RTP generado por el cliente SIP que recibe la llamada

Fuente: López, D, *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6*

En las figuras 4.13 y 4.14 se observa que el *jitter* generado se presentó constante durante todo el tráfico RTP en ambos clientes.

D. López, 2011, luego analiza los resultados obtenidos de las 10 llamadas realizadas, realizando observaciones que se resumen en la Tabla 4.3.

Tabla 4.3: Resultados de las 10 llamadas realizadas utilizando IPv6 e IPv4

N. de llamada	N.de paquetes	Tiempo de transmisión en segundos IPv6	Tiempo de transmisión en segundos IPv4
1	7760	78.52	117.34
2	9524	95.93	143.77
3	14927	153.21	229.27
4	24448	253.25	369.23
5	33833	345.16	512.1
6	36890	386.4	548.12
7	45317	455.42	681.07
8	48679	491.24	735.09
9	54299	552.75	814.81
10	64321	640.49	953.37
Promedio	**33.9998**	**345.237**	**510.417**

Fuente: López, D. *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6*

El tiempo se presenta en segundos que cada protocolo utilizó para entregar el total de paquetes establecidos para cada llamada. La diferencia del tiempo total utilizado por cada protocolo para la entrega total de paquetes definidos en las capturas del tráfico RTP es notable.

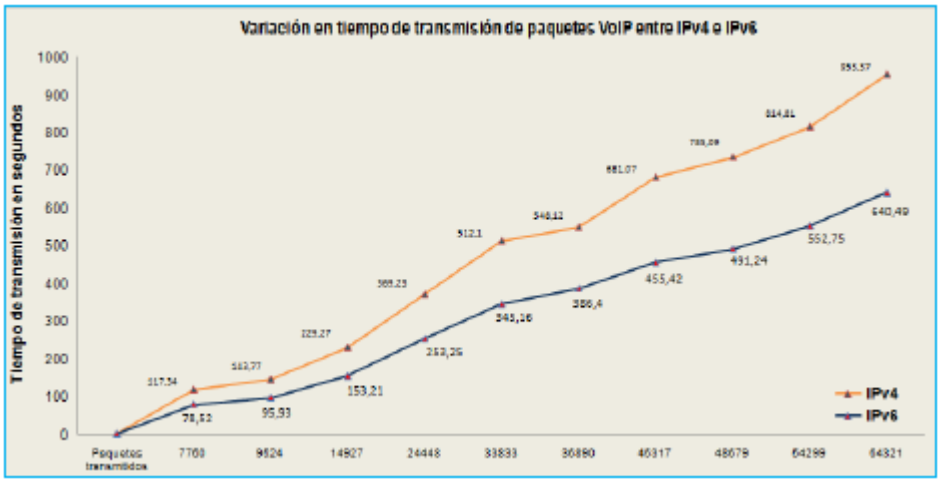


Figura 4.15: Tiempo de transmisión de paquetes VoIP entre Ipv4 e IPv6

Fuente: López David, *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6*

De acuerdo a la Figura 4.15, en que se presentan los tiempos promedios de transmisión entre IPv4 e IPv6 que se muestran en la tabla 8, permite calcular el porcentaje de mejora de IPv6 con respecto a IPv4, lo que brinda un 32% de mejora.

Tabla 4.4: Paquetes enviados por segundo entre IPv4 e IPv6

N. de llamada	N.de paquetes	Número de Paquetes enviados / seg por IPv6	Número de Paquetes enviados / seg por IPv4
1	7760	98.093	64.932
2	9524	99.491	65.37
3	14927	96.224	66.568
4	24448	98.307	67.323
5	33833	97.963	67.008
6	36890	100.271	66.568
7	45317	99.379	66.911
8	48679	99.755	66.885
9	54299	99.294	67.85
10	64321	100.176	67.202
Promedio	33.9998	98.8953	66.6617

Fuente: López, D. *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6*

La Tabla 4.4 muestra el promedio de paquetes enviados por segundo en cada llamada entre los dos protocolos. D. López, en su trabajo presenta el promedio de paquetes transmitidos por segundo, mostrando que IPv6 transmite un mayor número de paquetes en relación a IPv4.

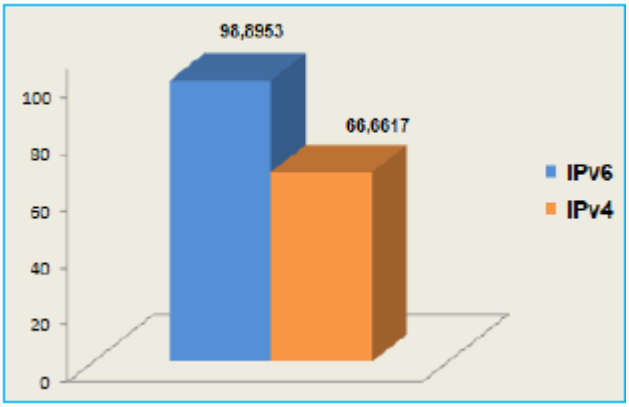


Figura 4.16: Promedio de paquetes VoIP transmitidos entre IPv4 e IPv6

Fuente: López, D. *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6*

De igual manera el *jitter* promedio obtenido en este trabajo generado entre IPv4 e IPv6 en la transmisión de cada una de las llamadas se presenta en la Tabla 4.5.

Tabla 4.5: Jitter promedio generado en la transmisión de VoIP entre IPv4 e IPv6

N. de llamada	N.de paquetes	Jitter promedio IPv6	Jitter promedio IPv4
1	7760	17.83	4.58
2	9524	17.58	4.62
3	14927	17.52	4.63
4	24448	17.05	4.63
5	33833	17.56	4.6
6	36890	17.49	4.62
7	45317	17.49	4.62
8	48679	17.56	4.63
9	54299	17,51	4.58
10	64321	17.55	4.58
Promedio	33.9998	17.51	4.60

Fuente: López David, *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6*

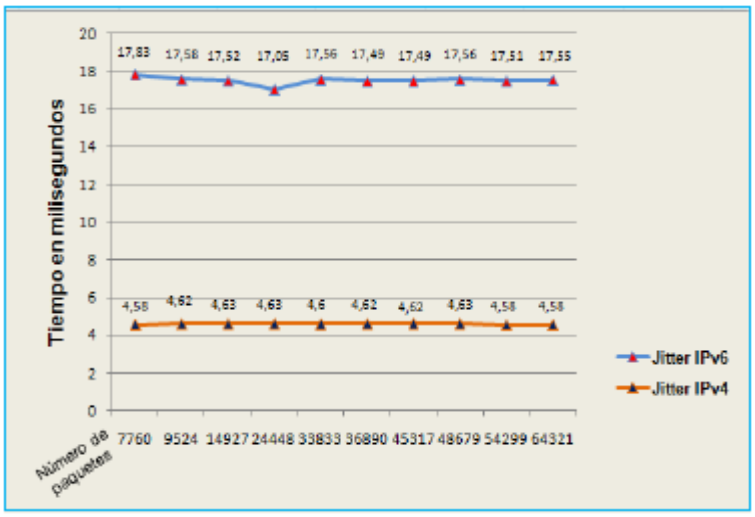


Figura 4.17: *Jitter* generado en la transmisión de paquetes VoIP entre IPv4 e Ipv6

Fuente: López, D. *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6*

En la Figura 4.17 grafica los datos mostrados en la tabla 10, observándose que IPv6 presenta un *jitter* promedio de 17,51, que es mucho mayor que el *jitter* promedio que presenta Ipv4 con un valor de 4,50, pero no llega a afectar mucho en la Calidad de Servicio, este valor promedio se encuentra dentro del rango de intervalos tolerado establecido por la recomendación ITU-T G. 114 que establece que el *jitter* es tolerable si se encuentra entre los 100 ms y 250 ms.

4.2 Análisis comparativo de investigación realizada de Calidad de Servicio (QoS) en redes inalámbricas mediante IPv4 e IPv6.

La existencia de lugares de difícil acceso o el costo de la infraestructura necesaria es un limitante para las redes fijas, por lo que surgen las redes inalámbricas, que nos permiten obtener comunicación entre terminales lejanos y móviles sin la necesidad de cables. En procura de que esta comunicación sea en tiempo real y con velocidad de acceso mayor de acuerdo al aumento de las necesidades, una de las principales dificultades que las redes inalámbricas en la actualidad presentan es que la Internet trabaja con la versión 4 del protocolo IP, esto es el protocolo IPv4. El protocolo IPv4 se ha implementado de una manera extensa, su desarrollo sin embargo exige un constante mejoramiento de este tipo de redes inalámbricas, así como la creación de nuevas tecnologías que permitan mantener una calidad de conexión.

Teóricamente al no contarse con un diseño definido y los inconvenientes que la movilidad genera, una de las principales desventajas de las redes inalámbricas con protocolo IPv4 es satisfacer la Calidad de Servicio (QoS) que requieren los usuarios y algunas aplicaciones, lo que da lugar a buscar una nueva red que soporte la incorporación y desarrollo de nuevos servicios y el desenfrenado aumento de usuarios, por lo que aparece IPv6 como una solución a inconvenientes como el retardo, dado que los paquetes tienen que ser procesados en cada router, lo que implica cierto retardo en la transmisión de los mismos.

Estos criterios son considerados en las simulaciones realizadas por Matías Robles, al momento de analizar la diferencia entre tráficos

transmitidos en redes inalámbricas aplicando Calidad de Servicio (QoS), o sea utilizando protocolo IPv6, en comparación con tráficos sin Calidad de Servicio (QoS), esto es usando protocolo IPv4, observa los resultados obtenidos en relación a parámetros como delay (retardo), jitter (variación en el retardo), bandwidth (ancho de banda),

En su trabajo de investigación se apoya en la conveniencia de utilizar un campo de la cabecera IP para indicar la Calidad de Servicio (QoS) necesaria. Utiliza el campo Flow Label (Etiqueta de Flujo) que se encuentra en la cabecera de los paquetes IPv6 para manejar los flujos que requieren soporte de Calidad de Servicio (QoS), lo mejora indicando qué calidad de servicio se necesita, lo que es muy útil en comunicaciones en tiempo real.

El tener el campo Flow Label en la cabecera de IPv6 un tamaño de 20 bits, permite poder especificar una gran cantidad de flujo de acuerdo a sus requerimientos. Esta consideración es importante puesto que en la cabecera IPv6 existe el campo Traffic Class (Clase de Tráfico) que cumple la misma función y tiene el mismo tamaño que el campo Type of Service (Tipo de Servicio) correspondiente a la cabecera de IPv4, que puede ser utilizado también para indicar qué Calidad de Servicio (QoS) se desea, sin embargo utiliza el campo Flow Label por su tamaño.

En los gráficos obtenidos se muestra el resultado de las simulaciones realizadas sin aplicar Calidad de Servicio (QoS) y aplicando Calidad de Servicio (QoS), para poder compararlos se mantiene en ambas redes la misma cantidad de tráficos y los mismos momentos de inicio de las transmisiones.

En el primer caso sin aplicar Calidad de Servicio (QoS) en los primeros 10 segundos el Tráfico_1 consume un total de aproximadamente 56 Kbytes por segundo, al ir adicionando otros tráficos el ancho de banda total se empieza a compartir entre todos los tráficos en forma casi simétrica. Al agregarse un nuevo tráfico el ancho de banda que recibe cada tráfico es similar, lo que provoca una degradación en el rendimiento,

lo que no permite cumplir con determinados servicios requeridos por alguna conexión.

En el segundo caso se aplican técnicas de Calidad de Servicio (QoS), el gráfico obtenido muestra el rendimiento de la red completamente diferente al caso anterior. El Tráfico_1 con prioridad 3 (menor prioridad), consume de igual forma que en el caso anterior aproximadamente 56 Kbytes por segundo durante los primeros 10 segundos. Cuando se inicia un tráfico de mayor prioridad, éste obtiene el mayor ancho de banda durante toda la simulación. Las diferentes prioridades aplicadas a cada uno de los tráficos utilizados determina el rendimiento de la misma. Estos resultados confirman que la prioridad del tráfico característica del protocolo IPv6 determina el rendimiento brindado.

En el trabajo realizado por David López realiza el análisis comparativo entre IPv4 e IPv6 en cuanto al jitter generado y el retardo promedio entre paquetes. De acuerdo a las simulaciones realizadas en este trabajo obtiene que utilizando el protocolo IPv6 no hubo pérdida de paquetes, por lo que todos los paquetes fueron estregados a su destino.

De acuerdo a la Tabla 4.3 se observa los datos obtenidos por cada llamada realizada para el protocolo IPv4 e IPv6, la variación del tiempo total utilizado por cada uno de los protocolos para entregar el total de paquetes, muestra una diferencia de 165.18 ms en beneficio de IPv6, lo que en porcentaje representa el 32% de mejora. Además el promedio de paquetes transmitidos por segundos de acuerdo a la Figura 4.16 utilizando IPv6 es mayor respecto al número de paquetes que transmite IPv4 por segundo. En la Tabla 4.5 IPv6 muestra un jitter promedio mayor que el jitter que presenta IPv4, sin embargo no incide en la Calidad de Servicio (QoS) ya que el promedio se encuentra dentro del rango de intervalos de tolerancia que establece que el jitter es tolerable si se encuentra entre los 100 ms y 250 ms.

Según lo expuesto IPv6 adiciona mejoras en el enrutamiento incorporando una estructura de direcciones jerarquizadas, lo que le permite tener bloques adyacentes de direcciones en este protocolo, con lo

que se tiene una IPv6 que recoge los mismos protocolos de IPv4, así como su objetivo básico, pero con mejoras lo que permite sobre todo abrir nuevas posibilidades.

En cuanto al retardo y al uso de ancho de banda el utilizar un entorno IPv6 se presenta más óptimo para aplicaciones en tiempo real, ya que se logra transmitir la misma cantidad en un tiempo menor que utilizando IPv4.

En relación al jitter se presenta a una mayor escala con protocolo IPv6, pero al comparar los valores del jitter promedio y máximo obtenidos con los intervalos de tolerancia de acuerdo a lo recomendado por ITU-T G.114, estos valores permiten tener una buena calidad de llamada.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. El estándar 802.11e está enfocado a proveer Calidad de Servicio mediante el manejo de prioridades de acuerdo a las diferentes clases de tráfico, lo que ayuda a mejorar la transmisión de aplicaciones en tiempo real y disminuir los retardos en redes inalámbricas, volviéndolas redes más seguras.

2. El retardo obtenido utilizando el protocolo IPv6 fue menor para la transmisión de paquetes de voz en comparación a igual cantidad de paquetes transmitidos usando protocolo IPv4.

3. Los parámetros *delay, jitter*, pérdida de paquetes y ancho de banda que determinan la Calidad de Servicio (QoS) que ofrece una red en un entorno IPv6 es más óptimo que para un entorno IPv4.

4. Redes inalámbricas con tecnología IPv4 presentan deficiencias para proveer Calidad de Servicio (QoS) a aplicaciones con requerimiento de tiempo real como video conferencia, VoIP, etc., inconvenientes que son mejorados utilizando el protocolo IPv6.

5. Debido al aumento constante de aplicaciones en las redes de datos y de las exigencias del usuario, hacen de la Calidad de Servicio una necesidad prioritaria e inevitable.

6. A parte del direccionamiento extendido que ofrece implementar el protocolo IPv6 en redes inalámbricas, mejora la Calidad de Servicio que ofrecen, debido a que este protocolo permite configurar su cabecera, convirtiéndose en una ventaja para este tipo de redes, aunque la disponibilidad de esta versión de IP es limitada aún.

7. De acuerdo a los resultados de las simulaciones presentadas en esta tesis, nos permite concluir que el rendimiento de una red inalámbrica mejora notablemente cuando se le aplican mecanismos que brindan Calidad de Servicio.

RECOMENDACIONES

1.-Toda red inalámbrica conformada por un gran número de equipos y de usurarios, a la que se necesita implantar QoS, es necesario realizar un estudio exhaustivo para determinar los requerimientos de la red y los mecanismos para garantizar el mejor servicio.

2.-Comprobar el uso eficiente de software libre para la simulación de las aplicaciones presentadas, hace necesario recomendar su implementación de una manera más generalizada, por los múltiples servicios que prestan y por el ahorro en el costo de esta tecnología.

GLOSARIO

AC: *Access Categories,* Categorías de Acceso.

AIFS: Arbitrary Interframe Space, Espacio Inter-Trama Arbitrario.

WAP*: Wireless Access Poin,* Punto de acceso inalámbrico.

Beacon: Trama de gestión que contiene información relacionada con el CSMA/CA.

BSS*:* Basit Service Set, Conjunto de servicios básicos.

CSMA/CA*: Carrier Sense Multiple Access/Collision Detect*, Múltiple acceso por detección de portadora evitando colisiones. Método de transferencia de datos que se utiliza para prevenir pérdidas de los datos en una red.

CW: Ventana de contienda.

DCF: Función de Coordinación Distribuída.

DHCP: *Dinamic Host Configuration Protocol*, Protocolo dinámico de la configuración del anfitrión. Protocolo que deja un dispositivo en una red local, conocida con servidor de DHCP, asigna direcciones temporales del IP a los otros dispositivos de la red.

Diff-Serv: Differentiated Services, Servicios diferenciados.

DIFS: DCF *Interframe Space*, Espacio Inter-Trama DCF.

DNS: *Domain Name Server.* Traduce los nombres de *webside* a direcciones del IP.

DSCP*: Differentiated Services Code Point*. Punto de código de servicios diferenciados.

Dominio: Nombre específico para una red de computadoras.

EDCA: *Enhanced Distributed Channel Access.* Función mejorada de distribución de acceso al canal.

EIFS: IFS Extendida.

Explorador: Programa para observar y obrar con la información proporcionada por el *Word Wide Web.*

FTP: *File Transfer Protocol.* Protocolo estándar para enviar archivos entre las computadoras sobre una red TCP/IP y el Internet.

HCCA: HCF *Controlled Channel Access*.

HCF*: Hybrid Coordination Funcion.* Función de Coordinación Híbrida*.*

HOST: Identifica al ordenador central en un sistema informático complejo.

HTTP: Protocolo del transporte del hipertexto. Protocolo de comunicaciones conectada a los servidores en el Word Wide Web.

ICMP: Internet Control Message Protocol.

IEEE: *Instituto de los Ingenieros Electrónicos Eléctricos.* Instituto independiente que desarrolla estándares del establecimiento de una red.

IETF: Grupo de Trabajo sobre Ingeniería de Internet.

IGMP: Internet Group Management Protocol.

IntServ: Integrated Services, Servicios Integrados.

IP: Internet Protocol. Protocolo que envía datos sobre una red.

IP *ADRESS*: Dirección que identifica a una computadora o un dispositivo en una red.

IFS: Espaciado entre tramas.

IHL*: Internet Header Length*.

MAC: *Media Access Control*. Dirección única que un fabricante asigna a cada dispositivo de la red.

Mbps: *Megabytes* por segundo. Un millón de bits por segundo, unidad de medida para la transmisión de datos.

MPLS: Multiprotocolo de conmutación de etiquetas.

MSDU: Unidad de datos de servicio de MAC.

NAT: Traducción de direcciones de red.

Paquet: Unidad de los datos enviados sobre una red.

PCF: Función de Coordinación Puntual.

Polling: También conocido como protocolo por sondeo. Este método de acceso se caracteriza por contar con un dispositivo controlador central, que es una computadora inteligente, que pasa lista a cada nodo en una secuencia predefinida solicitando el acceso a la red. Es una forma de repartir un canal entre usuarios competidores en el cual se evitan los colisiones por medio del controlador central.

P2P: Peer-to.-Peer. De par a par o de punto a punto. Se refiere a la red de intercambio de archivos entre usuarios.

QAP: ´Punto de Acceso con Calidad.

QBSS *(Quality of Service Basic Set*): Grupo de servicio básico con Calidad de Servicio.

QSTA: *Quality of Service Stations*, Estaciones con Calidad de Servicio.

Red: Varias computadoras o dispositivos conectados con el fin de compartir, almacenar, y/o transmitir datos entre los usuarios.

RFC: Formato estándar en Internet.

Router: Permite la interconexión de redes y su función es la de guiar paquetes de datos para que fluyan hacia la red correcta y llegar a su destino.

RSVP: *Resource Reservation Protocol*, Protocolo de reserva de recursos.

SBM: Administración del ancho de banda de la subred.

Servidor: Cualquier computadora cuya función en la red es de proporcionar el acceso de los usuarios a los archivos, a la impresión, comunicaciones y a otros servicios.

Scheduling: Algoritmo de gestión de recursos. Determina el instante en que un usuario que tiene acceso al sistema a través del *MAC* puede iniciar una transmisión. Indica también la cantidad de recursos que puede utilizar en la transmisión. Es un mecanismo que requiere reglas de priorización y un algoritmo para distribuir los recursos entre los usuarios, para garantizar la Calidad de Servicio.

SIPP: *Simple IP Plus*.

Software: Programa. Serie de instrucciones que realizan una tarea en particular.

Streaming: Transmisión en tiempo real, sobre todo a través de Internet.

TC: *Traffic Class*. Clases de tráfico.

TCP/IP: Sistemas de protocolos que hacen posible servicios como Telnet, E-mail y otros, entre ordenadores que no pertenecen a la misma red.

ToS: Tipo de Servicio.

TS: Traffic Stream.

TTL: Tiempo de vida.

TSPEC: Especificaciones de Tráfico.

TXOP: Oportunidad de Transmisión.

UDP: *User Datagram Protocol*. Protocolo del nivel de transporte que se basa en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido con antelación una conexión, ya que la cabecera del datagrama tiene suficiente información.

WECA: *Wireless Ethernet Compatibility Alliance*. Alianza de compatibilidad Ethernet inalámbrica.

WEP2: Privacidad equivalente al cable. Sistema de encriptación de estándar. Es un algoritmo de seguridad que mejora los inconvenientes que presenta WEP

WPA: *Wi FI Protected Access*. Alto nivel de seguridad inalámbrica para la red.

LISTADO DE REFERENCIAS BIBLIOGRAFIAS

6SOS. (s.f.). (5 de enero de 2004). *El protocolo IPv6*. Recuperado el 15 de septiembre de 2012, de http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf

Ahuatzin, G. (s.f.). *Desarrollo de un esquema de traducción de direcciones IPv6-IPv4-IPv6*. Recuperado el 15 de septiembre de 2012, de http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo2.pdf

Andreu, F. (2006*). Redes WLAN. Fundamentos y aplicaciones de seguridad.* Barcelona. Editorial Marcombo S. A.

Andreu, J. *Servicios en red.* Edit. Editex.

Bautista, D. L. (julio de 2011). *Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6.* Recuperado el 21 de septiembre de 2012, de http://www.unsij.edu.mx/tesis/digitales/3.%20DAVID%20LOPEZ%20BAUTISTA.pdf

Banchs, A., & Vollero, L. (24 de agosto de 2005). *Computer Networks*. Recuperado el 15 de septiembre de 2012, de http://www.netcom.it.uc3m.es/publications/pdf/2006/comnet06.pdf

Boquera, M. C. (2003). *Servivios Avanzados de Telecomunicación.* Madrid: Díaz de Santos S.A. C, M.

Cabeza, E. C. (2009). *Fundamentos de Routing.*

Calidad de servicios en redes de servicios Diferenciales. (s.f.). Recuperado el 30 de julio de 2012, de http://www.tid.es/documentos/revista_comunicaciones_i+d/numero24.pdf

Carballar, J.A. (2007). *VoIP. La Telefonía de Internet*.

Cisco. (s.f.). Recuperado el 13 de agosto de 2012, de http://docwiki.cisco.com/wiki/Internetworking_Technology_Handbook#Quality_of_Service_Networking

Cisco. (2010). *Redes Cisco, Instalación y administración de hardware y software.* Manuales USERS.

Dordoigne, J. (2011). *Redes Informáticas.* Barcelona: Ediciones ENI.

Ettikan Kandasamy, T. H. (s.f.). Transition Mechanism Between IPv4 & IPv6 and deciding your choice. Obtenido de http://www.my.apan.net/ipv6/Papers/Transition-Mechanism-IPv4_IPv6.pdf.

Fernando Andreu, I. P. (2006). *Redes WLAN. funadamentos y aplicaciones de seguridad.* Barcelona: Editorial Marcombo S. A.

Francesioni, H. A. *Psec en ambientes IPv4 e IPv6*. Argentina.

Feid, S, 1998 *TCP/IP: Architecture, Protocols and Implementation with IPv6 and IP Security*. USA: Mc Graw Hill

Holt, A. (2010). *802.11 Wireless Networks.* Springer.

Huidobro, J.M, Roldán D. (2005). *Comunicaciones en Redes WLAN*. Copyright.

Izaskum Pellejero, F. A. (2006). *Fundamentos y aplicaciones de seguridad en redes Wlan.* Barcelona, España: Marcombo S.A.

Jaime Lliret Mauri, N. G. (2008). IPTV: La Televisón por Internet. España: Editorial Vértice.

Jara, F. (abril de 2009). Estudio e implementación de una red IPv6 en la UTSFM. Obtenido de www.implementacionipv6.utfsm

Lliret J., N. G. (2008). *IPTV: La Televisón por Internet.* España: Editorial Vértice.

Legal, D. (2011). *Videovigilancia: CCTV usando videos IP.* Málaga, España: Editoral Vértice.

León, M. (2002) *"Quality of Service of the Internet Protocols",* en International Symposium on Advanced Distributed System.

López, D. (2011). Implementación de protocolos de señalización VoIP sobre un entorno de red IPv6. Oaxaca.

Loshin, P. I*Pv6 Theory protocol and practice*. Estados Unidos de América: Morgan Kauffman Publisers.

Majkonoski, J., & Casadovall, F. (s.f.). *Calidad de servicio en WLAN considerando un escenario mixto 8002.11e y 802.11b*. Recuperado el 15 de septiembre de 2012, de http://www.aroma-ist.upc.edu/publicdocuments/conferences/C15.pdf

Mathon, P. (2001). *TCP/IP Entorno Windows 2000*. ENI

Mathon, P. (2004). *Windows Server 2003 Servicios de Red TCP/IP.* Barcelona: ENI.

Moya, J. M. (2005). *Sistemas de Telecomunicación e Informáticos.* Thomson Paraninfo.

Pablo Gil, J. P. (2010). *Redes y transmisión de datos.* Iniversidad de Aliicante.

Palacios, E., & Romero, M. (2012). *Instrumentación Virtual.* Guayauil, Ecuador: CODEU.

Parsons, J. J., & Oja, D. (2008). *Conceptos de computación. Nuevas perspectivas.* México: Ediciones OVA.

Pellejero, I., Andreu, F., & Lesta, A. (2006). *Redes Wlan.* Barcelona, España: Editorial Marcombo S. A.

Piquero, J. V. (2010). *Prácticas de redes.* Depósit (s.f.). Recuperado el 30 de julio de 2012, de www.nwfusion.com/news/tech/2002/1104techupdate.html

Rivasainz, A. (abril de 2006). *Impactos de implementación del protocolo IPv6 para el proveedor de servicios de telecomunicaciones*. Recuperado el 10 de septiembre de 2012, de http://www.wiphala.net/research/project/ipv6/impactos_de_implementacion_del_protocolo_ipv6_para_un_proveedor_de_servicios_de_telecomunicaciones_un_enfo

Robles, M. (2008). QoS en redes wireless con IPv&. Recuperado el 21 de septiembre de 2012, de http://postgrado.info.unlp.edu.ar/Carreras/Magisters/Redes_de_Datos/Tesis/Robles_Matias.pdf

Señalización para QoS en redes IP. (s.f.). Recuperado el 30 de julio de 2012, de http://www.ahciet.net/comin/portaly/1000/10002/10007/10300/docs/qos.pdf

Ternera, M. d. (2010). *Redes Locales.* madrid, España: Ediciones Paraninfo, S.A.

Trejo, g. J. (s.f.). Recuperado el 31 de 07 de 2012, de http://mixteco.utm.mx/~resdi/historial/Analisis_de_la_Calidad_de_Servicio_por_Medio_del_Modelo_Diferencial.pdf

Zhu, C. (2011). *Streaming Media Architectures, Techniques and Applicatios.* British Library

ANEXOS

ANEXO 1

SIMULADOR NS-2

Ns, *network simulator*, es una herramienta muy potente dentro del campo de la simulación de redes. Es a la vez muy flexible dada la posibilidad de trabajar con scripts tcl que nos permite agregar toda la potencia de un lenguaje de programación a los propios elementos de la simulación.

NS (Network Simulator) en la versión 2, conocido como NS-2, es un simulador de redes orientado a eventos. Fue desarrollado como parte del proyecto VINT (Virtual Internet *Testbed),* que consistía en una colaboración de varios institutos y organizaciones entre las que se incluían la Universidad de Berkeley, AT&T, Xeros PARC y ETH. La primera versión del simulador estuvo disponible en el año 1995 y, para 1996, ya estaba disponible la segunda versión.

NS-2 (*Network Simulator* 2, versión 2.28), es una de las herramientas más potentes en lo que a simulación de sistemas de comunicaciones inalámbricas se refiere; no solo brinda la ventaja de ser un software de libre distribución, sino que consta de una amplia documentación para su uso.

En el presente proyecto se utilizará el simulador para medir la Calidad de Servicio (QoS) a través de la comparación entre las versiones 4 y 6 de IP, para ello se realizará la simulación de un sistema compuesto por:
http://dspace.epn.edu.ec/bitstream/15000/8522/1/T10981CAP3.pdf

El simulador NS-2 está disponible para varias plataformas, permite la configuración de una gran cantidad de parámetros tales como la topología de la red, la pila de protocolos y parámetros específicos de cada protocolo. También permite evaluar el impacto de diferentes tipos de tráfico de red. Al ser un producto de código abierto está en constante evolución.

El proceso de simulación se realiza a través del desarrollo de scripts en OTcl, en el cual se especifican protocolos, estructuras físicas, tráficos y orden de los eventos, entre otros parámetros a simular. Después el archivo dado es procesado y los resultados pueden ser entregados mediante el uso de tres tipos de archivos diferentes: los archivos generados por el usuario, los archivos de traza y los archivos .nam. El simulador NS consta de un núcleo principal, escrito en C++, al que se invoca simplemente tecleando ns en la línea de comandos (una vez este ha sido correctamente instalado). Luego el usuario puede interactuar directamente con el simulador, a través de un lenguaje de interface.

El simulador NS-2 brinda una característica limitada para la simulación de redes inalámbricas ad hoc según el estándar IEEE 802.11, sin soporte para Calidad de Servicio (QoS). Por lo que se debe instalar un parche adicional para brindar soporte de calidad de servicio según el estándar IEEE 802.11e, el cual es producto del grupo de trabajo denominado TKN (*Telecommunication Networks Group*) de la facultad de telecomunicaciones de la Universidad de Berlín.

Módulos adicionales del simulador NS-2

Las herramientas o módulos adicionales con que cuenta NS-2 para presentar resultados son el xgraph y el nam.

• XGRAPH: Esta herramienta permite mostrar gráficos bidimensionales de parámetros definidos por el usuario y que son almacenados en un archivo como resultado de ejecutar el script de simulación.

• NAM: Esta herramienta permite representar gráficamente el diseño de la red. Además, permite visualizar dinámicamente el proceso de simulación permitiendo interpretar los archivos con extensión. nam que se generan en el proceso de la simulación.

Para descargar su código fuente se lo realiza de la siguiente dirección de Internet: http://www.isi.edu/nsnam/ns

Para conseguir una correcta instalación del simulador NS-2 son:

1. Crear el directorio NS-2 y copiar ahí todos los paquetes descargados que se van a instalar.

2. Descomprimir cada archivo utilizando el comando tar –zxvf nombre.ext

3. Entrar a cada directorio donde se han descomprimido los archivos descargados y compilar ahí cada paquete, utilizando los comando ./configure y make. Para que la instalación sea satisfactoria, los paquetes se deben compilar en el siguiente orden:

a. Tcl 8.4/unix
b. Tk 8.4/unix
c. Otcl
d. Tclcl
e. NS-2 2.28 (previamente se deben copiar los archivos /tcl 8.4/unix/libtcl8.4.so y /tk 8.4/unix/libtk8.4.so en el directorio/usr/local/)
f. Nam (opcional)
g. Xgraph (opcional)
h. Tcl debug (opcional)

4. Ejecutar el comando ./*validate* si se desea probar que funcione el NS-2 y el nam. Para que funcione correctamente el ns2 es necesario copiar el archivo tcl8.4.5/*library/init.tcl* en el directorio usr/local/lib/tcl8.4

Los ejecutables creados se pueden almacenar en un mismo directorio.

Cuando se quiere acceder a recursos de sistemas Linux utilizando sistema operativo Microsoft, se presenta el inconveniente de poder realizar una conexión remota ssh al ordenador Linux. Si aparte de la conexión tipo ssh se necesita tener otros resultados como gráficos en el equipo, es necesario instalar un servidor de ventanas en el ordenador con Windows. Este software agrega al equipo Windows herramientas como poder realizar conexiones ssh, tener un servidor con ventanas,

permitiendo trabajar como si se lo estuviera realizando con un sistema operativo Linux.

El primer paso es ingresar en la página de *Cygwin/x* y bajar el software haciendo *click* en el enlace setup.exe. Luego es necesario ejecutar el software o guardarlo en el ordenador, si lo que se quiere es guardarlo, hay que seleccionar el directorio en donde se almacenará este fichero, a donde se tendrá que ingresar en el caso de querer ejecutar el archivo bajado. Cuando el usuario selecciona el fichero bajado para ejecutarlo aparece una ventana de bienvenida a *Cygwin*/x, allí se presenta la versión del programa instalado y además se detalla lo que se puede realizar con el fichero en ejecución. En este paso hay que decidir si se quiere realizar la instalación desde la Internet o bajar el software o realizar la instalación de ficheros previamente bajados. Luego se debe de elegir el directorio en donde se instalará el software, quienes pueden tener acceso, el formato que tendrán los ficheros de texto, para este caso será Unix. Se debe de indicar el directorio que se utilizará para almacenar los ficheros temporales de la instalación. A continuación se solicita al usuario el tipo de conexión a Internet con el que trabaja para configurar un proxy de ser necesario.

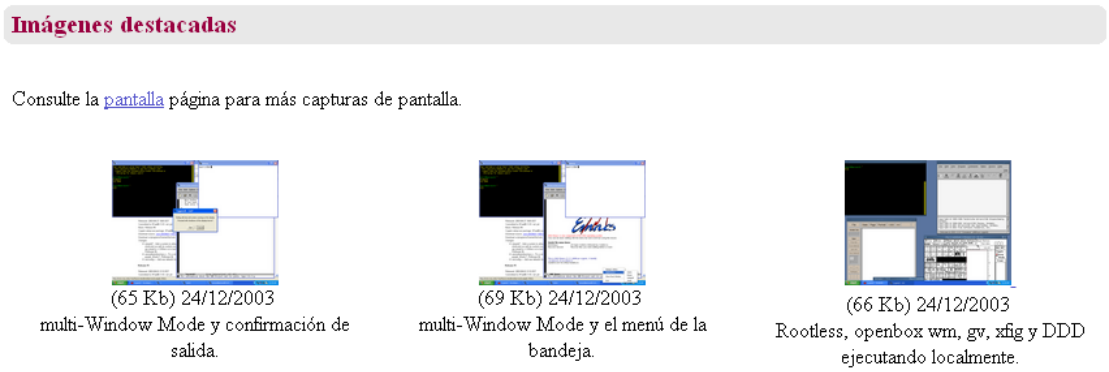


Imagen que aparece en la web de Cygwin/X

Cygwin / X se instala a través de Cygwin setup.exe y el proceso de instalación detallada se lo encuentra en la Guía del usuario de Cygwin / X . Aún ya teniéndose instalado Cygwin, se puede agregar Cygwin / X

para su instalación mediante la descarga de la última setup.exe , ejecutar la instalación, y la selección de la 'xinit "paquete de la' X11 'categoría.

ANEXO 2

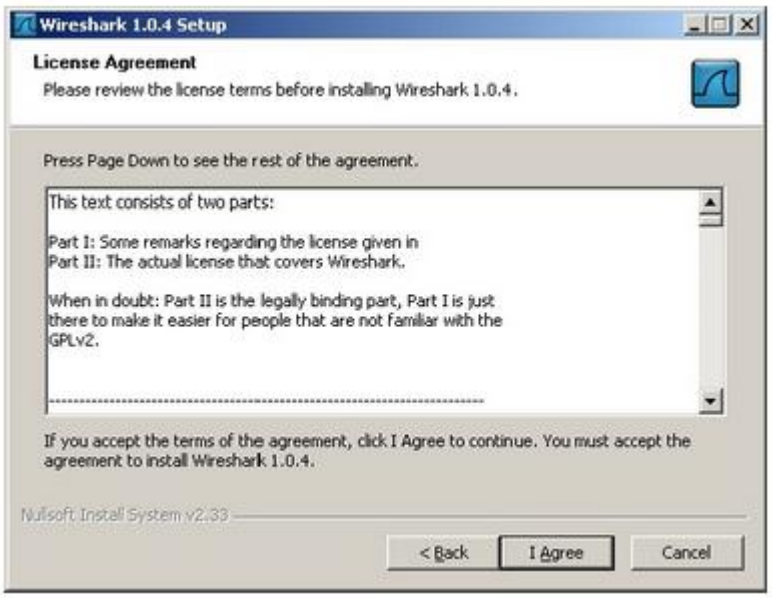
INSTALACIÓN Y CONFIGURACIÓN DE WIRESHARK

Es un analizador de protocolos utilizado como una herramienta de diagnóstico de redes y de desarrollo de aplicaciones de res. Para instalar y configurar esta herramienta en sistemas Linux requiere conectividad con Internet.

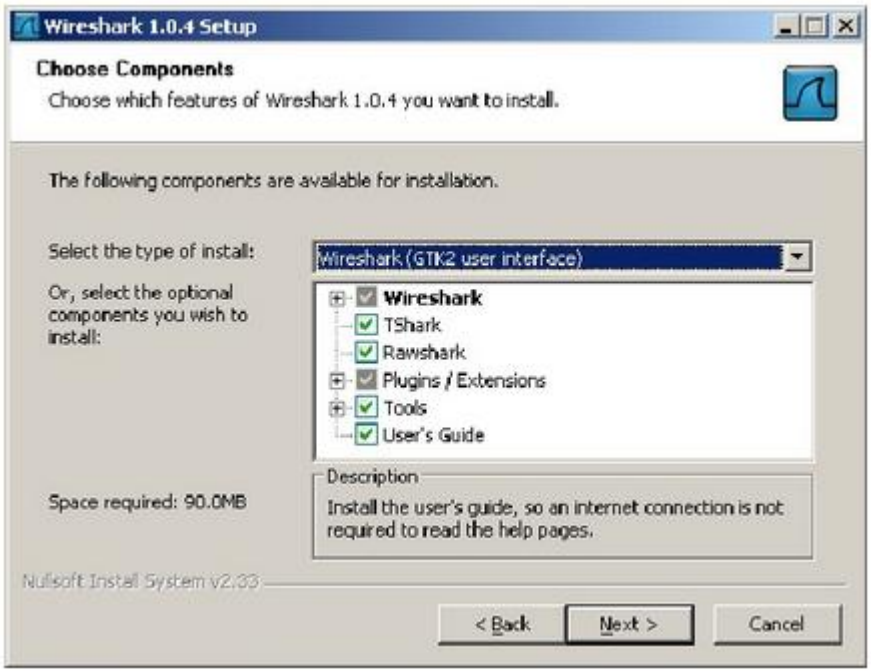
Wireshark es software libre y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD y MAC OS X, así como en Microsoft Windows.

Instalación de Wireshark

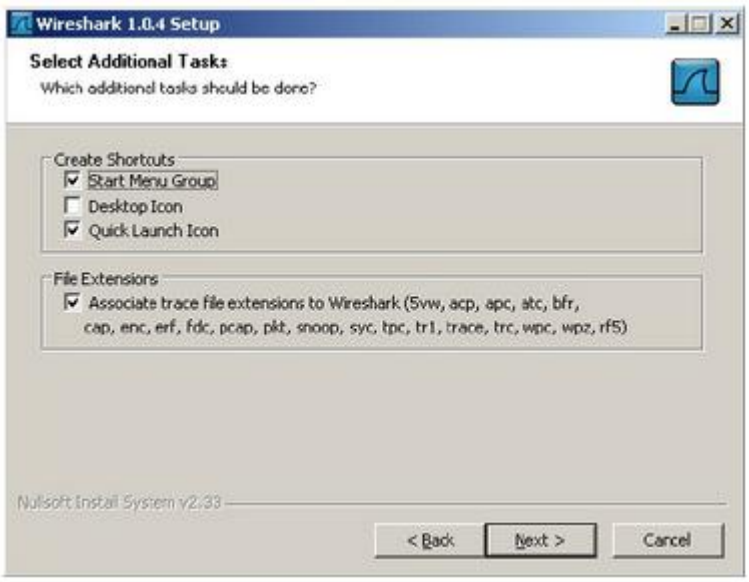
Después de descargar, se lo ejecuta y se clic en siguiente.



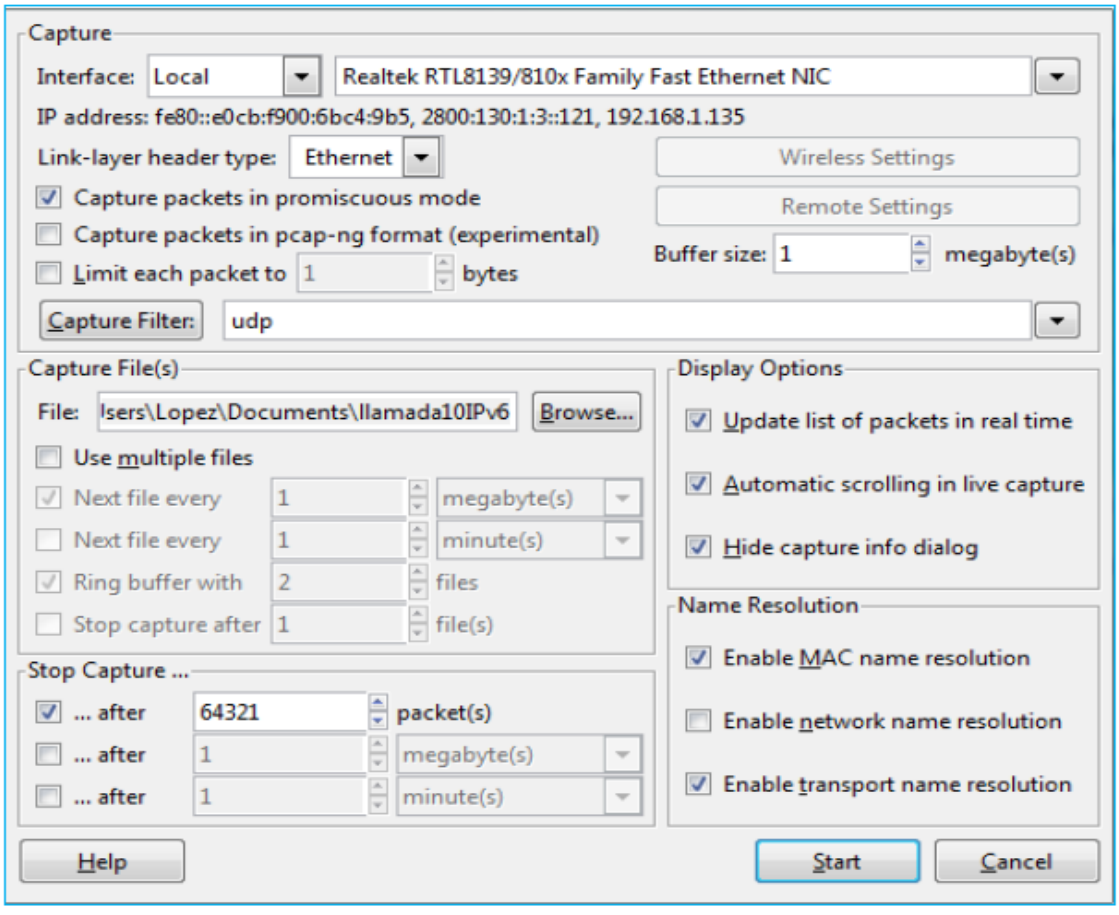
Se acepta el contrato de licencia y clic en siguiente



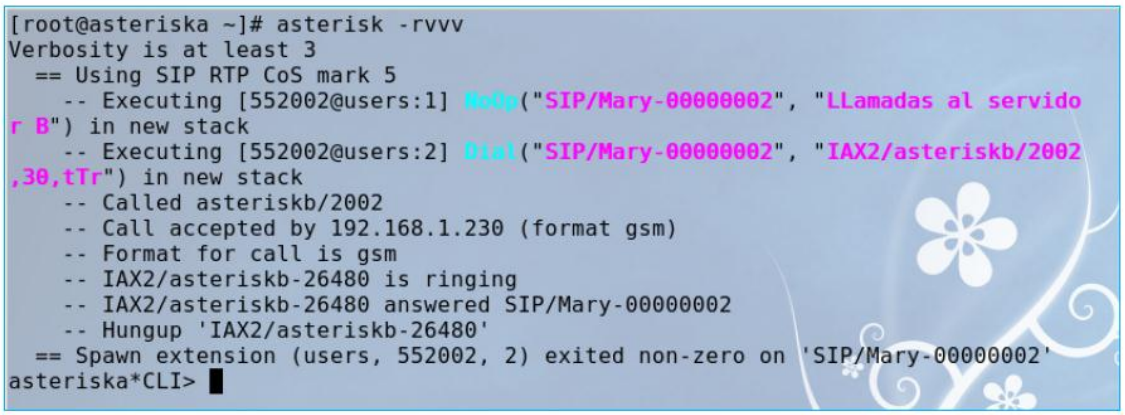
Componentes que son parte de su instalación



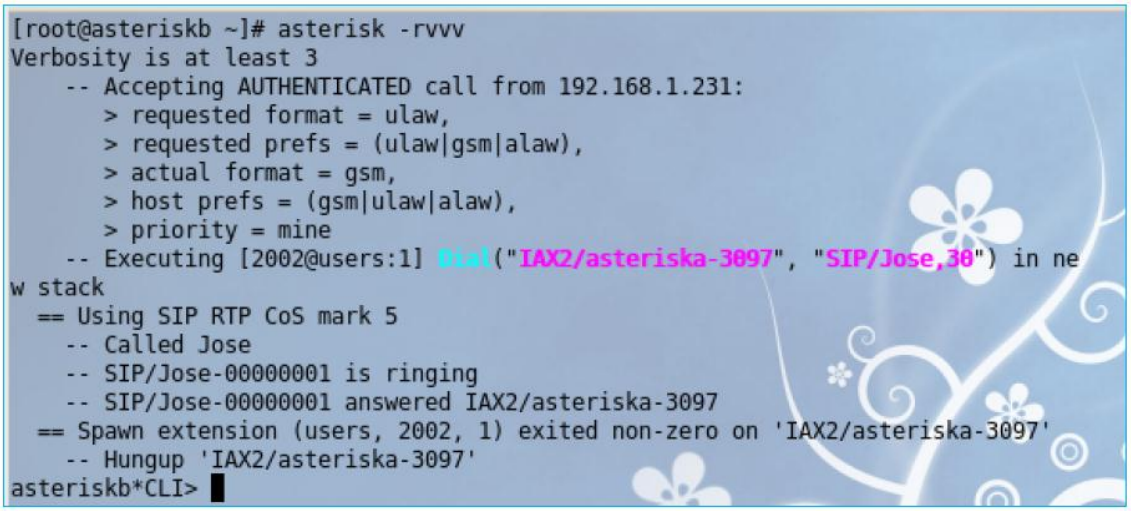
Es necesario especificar el filtrado de los paquetes VoIP, para que se pueda visualizar en la pantalla del programa. Es necesario acceder al menú Capture-Options. Se definen los parámetros y se inicia la captura con Start.



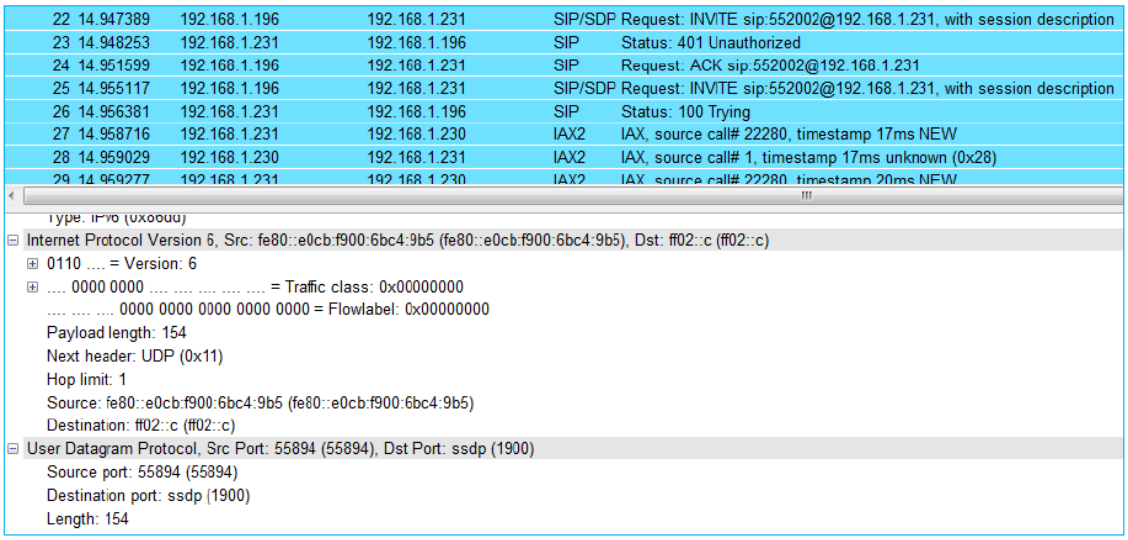
Se observa a continuación el proceso de una llamada solicitada por el usuario A con la extensión 2002 del servidor B.

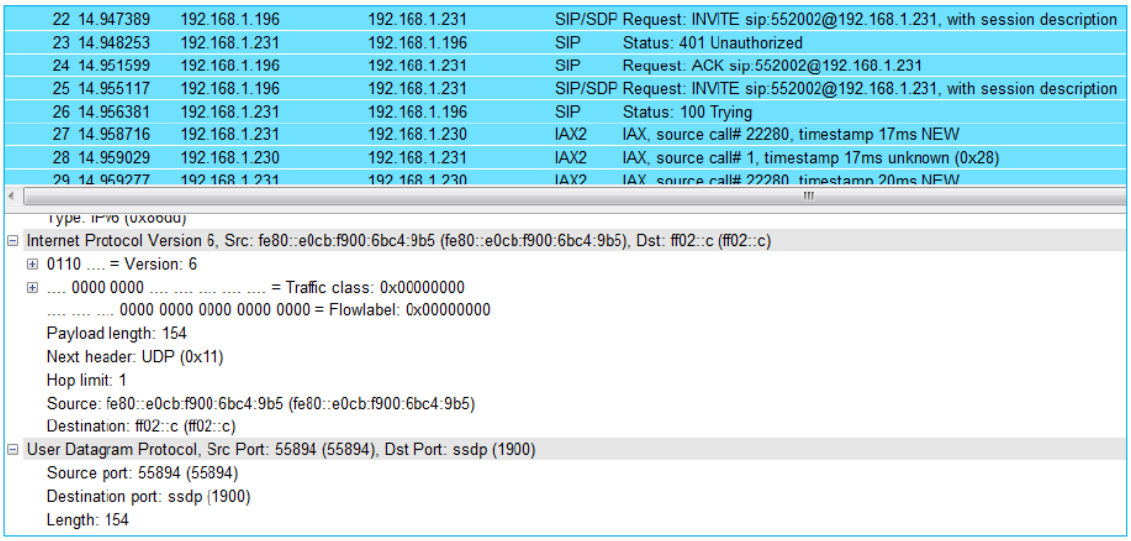


El servidor B responde la llamada y la dirige a la extensión marcada por la extensión del servidor A.



En la siguiente figura se observa un fragmento de la captura de paquetes con Wireshark, realizada entre dos extensiones IPv4 y dos extensiones IPv6.


22 14.947389 192.168.1.196 192.168.1.231 SIP/SDP Request: INVITE sip:552002@192.168.1.231, with session description
23 14.948253 192.168.1.231 192.168.1.196 SIP Status: 401 Unauthorized
24 14.951599 192.168.1.196 192.168.1.231 SIP Request: ACK sip:552002@192.168.1.231
25 14.955117 192.168.1.196 192.168.1.231 SIP/SDP Request: INVITE sip:552002@192.168.1.231, with session description
26 14.956381 192.168.1.231 192.168.1.196 SIP Status: 100 Trying
27 14.958716 192.168.1.231 192.168.1.230 IAX2 IAX, source call# 22280, timestamp 17ms NEW
28 14.959029 192.168.1.230 192.168.1.231 IAX2 IAX, source call# 1, timestamp 17ms unknown (0x28)
29 14.959277 192.168.1.231 192.168.1.230 IAX2 IAX, source call# 22280, timestamp 20ms NEW
Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: fe80::e0cb:f900:6bc4:9b5 (fe80::e0cb:f900:6bc4:9b5), Dst: ff02::c (ff02::c)
0110 .... = Version: 6
.... 0000 0000 .... = Traffic class: 0x00000000
.... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
Payload length: 154
Next header: UDP (0x11)
Hop limit: 1
Source: fe80::e0cb:f900:6bc4:9b5 (fe80::e0cb:f900:6bc4:9b5)
Destination: ff02::c (ff02::c)
User Datagram Protocol, Src Port: 55894 (55894), Dst Port: ssdp (1900)
Source port: 55894 (55894)
Destination port: ssdp (1900)
Length: 154


22 14.947389 192.168.1.196 192.168.1.231 SIP/SDP Request: INVITE sip:552002@192.168.1.231, with session description
23 14.948253 192.168.1.231 192.168.1.196 SIP Status: 401 Unauthorized
24 14.951599 192.168.1.196 192.168.1.231 SIP Request: ACK sip:552002@192.168.1.231
25 14.955117 192.168.1.196 192.168.1.231 SIP/SDP Request: INVITE sip:552002@192.168.1.231, with session description
26 14.956381 192.168.1.231 192.168.1.196 SIP Status: 100 Trying
27 14.958716 192.168.1.231 192.168.1.230 IAX2 IAX, source call# 22280, timestamp 17ms NEW
28 14.959029 192.168.1.230 192.168.1.231 IAX2 IAX, source call# 1, timestamp 17ms unknown (0x28)
29 14.959277 192.168.1.231 192.168.1.230 IAX2 IAX, source call# 22280, timestamp 20ms NEW
Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: fe80::e0cb:f900:6bc4:9b5 (fe80::e0cb:f900:6bc4:9b5), Dst: ff02::c (ff02::c)
0110 .... = Version: 6
.... 0000 0000 .... = Traffic class: 0x00000000
.... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
Payload length: 154
Next header: UDP (0x11)
Hop limit: 1
Source: fe80::e0cb:f900:6bc4:9b5 (fe80::e0cb:f900:6bc4:9b5)
Destination: ff02::c (ff02::c)
User Datagram Protocol, Src Port: 55894 (55894), Dst Port: ssdp (1900)
Source port: 55894 (55894)
Destination port: ssdp (1900)
Length: 154