*REPÚBLICA BOLIVARIANA DE VENEZUELA*

*UNIVERSIDAD DEL ZULIA*

*FACULTAD EXPERIMENTAL DE CIENCIAS*

DIVISIÓN DE PROGRAMAS ESPECIALES

*LICENCIATURA EN COMPUTACIÓN*

**CALIDAD DE SERVICIO BAJO BGP EN SISTEMAS AUTÓNOMOS CONECTADOS POR ENLACES A 5.7 GHZ Y NODOS MÓVILES EN IPv6**

## Trabajo Especial de Grado presentado como

## Requisito para optar al título de Licenciado en Computación

### Autor: Jianfeng, Wu

Tutor**:** MSc. Alfredo Acurero

Maracaibo, junio 2012

**CALIDAD DE SERVICIO BAJO BGP EN SISTEMAS AUTÓNOMOS CONECTADOS POR ENLACES A 5.7 GHZ Y NODOS MÓVILES EN IPv6**

*Jianfeng Wu*

*C.I. No.: 82.212.950*

*Teléfono: 0261 – 7325736 / 0412-6625944*

*Conj. Resid. Grano de Oro, Torre B, Apt. 3A, Maracaibo*

*Correo electrónico:* [*alexjianfeng@hotmail.com*](alexjianfeng@hotmail.com)

*MSc. Alfredo Javier Acurero Álvarez*

*C.I. No.: 9.783.996*

*Correo electrónico:* [aacurero@luz.edu.ve](mailto:aacurero@luz.edu.ve)

WU, JIANFENG. **“Calidad de Servicio bajo BGP en Sistemas Autónomos conectados por enlaces a 5.7 Ghz y nodos móviles en IPv6”.** Trabajo Especial de Grado. Universidad del Zulia. Facultad Experimental de Ciencias. División de Programas Especiales. Licenciatura en Computación. Maracaibo. Venezuela. 2011.105 p.

**RESUMEN**

Actualmente, el estudio de conectividad inalámbrica entre Sistemas Autónomos no ha sido muy explorado, por lo que se pretende en este proyecto, asociar el nuevo protocolo de direccionamiento IPv6 con dicha problemática. Consecuentemente, el objetivo fundamental de esta investigación fue analizar el comportamiento del protocolo IPv6 en Sistemas Autónomos conectados por enlaces de 5.7 GHz usando parámetros de medición de QoS y nodos móviles. Aplicando los principios de Bisquerra (2000), se estableció la metodología en cuatro (4) fases, las cuales se dividen en: recopilación de información, diseño de topologías y/o ambientes de pruebas, pruebas de medición y recopilación de información de los resultados y el tratamiento y análisis estadístico de los datos obtenidos. A través de los resultados obtenidos en el análisis-comparativo entre el protocolo IPv6 e IPv4 en este entorno de red, se observó que IPv6 presentó en general un menor desempeño frente a IPv4, pero mediante el uso del método estadístico ANOVA se concluye que a causas de diferencias no considerables, IPv6 no influye significativamente en el rendimiento de una red con las características estudiadas.

**Palabras Clave:** IPv6, Sistemas Autónomos, QoS, tecnología inalámbrica.

**Dirección electrónica:** alexjianfeng@hotmail.com

WU, JIANFENG. **“Quality of Service under BGP in Autonomous Systems connected by 5.7 Ghz links and mobile nodes in IPv6”.** Trabajo Especial de Grado. Universidad del Zulia. Facultad Experimental de Ciencias. División de Programas Especiales. Licenciatura en Computación. Maracaibo. Venezuela. 2011. 105 p.

**ABSTRACT**

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

**Key words:** IPv6, Autonomous Systems, QoS, Wireless technology.

**E-mail:** alexjianfeng@hotmail.com

**ÍNDICE GENERAL**

|  |  |
| --- | --- |
|  | **Pág.** |
| **RESUMEN**……………………………………………………………………………….….  **ABSTRACT**…………………………………………………………………………………  **ÍNDICE DE ILUSTRACIONES**……………………………………………………………  **INTRODUCCIÓN**…………………………………………………………………….……. | 3  4  8  13 |
| **CAPITULO I**………………………………………………………………………………...  **PLANTEAMIENTO DEL PROBLEMA**…………………………………………………..  1. Planteamiento del Problema…..………………………………...…...……………......  2. Objetivos de la investigación………..………………………………………..………..  2.1. Objetivo General.………………………………….…………………...……………..  2.2. Objetivos Específicos………………...………………………...……………............  3. Justificación e importancia de la investigación..……………………………….…….  4. Delimitación de la investigación……………………………………………………….  **CAPÍTULO II**………………………………………………………………………………..  **MARCO TEÓRICO**…………………………………………………………………………  1. Antecedentes de la Investigación...………………………………………….………..  2. Bases Teóricas.......................................................................................................  2.1. Protocolo de internet versión 6……………………………………………......…….  2.2. Arquitectura de Direccionamiento Ipv6…………………………………………..…  2.3. Formato de la cabecera IPv4 - IPv6…………………………….………….……….  2.4. Calidad de servicio (QoS)…………………………………………………….………  2.4.1. Modelos Calidad de servicios.............................................…………..………..  2.4.1.1. Servicio de Mejor Esfuerzo...........................................................................  2.4.1.2. Arquitectura de Servicios Integrados (ISA)...................................................  2.4.1.3. Arquitectura de Servicios Diferenciados (DiffServ).......................................  2.4.2. Manejo de Congestión………………………………………………………….…..  2.5. Redes Inalámbricas (WLAN)...............................................................................  2.5.1. Topologías de redes.........................................................................................  2.5.2. Estándares WLAN............................................................................................  2.6. Red de área amplia (WAN).................................................................................  2.6.1. Sistemas Autónomos………………………………………………………………  2.6.2. Protocolo de Enrutamiento de Pasarela Frontera (BGP)………………………  2.6.2.1. Procedimientos Funcionales del BGP…………………………………………  2.6.2.2. Formato de los Mensajes BGP………………………………………………….  2.7. Términos básicos…...…………………………………………………………………  **CAPÍTULO III**……………………………………………………………………………….  **MARCO METODOLÓGICO**………………………………………………………………  1. Tipo de investigación……………………………………………………………………  2. Diseño de Investigación………………………………………………………………..  3. Técnicas e Instrumentos de Recolección de Datos…………………………………  4. Metodología………………………………………………………………………………  5. Herramientas Utilizadas..…………………………….…………………………………  6. Diseño del Experimento………………………………………………………………...  **CAPÍTULO IV**……………………………………………………………………………….  **ANALISIS Y DISCUSIÓN DE LOS RESULTADOS**………………………..…………  1. Análisis y descripción de los Resultados……………………………………….….....  1.2. Sustentación teórica de los Resultados………………….……………………….  2. Análisis estadísticos de los resultados………………………………………………..  **CONCLUSIONES**………………………………………………………………………….  **RECOMENDACIONES**……………………………………………………………………  **ANEXO**………………………………………………………………………………………  **ÍNDICE DE REFERENCIAS**……………………………………………………………… | 15  16  16  18  18  18  18  20  21  22  22  23  23  27  31  35  36  36  36  37  43  45  46  47  50  52  54  54  55  57  59  60  60  60  61  61  67  69  83  84  84  89  90  98  99  100  101 |
|  |  |

**ÍNDICE DE ILUSTRACIONES**

|  |  |  |
| --- | --- | --- |
| **Imágenes** | **Titulo** | **Pág.** |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35  36 | Nomenclatura de direcciones IPv6……………………………………...  Cabecera IPV4…………………………………………………………….  Cabecera IPV6…………………………………………………………….  Datos analizables con Match y listas de acceso……………………...  Marcado con Diffserv y sin Diffserv……………………………………..  Categorías de tráfico……………………………………………………..  Topologías de redes………………………………………………………  Implementación serial de DTE y DCE…………………………………..  Conexión serial interconectada………………………………………….  Interfaces fijas……………………………………………………………..  Interfaces de puerto serial modular……………………………………..  Sistema Autónomo……...…………..……………………………………  Mensajes de BGP…………………………………..……………………..  Formato de los mensajes de BGP.……………………………………...  Topología y/o ambiente de pruebas……………………………..……...  Configuración del Router 1……………………………………………....  Configuración del Router 2……………………………………………….  Configuración de Switches 1 y 2………………………………………...  Pruebas con IPERF para detectar el ancho de banda del ambiente..  Configuración de Listas de Acceso de los protocolos IPv4 / IPv6…...  Configuración de Clases de Tráficos de los protocolos IPv4 / IPv6…  Configuración de Marcado y Políticas de Tráficos en IPv4 / IPv6…...  Captura de Transmisión por medio del Wireshark ver. .1.4.4………..  Aplicación de Filtros en Wireshark ver. 1.4.4……....……..…………...  Configuración de VideoLAN en la PC de Destino...…………………...  Comienzo de la emisión de Video……….………………………………  Elección del protocolo RTP………………………………………………  Configuración de Dirección y Puerto de Destino………………………  Último paso para iniciar la transmisión………………………………….  Configuración de DITG en la PC de Destino en espera de transmisión…………………………………………………………………  Configuración de DITG en la PC de Destino en espera de transmisión…………………………………………………………………  Ejemplo de captura de resultados de DITG para Datos y Voz……….  Ejemplo de captura de Bitrate en Wireshark…………………………...  Decodificación en Protocolo RTP de paquetes en Wireshark………..  Analizador de Flujo RTP en Wireshark…………………………………  Ejemplo de cálculo de delay y jitter usando Excel……………………. | 29  31  33  38  39  39  46  50  50  51  51  52  53  55  62  63  64  65  68  71  71  72  73  74  74  75  75  76  76  77  77  78  79  80  80  81 |
| **Tablas** | **Titulo** | **Pág.** |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14 | Ejemplo de Consolidación de datos obtenidos de IPv4/IP6 sin QoS Tráfico Bajo………………………………………………………………...  Ejemplo de Resumen de Tablas categorizadas por los indicadores de QoS……………………………………………………………………..  Tabla de Resultados Totales del Porcentaje (%) de Paquetes Perdidos……………………………………………………………………  Tabla de Resultados Totales del Delay (Latencia)……………………  Tabla de Resultados Totales del Jitter………………………………….  Tabla de Resultados Totales del Bitrate……………………………….  Tabla de valores de Porcentaje de Paquetes Perdidos en SPSS….  Tabla ANOVA del Porcentaje de Paquetes Perdidos…………………  Tabla de Valores de Delay en SPSS…………………….……..……...  Tabla ANOVA del Delay………………………………………………....  Tabla de Valores del Jitter ……………………………………………….  Tabla ANOVA del Jitter.………..………………………………………...  Tabla de Valores del Bitrate……………………………………………...  Tabla ANOVA del Bitrate.………………………………………………... | 81  82  84  86  87  88  92  92  93  94  95  95  96  97 |
| **Gráficos** | **Titulo** | **Pág.** |
| 1  2  3  4 | Gráfico de Porcentaje de Paquetes Perdidos………………………….  Gráfico de Delay (Latencia)…………………..………………………….  Gráfico del Jitter………………………………..………………………….  Gráfico del Bitrate………….…………………..…………………………. | 85  86  87  89 |
| **Anexos** | **Titulo** | **Pág**. |
| 1  2 | Tabla de Distribución F de Fisher con 0,05% de Coeficiente de Confianza………………………………………………….……………….  Intervalo de Coeficiente de Confianza α……………………………….. | 101  101 |

**INTRODUCCIÓN**

En la actualidad, la interconexión de computadoras personales y dispositivos electrónicos se extiende cada vez mayor, la cual hace que las direcciones IPv4 se acaben de manera fulminante. Por tal razón, se implementaron tecnología como el NAT para tratar de frenar un poco el agotamiento de dichas direcciones. Sin embargo, el uso de esta tecnología hace que muchos dispositivos de redes no puedan comunicarse públicamente. Por tal motivo, se desarrollaron el nuevo protocolo IPv6.

El protocolo IPv6 además de resolver el problema de agotamiento de direcciones IP, también ofrece muchas otras mejoras frente al antecesor IPv4, las cuales se describirán más adelante en este proyecto, dado que este protocolo IPv6 está en maduración y no ha sido muy estudiado en todos los ambientes de red existentes.(Granados, 2010)

El propósito de este proyecto estuvo enmarcado en el estudio e implementación del nuevo protocolo de Internet IPv6, con el fin de conocer sus funcionalidades y características que lo hacen considerablemente mejor que IPv4, dado que el mismo no ha cambiado desde su definición inicial y, aunque ha probado ser robusto y trabajar en redes globales, no siempre es capaz de adaptarse a las exigencias actuales.

En base a lo anterior se consideró pertinente evaluar la calidad de servicio bajo BGP en Sistemas Autónomos conectados por Enlace Inalámbrico a 5.7 Ghz y nodos móviles en IPv6 y así de alguna manera, hacer posible la implementación y estudio de IPv6, para poder llegar a un análisis comparativo entre IPv4 e IPv6 que permitió definir ciertos criterios de operatividad del nuevo protocolo.

Para ello, el proyecto se ha dividido, en un primer capítulo que especifica el problema, justificación e importancia del mismo, así como también el objetivo general y los objetivos específicos a desarrollar; un segundo capítulo que da soporte a los antecedentes de esta investigación y las bases teóricas en la cual fue desarrollado el proyecto; un tercer capítulo, en el cual se detalla el tipo y diseño de investigación, metodología utilizada, diseño del experimento; y por último, un cuarto capítulo, el análisis y descripción de los resultados.

**CAPÍTULO I**

**PLANTEAMIENTO DEL PROBLEMA**

1.- Planteamiento del problema.

# El crecimiento exponencial de Internet está llevando hacia el agotamiento de las direcciones IPv4, es decir a la progresiva merma de la cantidad de direcciones IPv4 disponibles. Este tema ha sido una preocupación desde los años 80, y se hace más inminente en 1993, cuando de manera oficial se pronostica el próximo fin de la era de IPv4, según el RFC1519: *“A esta tasa de crecimiento, todas las clases B serán agotadas dentro de aproximadamente 15 meses.”.*

# Como consecuencia, se ha convertido en el factor impulsor en la creación y adopción de diversas nuevas tecnologías, incluidas las direcciones CIDR (Classless Inter-Domain Routing, Enrutamiento Inter-Dominios sin Clases) y NAT (Network Address Translation, Traducción de Dirección de Red) como soluciones a corto plazo, mientras que el IPv6 se ve como un remedio a largo plazo para el agotamiento de las direcciones IPv4 (Bagnulo, 2004).

El IPv4 posibilita 232 ó unos 4294 millones de direcciones, en cambio el IPv6 admite 2128 ó 3,4 x 1038 ó 340 sextillones direcciones. El nuevo protocolo, no sólo ofrece un espacio mayor de direcciones, sino que además mejora o soluciona algunos problemas de su antecesor IPv4, tales como Direccionamiento público a cada dispositivo conectado a Internet, Movilidad basado en IPv6 (MIPv6) y mayor nivel de Seguridad por defecto (IPsec). (Díaz y col, 2007)

Estas nuevas características de IPv6 permiten dar mayor confiabilidad a las redes inalámbricas. Al incrementar estas propiedades hace que las redes con medio no guiado se emparejan cada vez más a las redes cableadas. Por lo tanto, su implementación se extiende hasta en las redes a gran escala como los Sistemas Autónomos, o *“Conjunto conexo de redes IP y Enrutadores (Router) bajo el control de una o varias organizaciones y con política de Enrutamiento común (RFC1930).”* (Fabero, 2008). Los Sistemas Autónomos son comúnmente los ISP (Internet Service Provider, Proveedor de Servicio de Internet) de un país, organizaciones trasnacionales e instituciones de gran flujo de datos en sus redes.

Por razones geográficas no siempre se puede establecer una conexión cableada entre los Sistemas Autónomos, por lo que se recurre a las redes inalámbricas. Tales motivos se pueden destacar: los ríos o bosques como obstáculos naturales que dificulta la instalación de cables; y patrimonios históricos, por tener una estructura de edificación inalterable que impide cualquier trabajo de cableado físico.

Actualmente, los Sistemas Autónomos se comunican entre sí bajo el protocolo IPv4 y BGP (Border Gateway Protocol, Protocolo de Enlace de Frontera), el cual *“es un protocolo de ruteo exterior para la comunicación entre routers en diferentes ASs.”* (Pezoa, 2002). Sin embargo, la gran madurez que está experimentando últimamente IPv6, obliga que hasta los Sistemas Autónomos lo implementen lo más rápido posible, tanto para cubrir todas las demandas de las direcciones IP requeridas, como para aprovechar todas las potencialidades que ofrece el IPv6 y estar a la par con los avances tecnológicos a nivel mundial.

Además, debido a la diferencia del tamaño de la cabecera de los paquetes entre el protocolo Ipv4 e IPv6 se hace notable el estudio comparativo en este ambiente de los Sistemas Autónomos, especialmente en enlaces inalámbricos donde se ha comprobado que se obtienen notables pérdidas de señal con respecto a los enlaces cableados; esta característica se afianza ya que según *“La potencia de la señal se ve disminuida por la dispersión geométrica del frente de onda, conocida comúnmente como pérdida en el espacio libre.”* (Flickenger, 2006)

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

2.- Objetivos de la Investigación

2.1.-Objetivo General

Analizar el comportamiento del protocolo IPv6 en Sistemas Autónomos conectados por enlaces de 5.7 GHz usando parámetros de medición de QoS y nodos móviles.

2.2.-Objetivos Específicos

* Investigar sobre IPv6, Sistemas Autónomos, WLAN y los parámetros de medición de QoS.
* Diseñar las topologías del ambiente de pruebas de Sistemas Autónomos.
* Configurar el entorno de trabajo en base a enlaces inalámbricos de 5.7 GHz entre sistemas autónomos y nodos móviles.
* Realizar pruebas según los parámetros de medición de Calidad de Servicio (QoS).
* Analizar los datos obtenidos aplicando un tratamiento estadístico.
* Aportar conclusiones a partir del análisis estadístico.

3.- Justificación e importancia de la investigación.

El desarrollo de la Internet desde sus inicios estuvo sumamente ligado al sector académico: redes de universidades y centro de investigaciones. El nuevo protocolo IPv6 no fue la excepción logrando su despliegue científico en el área antes mencionada. Con esta investigación se pretende que la Universidad del Zulia sea una de las instituciones pioneras en el estudio del protocolo emergente. Como consecuencia, se puede beneficiar de lo siguiente:

*“Mientras más tiempo se deje pasar en empezar a habilitar y probar IPv6, mayores serán los costos en inversión en aspectos como actualizaciones en Humanware, software y hardware; aunque se estima que los precios más altos en la transición a IPv6 ocurrirán con el entrenamiento y no con el software.” (*Fernández, 2007, s/p*).*

Además, la implementación de este protocolo IPv6 resuelve ampliamente las deficiencias nativas del IPv4, tanto a nivel de seguridad como movilidad, sin olvidar de la solución que daría IPv6 al problema del agotamiento de direcciones IP. Con esto, se permitiría la incorporación de nuevos dispositivos que tendrán direcciones IP públicas sin ningún inconveniente, logrando que estos aparatos se comuniquen entre sí sin restricciones de redes privadas del NAT. (Millán, 2004)

Para aprovechar al máximo las virtudes del naciente protocolo IPv6, los Sistemas Autónomos son los mejores candidatos a adoptarlo ya que estas grandes redes son principalmente los Proveedores de Servicios de Internet (ISP) que dan conectividad al mundo cibernético y a los usuarios finales. La transición del IPv4 a IPv6, puede ser más eficaz si se implican a los ISPs lo antes posible, lo que además, a la larga, les facilitará el ofrecer nuevos e incluso mejores servicios y aplicaciones, u ofrecer mejor calidad de servicio a los usuarios. (Millán, 2004)

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

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

En consecuencia, la realización de esta investigación aportará muchos elementos metodológicos de relevancia en la administración de redes y mejor aprovechamiento del ancho de banda, basándose en la sugerencia de la implementación del nuevo protocolo en redes inalámbricas dentro del ambiente de los Sistemas Autónomos. Por otra parte, se estará manteniendo a la Universidad del Zulia a la vanguardia de nuevas implementaciones para laboratorios, haciendo varias combinaciones entre el protocolo joven, calidad de servicio y redes inalámbricas.

4.- Delimitación de la investigación.

El transcurso de la investigación y de las pruebas realizadas sobre la misma, fueron realizadas en la Unidad de Redes e Ingeniería Telemática (URIT) adscrita al Departamento de Computación de la Facultad Experimental de Ciencias de la Universidad del Zulia desde febrero del 2010 hasta julio del 2011.

**CAPÍTULO II**

**CAPÍTULO II**

**MARCO TEÓRICO**

1.- Antecedentes de la Investigación.

Se han realizado algunas investigaciones serias sobre IPv6, incluyendo en ellas la implementación en redes inalámbricas, así mismo se tomaron en cuenta investigaciones sobre Calidad de Servicio en diferentes circunstancias de una red. Entre los diversos artículos, publicaciones, exposiciones realizados sobre los términos que enmarca esta investigación tenemos:

Castro (2009), realizó un proyecto de investigación en la Universidad del Zulia, que lleva por título “**Calidad de servicio de una WAN complementada con tecnología inalámbrica y el protocolo de Internet versión 6**”, brindando grandes aportes a ésta investigacióndeterminando la influencia de IPv6 respecto al rendimiento que ofrece en los extremos inalámbricos de una red de área amplia, así como un esquema comparativo entre el protocolo IPv6 e IPv4, así como el tratamiento estadístico para determinar la significancia de las diferencias entre ambos protocolos.

También en la Universidad Politécnica de Cataluña, Julian-Bertomeu (2005), realizó su proyecto de grado, que tiene por título**: Evaluación de los parámetros de QoS en entornos de Movilidad IP.** En dicho proyecto, se realizó el análisis de los parámetros de calidad de servicio para las comunicaciones de usuarios móviles y más concretamente en el proceso de handover que es donde más se pueden percibir y acusar degradaciones en la calidad de servicio. A través de esta indagación, se pudo apreciar el comportamiento de QoS en el entorno móvil, destacando la disminución del rendimiento de la red. Con esto, se hizo posible el entendimiento de las posibles causas de pérdidas de señal en el entorno móvil y la parametrización de la Calidad de Servicio en dicho ambiente, las cuales se tomaron como base en esta investigación

Por su parte, Majkowski y Palacio (2003), realizaron una investigación denominada “**Calidad de servicio en WLAN considerando un escenario mixto IEEE 802.11e y IEEE 802.11b**”, poniendo de manifiesto la necesidad de incluir mecanismos apropiados de gestión de recursos radio en redes IEEE 802.11 si se quiere garantizar la QoS en un sistema con acceso compartido entre las estaciones de tipo 802.11b y 802.11e. Esta indagación sirvió como base en esta investigación para establecer la prioridad en trasmisiones o aplicaciones de tiempo real que requieren de garantía de Calidad de Servicio como Video.

Por último, Hurtado (2009), realizó la investigación denominada “**Medición de Calidad de Servicio Bajo Protocolo BGP (Border Gateway Protocol) e IPv6”,** la cual tuvo como objetivo principal determinar la influencia del IPv6 en el protocolo de enrutamiento de frontera (BGP) mediante el uso de la calidad de servicio. Utilizó un diseño experimental que permitió crear ambientes de redes con y sin tráfico, bajo esquemas combinados entre IPv4 e IPv6. Mediante este trabajo, fue posible crear el marco teórico de todo lo referente al protocolo de enrutamiento entre los Sistemas Autónomos en la investigación.

2.- Bases teóricas.

2.1.- Protocolo de Internet versión 6 (IPv6).

Definición

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

El pro­tocolo actual, IPv4, cuenta con un espacio de direcciones de 32 bits que proporciona en teoría 4 billones de hosts direccionales a escala mundial, aunque, en la práctica, muchos menos, lo que hace que IPv4 no pueda soportar el aumento de los hosts que hay conectados globalmente. Network Address Translation (NAT) ha ampliado la vida de IPv4 junto a la asignación de las direcciones privadas, pero ésta no puede soportar el crecimiento de Internet y de los servicios P2P. IPv6 no sólo solventa este problema, sino también el de la escasez de direcciones, proporcionando un espacio de 128 bits que pueden permitir la asignación de un número casi ilimitado de direcciones, y el aumento de la seguridad de la red. (Díaz y col, 2007)

Las consecuencias de retrasar la implantación de IPv6, según Jordi Palet, CEO y director de Tecnología en Consulintel e involucrado en la organización IPv6 Forum, no es sólo que se incrementa el costo de la misma, sino la pérdida de oportunidades: “la transición a IPv6 es similar al efecto 2000, aunque en este caso no hay una fecha fija que nos obligue”. El experto ase­gura que las ventajas de IPv6 son, además de un mayor espacio para las direcciones, la escalabilidad, ya que ha sido diseñado para crecer sin los límites y parches de IPv4; una seguridad implícita, pues IPsec es obligatorio como parte del protocolo; y la movilidad, ya que facilita la nueva ge­neración de aplicaciones. En suma, “IPv6 nos abre las puertas de Internet para que ésta sea la base de las aplicaciones de nueva generación, muchas de las cuales ni siquiera podemos imaginar”. (Millán, 2004)

Según Millán (2004), IPv6 está diseñado especialmente para redes de alto rendimiento, como por ejemplo las redes ATM, pero manteniendo la eficiencia en redes de bajo ancho de banda, como por ejemplo en redes inalámbricas. Se prevé que se empiece a desplegar de una manera gradual, puesto que hay que mantener todas las infraestructuras que actualmente funcionan con IPv4.

Según Millán (2004), la necesidad de migrar a IPv6 está originada por las nuevas tendencias en el mundo actual de las telecomunicaciones, que podemos resumir en:

* La creciente movilidad de los usuarios de Internet, que desean acceder a los mismos servicios en cualquier momento y desde cualquier lugar.
* Las redes domesticas con avanzados sistemas de televigilancia, control, y seguridad.
* La convergencia de voz, video y datos, en infraestructuras basadas en IP.

Características principales.

Como se ha comentado, IPv6 fue diseñado como una evolución natural de IPv4. Es decir, todo lo que funcionaba perfectamente en IPv4 se ha mantenido, lo que no funcionaba se ha eliminado, y se ha tratado de añadir nuevas funciones manteniendo la compatibilidad entre ambos protocolos. Las características principales de IPv6) son:

* Mayor espacio de direcciones: en IPv6, las direcciones se componen de 16 octetos (ocho bits de la forma 00001111), es decir, 128 bits. Esto da lugar a 2 elevado a 128 (340 sextillones) de direcciones IP. Así, cada usuario contaría para sí con un internet del tamaño de la actual, y todavía sobrarían direcciones. El IPv4 “apenas” brinda espacio para algo más de cuatro mil millones de direcciones. Este pasaje a 128 bits hace posible soportar más niveles de jerarquía de direccionamiento y un mayor número de nodos direccionales, y simplifica la autoconfiguración de direcciones, como se verá más adelante.
* Paquetes eficientes y extensibles, sin que haya fragmentación en los enrutadores, alineados a 64 bits. Y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del enrutador.
* Renumeración y *multihoming*, que facilita el cambio de proveedor de servicios.
* Características de movilidad: la capacidad para que un nodo de la red mantenga la misma dirección IP a pesar de que este se desplace físicamente a otra área. Es decir que sin importar su ubicación, este pueda seguir siendo accesible a través de la misma dirección IP. Sin esta capacidad, los paquetes destinados a un nodo móvil no estarán posibilitados para llegar a destino mientras el nodo móvil se encuentre alejado de su enlace principal.
* Calidad de servicio y clases de servicios: IPv6 puede diferenciar los paquetes de datos como pertenecientes a un flujo particular, y así otorgar un ancho de banda en función de cada necesidad, ya sea para correo electrónico, comunicaciones de voz o videoconferencia. IPv6 puede soportar tráfico de información en tiempo real gracias a una etiqueta de flujo que permite al enrutador distinguir los paquetes en este periodo al asignar las direcciones de forma automática.
* Seguridad: IPv6 emplea como parte integral el entorno de seguridad IPSec, que no está implementado en todos los hosts del IPv4. Mediante ese entorno se logra la seguridad, confidencialidad e integridad del mensaje y la autentificación del remitente.
* Auto configuración de los nodos: Uno de los aspectos fundamentales de IPv6 es la incorporación de mecanismos que permitan la conexión automática (modelo *plug and play*) de equipos a la red. Pueden construirse direcciones globales usando como parte local la dirección MAC de un equipo y obteniendo el prefijo a través de un servidor de la red.
* Aplicaciones anycast y multicast: en IPv4 hay tres tipos de direcciones a las que dirigir un paquete IP: unicast (de un host hacia otro nodo), multicast (a varios nodos) y broadcast (a todos los nodos). En IPv6, los tipos de direcciones que existen son unicast, multicast y anycast.
* Wireless: IPv6 tiene cada vez más respaldo del sector de servicios inalámbricos. Así lo demuestra la alianza entre la Wireless Communications Association International (WCA) y el IPv6 Forum, por la cual ambas entidades colaborarán para hacer de IPv6 el protocolo de los nuevos servicios inalámbricos de acceso a Internet.
* Formato de encabezado más simple: el encabezado IPv6 es más sencillo y su tamaño es fijo. Se han suprimido campos como el checksum y los de fragmentación, y agregado uno para identificar flujos de datos. Las funciones de los campos eliminados se logran con encabezados de extensión, que permiten incorporar nuevas características al protocolo, como IPSec o movilidad.
* End to end: IPv6 no usa NAT, ya que tiene direcciones globales para todos los nodos. Así, éstos pueden reenviar cada paquete sin alterar su contenido. Uno de los problemas más graves de IPv4 es el tamaño de las tablas de ruteo en los enrutadores. En IPv6 se bajan las 130 mil entradas de las tablas de ruteo a sólo 10 mil. Esta reducción mejora el reenvío, ya que la dirección de destino de cada paquete que pasa por un enrutador tiene que buscarse en esa tabla.

2.2.- Arquitectura de direccionamiento IPv6.

Direccionamiento IPv6.

Según Millán (2004), las direcciones en IPv6, soportan un número de bits que cuadruplica al utilizado por las direcciones IPv4. Así, mientras el espacio de direccionamiento total en IPv4 es de 232 (4.294.967.296), en IPv6 lo es de 2128 (340.282.366.920.938.463. 463.374.607.431.768.211.456).

Para hacerse una idea del tremendo espacio de direcciones disponible, se suele indicar que esto supone, en un sentido teórico, más de 665.570 trillones de direcciones por metro cuadrado de la superficie del planeta Tierra.

Las direcciones IPv6 de 128 bits identifican interfaces individuales o grupos de interfaces. Las direcciones IPv6, cualquiera que sea el tipo, se asignan a las interfaces, no a los nodos. Puesto que cada interfaz pertenece a un único nodo, cualquiera de las direcciones de interfaces *unicast* de ese nodo podrá ser utilizada como un identificador del nodo. Una única interfaz puede tener múltiples direcciones IPv6 de cualquier tipo. Por ejemplo, una interfaz podrá tener una dirección *unicast*, otra *anycast*, y otra *multicast* simultáneamente.

Se distinguen tres tipos de direcciones en IPv6 según Millán (2004):

* *Unicast:* Las direcciones *unicast* identifican a una única interfaz, es decir, un paquete enviado a una dirección *unicast* será entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales. Estas direcciones pueden tener 3 alcances distintos.
* *Anycast***:** Las direcciones *anycast* identifican un grupo de interfaces, de forma que un paquete enviado a una dirección *anycast* será entregado a un miembro cualquiera del grupo, siendo generalmente el más cercano según la distancia asignada en el protocolo de enrutamiento.
* *Multicast***:** Las direcciones *multicast* identifican, al igual que las *anycast*, a un grupo de interfaces, pero un paquete enviado a una dirección *multicast* es enviado a todas las interfaces del grupo. Las direcciones de *broadcast* no existen en IPv6, su misión ha sido suplantada por las direcciones *multicast*.

El tipo específico de dirección IPv6 viene indicado por los primeros bits de la dirección. Este campo de longitud variable es denominado prefijo y permite conocer dónde está conectado un determinado nodo, es decir, su ruta de enrutamiento. La dirección IPv6 se compone, por consiguiente, de un prefijo seguido de un identificador de nodo.

- Ámbitos.

El protocolo IPv6 añade soporte para direcciones de distintos ámbitos, lo que quiere decir que tendremos direcciones globales y no globales. Si bien con IPv4 ya habíamos empleado direccionamiento no global con la ayuda de prefijos de red privados, con IPv6 esta noción forma parte de la propia arquitectura de direccionamiento. Cada dirección IPv6 tiene un ámbito, que es un área dentro de la cual ésta puede ser utilizada como identificador único de una o varias interfaces. El ámbito de cada dirección forma parte de la misma dirección, con lo que vamos a poder diferenciarlos a simple vista. (Peralta L, 2002)

- Nomenclatura de las direcciones

Tenemos tres formas comunes de representar direcciones IPv6 en texto según Peralta (2002):

* x:x:x:x:x:x:x:x donde cada x es el valor en hexadecimal de cada grupo de 16 bits de la dirección.
* x:x::x en el caso de que haya grupos contiguos de 16 bits todos cero. Es una abreviatura que servirá para hacer más cómodo el uso de algunas direcciones. Podemos ver un ejemplo comparativo de este caso y el anterior en la Imagen N º 1.
* x:x:x:x:x:x:d.d.d.d, donde las x son los seis grupos de 16 bits en hexadecimal de mayor peso de la dirección y las d son los valores decimales de los cuatro grupos de 8 bis de menor peso de la dirección. Esta forma es a veces más conveniente a la hora de manejar entornos mixtos IPv6 e IPv4. Por ejemplo: 0:0:0:0:0:FFFF:129.144.52.38 y en su forma abreviada ::FFFF:129.144.52.38.

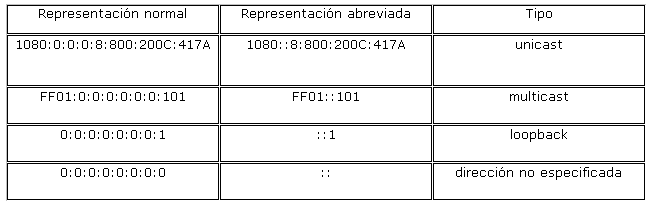


Imagen N° 1: Nomenclatura de direcciones IPv6.

Fuente: Peralta L (2002).

Para las direcciones unicast distinguimos tres ámbitos:

* + Link-local: para comunicaciones en el mismo enlace (no atraviesan los enrutadores). Empiezan todas por fe80:.
  + Site-local: local, para identificar interfaces en un mismo ’sitio’. La definición de ’sitio’ es un tanto genérica, pero en principio un ’sitio’ es el área topológica de red perteneciente a un edificio o un campus, perteneciente a una misma organización. Empiezan por fec0:.
  + Global: para comunicaciones con servicios públicos. Para identificar interfaces en toda Internet. Estas comienzan por 2001: o 3ffe:.

En lo que a ámbito se refiere, las direcciones anycast siguen la misma norma que las unicast. Sin embargo, para las direcciones multicast tenemos catorce posibles ámbitos, que identifican desde un interfaz local a una dirección global. Nodos de un mismo ámbito y visibles entre sí definen una zona. No se permite que un enrutador encamine tráfico entre diferentes zonas (perderían todo el sentido los ámbitos). (Peralta L, 2002)

Una de las grandes ventajas de los ámbitos es que permitirá la renumeración de prefijos sin mucha dificultad, ya que las direcciones de ámbito no global se mantendrán. Tenemos que esperar que se produzca alguna renumeración de prefijos globales, ya que según crezca una organización su prefijo se puede quedar pequeño y necesitar más espacio de direcciones. Y como hemos dicho antes, se tratará siempre que sea posible de mantener las tablas de enrutamiento al mínimo. Lo que sólo se consigue dando un prefijo nuevo mayor e invalidando el anterior, porque lo que seguramente sucederá será que las redes contiguas ya estén asignadas. (Peralta L, 2002)

- Nomenclatura de los prefijos

Según Peralta (2002), la representación de los prefijos de direcciones con IPv6 es similar a la que tenemos con CIDR con IPv4, dirección-ipv6/tamaño-prefijo. Donde dirección-ipv6 es alguna de las notaciones vistas en la sección anterior y tamaño-prefijo es un valor decimal que especifica cuantos bits de la dirección corresponden al prefijo. Por ejemplo, el prefijo en hexadecimal es 3FFE33300002, que son 48 bits, lo podemos escribir como:

3FFE:3330:0002:0000:0000:0000:0000:0000/48

3FFE:3330:2:0:0:0:0:0/48

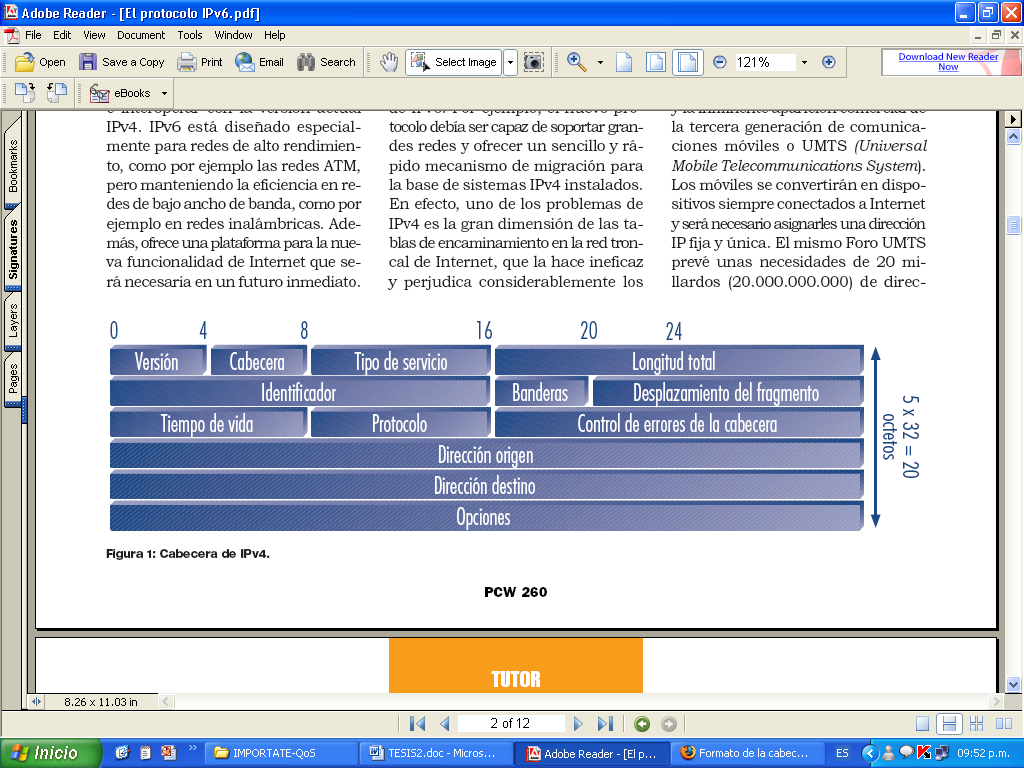
3FFE:3330:2::/48

Si queremos escribir la dirección y el prefijo, no hace falta que escribamos los dos de forma explícita. Por ejemplo, una dirección IPv6 del mismo prefijo asociado quedaría 3FFE:3330:2:1:250:BAFF:FE7A:E67E/48.

2.3- Formato de la cabecera IPv4 - IPv6

Según lo indicado por Millán (2004) la cabecera de IPv6, descrita principalmente en la RFC 2460, elimina o hace opcionales varios campos de la cabecera de IPv4, consiguiendo una cabecera de tamaño fijo y más simple, con el fin de reducir el tiempo de procesamiento de los paquetes manejados y limitar el coste en ancho de banda de la cabecera de IPv6.

La cabecera de IPv4, mostrada en la imagen 2, tiene una longitud variable mínima de 20 octetos. El bit más significativo se numera por 0 a la izquierda, y el menos significativo se numera por 31 a la derecha. La forma de transmitir los diferentes bytes sigue el orden conocido por *big endian*, es decir, de izquierda a derecha y de arriba abajo según la estructura presentada en la Imagen Nº 2. La cabecera consta de los siguientes campos:

  
Imagen N° 2. Cabecera IPV4.

Fuente: Millán R (2004).

**Versión (4 bits).** Es el número de versión de IP, es decir, 4.

**Cabecera (4 bits).** Especifica la longitud total de la cabecera en palabras de 32 bits. El valor mínimo y más común es de 5, siendo la longitud de cabecera mínima. Puesto que el campo es de 4 bits, se limita la longitud total de la cabecera a 60 bytes.

**Tipo de servicio (8 bits):** el campo tipo de servicio, TOS (Type Of Servíce), especifica la prioridad del paquete basándose en el retardo, rendimiento, seguridad y los requerimientos de coste se asigna 3 bits para los niveles de prioridad (llamada precedencia) y cuatro bits para indicar las necesidades especificas (en concreto retardo, rendimiento, coste y seguridad).

**Longitud total (16 bits):** Especifica el tamaño total del paquete, incluyendo la cabecera y los datos, en bytes.

**Identificador (16 bits):** Es un número único asignado por el dispositivo que envía el paquete, con el fin de que el destinatario pueda reensamblar un paquete fragmentado por los nodos intermedios.

**Banderas (3 bits).** Es un campo para el control de la fragmentación. El primer bit no es utilizado y esté siempre puesto a 0. Si el segundo bit es 0, significa que puede haber fragmentación, y si es 1, significa que no puede haber fragmentación. Si el tercer bit es 0, indica que es el último fragmento, y si es 1, indica que aún hay más fragmentos.

**Desplazamiento del fragmento (13 bits).** Es utilizado en los paquetes que han sido fragmentados para posibilitar el reensamblado total del paquete. Su valor indica el número de bloques de 8 bytes (sin contabilizar los bytes de la cabecera) que estaban contenidos en los fragmentos previos. En el primer fragmento, o en un .único fragmento, este valor es siempre 0.

**Tiempo de vida (8 bits):** el campo tiempo de vida, TTL (Time To Live), se define para indicar la cantidad de tiempo en segundos que se le permite al paquete permanecer en la red.

**Protocolo (8 bits):** Indica al protocolo de nivel superior al que IP deberá pasar los datos del paquete. Por ejemplo, UDP es 17 y TCP es 6.

**Control de errores de la cabecera (16 bits).** Es un campo para controlar los errores únicamente en la cabecera IP, exceptuando este campo.

**Dirección origen (32 bits).** Es la dirección del origen del paquete.

**Dirección destino (32 bits).** Es la dirección del destino del paquete.

**Opciones (variable).** No son requeridas en todos los paquetes.

La cabecera básica de IPv6, mostrada en la Imagen Nº 3, tiene una longitud fija de 40 octetos, consistiendo en los siguientes campos:

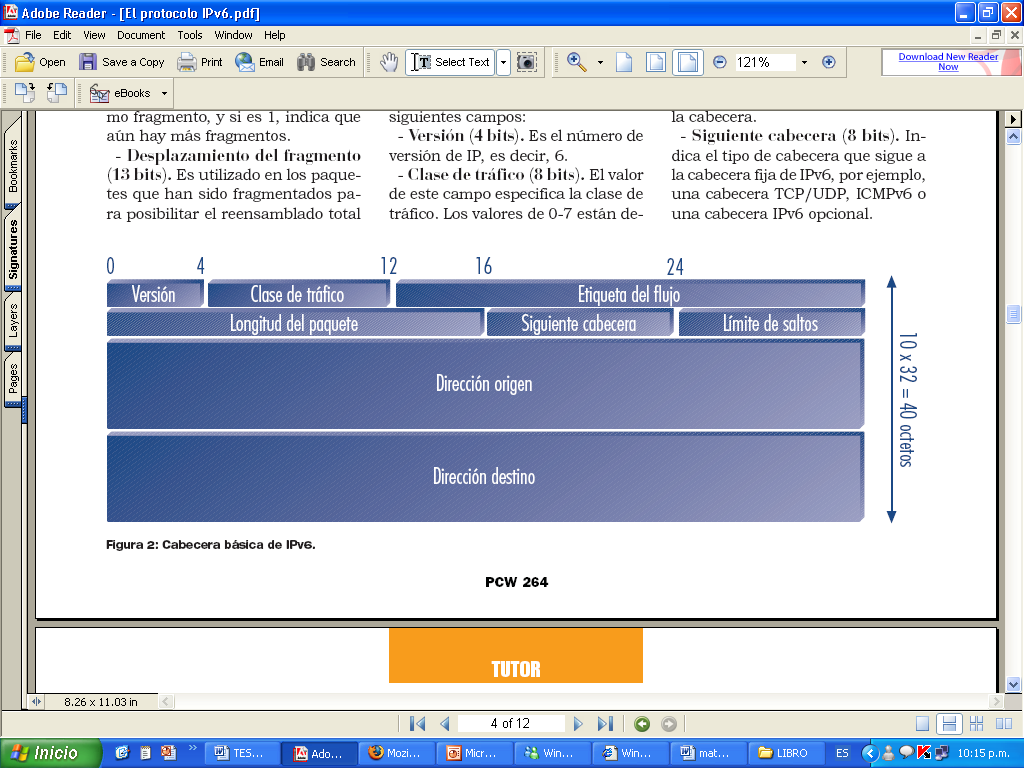


Imagen N° 3. Cabecera IPV6.

Fuente: Millán R (2004).

**Versión (4 bits).** Es el número de versión de IP, es decir, 6.

**Clase de tráfico (8 bits).** El valor de este campo especifica la clase de tráfico. Los valores de 0-7 están definidos para tráfico de datos con control de la congestión, y de 8-15 para tráfico de vídeo y audio sin control de la congestión.

**Etiqueta del flujo (20 bits).** El estándar IPv6 define un flujo como una secuencia de paquetes enviados desde un origen específico a un destino específico. Un flujo se identifica únicamente por la combinación de una dirección fuente y una etiqueta de 20 bits. De este modo, la fuente asigna la misma etiqueta a todos los paquetes que forman parte del mismo flujo. La utilización de esta etiqueta, que identifica un camino a lo largo de la red, permite conmutar en vez de encaminar. Su uso viene descrito en la RFC 1809.

**Longitud del paquete (16 bits).** Especifica el tamaño total del paquete, incluyendo la cabecera y los datos, en bytes. Es necesario porque también hay campos opcionales en la cabecera.

**Siguiente cabecera (8 bits).** Indica el tipo de cabecera que sigue a la cabecera fija de IPv6, por ejemplo, una cabecera TCP/UDP, ICMPv6 o una cabecera IPv6 opcional.

**Límite de saltos (8 bits).** Es el número de saltos máximo que le queda al paquete. El límite de saltos es establecido a un valor máximo por el origen y reducido en 1 cada vez que un nodo encamina el paquete. Si el límite de saltos disminuye y toma el valor 0, el paquete es descartado.

**Dirección origen (128 bits).** Es la dirección del origen del paquete.

**Dirección destino (128 bits).** Es la dirección del destino del paquete.

Se puede observar, de los 12 campos de la cabecera de IPv4 se ha pasado a 8 campos en IPv6. El motivo fundamental por el que estos campos (tipo de servicio, indicadores, identificación y control de errores) son eliminados es la innecesaria redundancia. En IPv4 se está facilitando la misma información de diversas formas, como es el caso del campo de control de errores, pues otros mecanismos de encapsulado de capas inferiores, por ejemplo IEEE 802, ya realizan esta función. El campo de desplazamiento de fragmentación de IPv4 ha sido eliminado, porque los paquetes ya no son fragmentados en los nodos intermedios, en IPv6 es un proceso que se produce extremo a extremo. El único campo realmente nuevo en IPv6 es la etiqueta de flujo.

2.4.- Calidad de Servicio (QoS).

Definición

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

Según Álvarez (2005), durante los últimos años han surgido variados métodos para establecer QoS en equipamientos de redes. Algoritmos avanzados de manejos de cola, modeladores de tráfico (traffic shaping), y mecanismos de filtrado mediante listas de acceso (access-list), han hecho que el proceso de elegir una estrategia de QoS sea más delicado. Cada red puede tomar ventaja de distintos aspectos en implementaciones de QoS para obtener una mayor eficiencia, ya sea para redes de pequeñas corporaciones, empresas o proveedores de servicios de Internet.

En términos generales, puede definirse la Calidad del Servicio (QoS) como la capacidad que tiene un sistema de asegurar, con un grado de fiabilidad preestablecido, que se cumplan los requisitos de tráfico, en términos de perfil y ancho de banda, para un flujo de información dado. (Sendazo, 2002).

2.4.1- Modelos de calidad de servicio.

2.4.1.1.- Servicio de Mejor Esfuerzo.

Se le llama servicio de mejor esfuerzo al que la red provee cuando hace todo lo posible para intentar entregar el paquete a su destino, donde no hay garantía de que esto ocurra. Una aplicación enviará datos en cualquier cantidad, cuando lo necesite, sin pedir permiso o notificar a la red. Éste es el modelo utilizado por las aplicaciones de FTP y HTTP. Obviamente, no es el modelo apropiado para aplicaciones sensibles al retardo o variaciones de ancho de banda, las cuales necesitan de un tratamiento especial. (Álvarez, 2005)

2.4.1.2.- Arquitetura de Servicios Integrados (ISA).

Explica García (2002), que para proporcionar diferentes compromisos de QoS, el IETF ha desarrollado el modelo de servicios integrados, que requieren que recursos tales como el ancho de banda y la memoria temporal sean reservados explícitamente para un flujo de datos dado para asegurar que la aplicación recibe su QoS solicitada. Esta estructura requiere la utilización de *clasificadores de paquetes* para identificar flujos que van a recibir un cierto nivel se servicio. También requiere la utilización de un *gestor de salida de paquetes* para tratar el envió de diferentes flujos de paquetes en la forma en la que se asegura que se satisfacen los compromisos de QoS. El *control de admisión* también es necesario para determinar si un dispositivo de enrutamiento tiene recursos necesarios para aceptar un flujo nuevo.

El protocolo de reserva de recursos, RSVP (Resource Reservation Protocol), se utiliza en el modelo de servicios integrados para proporcionar los mensajes de reserva necesarios para establecer un flujo con una QoS solicitada a través de la red. RSVP se utiliza para informar a cada dispositivo de enrutamiento de la QoS solicitada, y si se encuentra admisible el flujo, cada dispositivo de enrutamiento, a su vez, ajusta su clasificador de paquetes y el gestor de salida para tratar el paquete de datos dado. (Danysoft, 2006)

Para describir el tráfico y las necesidades de QoS de un flujo se utiliza un *descriptor de flujo*. Este descriptor consiste en dos partes: una *especificación de filtro (filterspec)* que proporciona la información requerida por el clasificador de paquetes para identificar los paquetes que pertenecen al flujo y una *especificación de flujo (flowspec)* que consiste en una *especificación de tráfico (Tspec*) y una *especificación de solicitud de servicio* *(Rspec).* La Tspec especifica el comportamiento del tráfico. La Rspec describe la QoS solicitada en términos de ancho de banda, retardo de los paquetes y perdida de paquetes.

2.4.1.3.- Arquitectura de Servicios Diferenciados (DiffServ).

Para García (2002), el modelo de servicios integrados fue el primer paso para proporcionar QoS en una red. Sin embargo, este modelo requiere que un dispositivo de enrutamiento mantenga un estado específico de flujo para cada flujo que está manteniendo el dispositivo de enrutamiento. Esta necesidad proporciona algunas preocupaciones. Primero, la cantidad de información de estado se incrementa proporcionalmente con el número de flujos. De esta forma los dispositivos de enrutamiento podrían necesitar un espacio de almacenamiento enorme y demandar una gran potencia de procesamiento. Segundo, el modelo de servicios integrados hace que los dispositivos de enrutamiento sean más complejos, ya que necesitan implementar el protocolo RSVP, el control de admisión, el clasificador de paquetes y algoritmos sofisticados de gestión de salida de paquetes.

A causa de las cuestiones de escalabilidad y complejidad asociadas al modelo de servicios integrados, IETF ha introducido otro modelo de servicio llamado modelo de servicios diferenciados, DS (Differentiated Services), que fue pensado para que sea más simple y más escalable.

Para Valencia (2008), en Diffserv los paquetes son clasificados y marcados en el origen, y en base a clases. El resto de los equipos de la red utilizarán la información de marcado de cada paquete y técnicas de gestión de colas para priorizar unos tráficos frente a otros. Puede clasificarse el tráfico en base al flujo al que pertenece (IP y puerto origen y destino), y aplicar alguna acción de Calidad de Servicio a ese flujo completo o en base a una clase (Se identifica la clase con el análisis de la cabecera IP, listas de acceso, interface por el que entra, entre otras).

Lo ideal es hacer la clasificación y el marcado lo más cerca de origen que sea posible. Si el tráfico marcado atraviesa varios sistemas autónomos, hay que fijar con ellos las reglas de QoS.

Marcado y Clasificación

Según Valencia (2008), consiste en marcar cada paquete con una determinada prioridad en función de la calidad de servicio que se le desea asignar. DiffServ cuenta con los enrutadores de bordes para realizar la clasificación de los distintos tipos de tráfico que circulan por la red, es necesario clasificar este tráfico en clases y determinar la forma en que serán manejadas estas clases de tráfico a medida que circulan por la red. Se marca en el campo DS o lo que es igual Differenciated Services Code Point (DSCP), de la cabecera IP, para indicar el PHB (comportamiento por salto) que debe experimentar un paquete en cada nodo. DSCP sustituye los tres bits de IP precedente del campo de Tipo de Servicio (TOS) del paquete IPv4, al igual que el campo Clase de Tráfico (CoT) de ocho bits del paquete IPv6, por seis bits, los otros dos bits están actualmente sin utilizar CU (Currently Unused). Esto le permite configurar hasta 64 prioridades de tráfico diferentes. (Valencia, 2008)

En el modelo DS, los valores diferentes del campo DS corresponden a diferentes tratamientos de envío de paquetes en cada dispositivo de enrutamiento, llamados PHB (Per Hop Behaviors). A diferencia del modelo de servicios integrados donde el dispositivo de enrutamiento reserva algunos recursos para cada flujo, en el modelo DS el dispositivo de enrutamiento asigna recursos sobre la base de un agregado para cada PHB. (Valencia, 2008)

En particular, un código PHB implícito de 000000 se guarda para utilizado para el tráfico convencional del mejor esfuerzo, y el código 11xOOO se utiliza para tráfico de control de red. Si se recibe un paquete con un código no reconocido, el paquete se envía como si estuviera marcado con el código PHB implícito.

* Clasificación: El marcado por clases clasifica paquetes en clases en base a las cabeceras y a listas de acceso. La imagen Nº 4 representa los datos que pueden ser analizados:

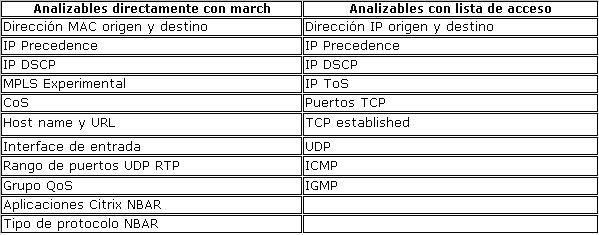


Imagen Nº 4: Datos analizables con Match y listas de acceso.

Fuente: Valencia (2008).

* Marcado: Reparto de los bits en el byte de ToS de IP, Ver Imagen N° 5:

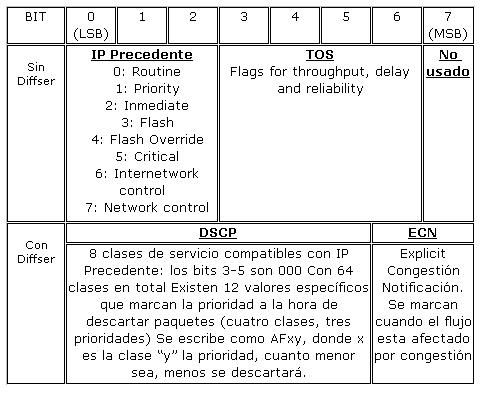


Imagen N° 5: Marcado con Diffserv y sin Diffserv.

Fuente: Valencia (2008).

El tráfico es marcado con la finalidad de que futuras clasificaciones sean más rápidas:

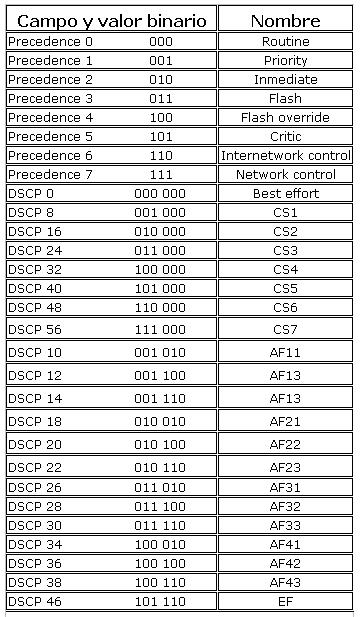


Imagen N° 6: Categorías de tráfico.

Fuente: Valencia (2008).

Comportamiento por salto.

El tratamiento estándar del mejor esfuerzo que implementan los dispositivos de enrutamiento cuando envían tráfico se define como el PHB implícito (DE). Para proporcionar clases adicionales de tráfico, la IETF ha definido PHB adicionales. Hasta ahora se han defino dos adicionales: PHB de envío rápido y el PHB de envió asegurado. (García, 2002)

El PHB de envío rápido, EF PHB (Expedited Forwarding PHB), proporciona un servicio extremo a extremo de bajas pérdidas, baja latencia, baja variación de retardo y con un ancho de banda asegurado a través de dominios DS. Para los puntos finales de la conexión, el servicio obtenido al utilizar EF PHB es equivalente a una «línea virtual alquilada». Este tipo de servicio se llama a veces «servicio de alta calidad». (García, 2002)

Para asegurar una latencia muy baja y el ancho de banda garantizado, la tasa de llegada del agregado de paquetes con EF PHB en cada nodo debería ser menor que el agregado mínimo permitido de la velocidad de salida. Así, cada nodo DS se debe configurar con una velocidad de salida mínima para EF PHB, independientemente de cualquier otro tráfico. Además, la velocidad de llegada del agregado se debe modelar y vigilar para que sea siempre menor que la velocidad de salida mínima configurada. (García, 2002)

Los paquetes que se marcan como EF PHB se codifican con el código 10 111 O. Cuando un paquete EF entra en un nodo DS, se situará en una cola de salida que se espera sea corta, y se le atiende rápidamente de forma que el tráfico EF mantenga significativamente niveles más bajos de latencia, de pérdida de paquetes y de variación del retardo. Para implementar EF PHB se pueden adoptar diferentes tipos de mecanismos de gestión de colas de salida, como cola con prioridad y cola pesada equitativa. Nótese que el modelo DS especifica el PHB pero no el mecanismo para proporcionar PHB. (García, 2002)

Para García (2002), el PHB de envío asegurado, AF PHB (Assured Forwarding PHB), entrega el tráfico agregado de un cliente particular con una seguridad alta (es decir, una probabilidad alta de que el tráfico se entregue al destino), mientras que el tráfico agregado no exceda el perfil de tráfico (por ejemplo, la tasa de información contratada). Al cliente, sin embargo, se le permite enviar su tráfico más allá del perfil de tráfico, con la advertencia de que al tráfico en exceso no se le dará una seguridad alta. A diferencia de EF PHB, AF PHB no está pensado para aplicaciones de baja latencia y baja variación del retardo.

Se han definido cuatro clases AF independientes en el grupo AF PHB que ofrecen varios niveles de seguridad en el envío. Dentro de cada clase AF, los paquetes tienen asignado uno de los tres posibles valores de precedencia de descarte. Si existe congestión en un nodo, la precedencia de descarte determina la importancia relativa del paquete dentro de la clase AF. Un nodo DS debe mantener la secuencia de paquetes IP en el mismo microflujo que pertenece a la misma clase AF, a pesar de los valores de precedencia de descarte.

Un paquete IP asociado con una clase AF i y una precedencia de descarte j se marca con un código AF AFij. Los valores recomendados del código Afij son los siguientes: AFll = 010100, AF12 = 001100, AF13 = 001110, AF2l = 010010, AF22 = 011100, AF23 = 010110, AF31 = 011010, AF32 = 011100, AF33 = 011110, AF4l = 100010, AF42 = 100100, AF43 = 100110. Dentro de cada clase AF el código AFx1 produce menor probabilidad de pérdida que el código AFx2, que, a su vez, produce una menor probabilidad de pérdida que el código AFx3.

Un servicio que el grupo AF PHB puede implementar es el servicio olímpico, que consta de tres clases de servicio: bronce, plata y oro. El objetivo es asignar los paquetes a estas tres clases de forma que los paquetes en la clase oro experimenten una carga más ligera que los paquetes en la clase plata y en la clase bronce. Las clases de servicio bronce, plata y oro se pueden asociar a las clases AF 1,2 Y 3, respectivamente. Los paquetes dentro de cada clase se pueden asociar a su vez a uno de los tres valores de precedencia de descarte.

2.4.2- Manejo de Congestión

Según Álvarez (2005), existen varios niveles en los cuales se puede proveer de calidad de servicio en una red IP. Uno de ellos es el de contar con una estrategia de manejo de los paquetes en caso de congestión, o evitar que la red alcance este estado, descartando paquetes a medida que estos ingresan a la red.

El manejo de congestión es un término general usado para nombrar los distintos tipos de estrategia de encolamiento que se utilizan para manejar situaciones donde la demanda de ancho de banda solicitada por las aplicaciones excede el ancho de banda total de la red, controlando la inyección de tráfico a la red, para que ciertos flujos tengan prioridad sobre otros, como los descritos por Álvarez (2005) a continuación:

a) **FIFO**. Es el tipo más simple de encolamiento, se basa en el siguiente concepto: el primer paquete en entrar a la interfaz, es el primero en salir. Es adecuado para interfaces de alta velocidad, sin embargo, no para bajas, ya que FIFO es capaz de manejar cantidades limitadas de ráfagas de datos. Si llegan más paquetes cuando la cola está llena, éstos son descartados. No tiene mecanismos de diferenciación de paquetes.

b) **Fair Queuing**. FQ, generalmente conocido como WFQ (Weighted Fair Queueing, en inglés), es un método automatizado que provee una justa asignación de ancho de banda para todo el tráfico de la red, utilizado habitualmente para enlaces de velocidades menores a 2048 [Kbps]. WFQ ordena el tráfico en flujos, utilizando una combinación de parámetros. Una vez distinguidos estos flujos, el enrutador determina cuáles son de uso intensivo o sensibles al retardo, priorizándolos y asegurando que los flujos de alto volumen sean empujados al final de la cola, y los volúmenes bajos, sensibles al retardo, sean empujados al principio de la cola. Sin embargo, la carga que significa para el procesador en los equipos de enrutamiento, hace de esta metodología poco escalable, al requerir recursos adicionales en la clasificación y manipulación dinámica de las colas.

c) **Priority Queuing**. El Encolamiento de Prioridad (Priority Queueing, en inglés) consiste en un conjunto de colas, clasificadas desde alta a baja prioridad. Cada paquete es asignado a una de estas colas, las cuales son servidas en estricto orden de prioridad. Las colas de mayor prioridad son siempre atendidas primero, luego la siguiente de menor prioridad y así. Si una cola de menor prioridad está siendo atendida, y un paquete ingresa a una cola de mayor prioridad, ésta es atendida inmediatamente. Este mecanismo se ajusta a condiciones donde existe un tráfico importante, pero puede causar la total falta de atención de colas de menor prioridad (starvation).

d) **Custom Queuing**. Para evadir la rigidez de PQ, se opta por utilizar Encolamiento Personalizado (CQ: Custom Queueing, en inglés). Permite al administrador priorizar el tráfico sin los efectos laterales de inanición de las colas de baja prioridad, especificando el número de paquetes o bytes que deben ser atendidos para cada cola. Se pueden crear hasta 16 colas para categorizar el tráfico, donde cada cola es atendida al estilo Round-Robin. CQ ofrece un mecanismo más refinado de encolamiento, pero no asegura una prioridad absoluta como PQ. Se utiliza CQ para proveer a tráficos particulares de un ancho de banda garantizado en un punto de posible congestión, asegurando para este tráfico una porción fija del ancho de banda y permitiendo al resto del tráfico utilizar los recursos disponibles.

e) **Class-Based WFQ**. WFQ tiene algunas limitaciones de escalamiento, ya que la implementación del algoritmo se ve afectada a medida que el tráfico por enlace aumenta; colapsa debido a la cantidad numerosa de flujos que analizar. Cada clase posee una cola separada, y todos los paquetes que cumplen el criterio definido para una clase en particular son asignados a dicha cola. Una vez que se establecen los criterios para las clases, es posible determinar cómo los paquetes pertenecientes a dicha clase serán manejados. Si una clase no utiliza su porción de ancho de banda, otras pueden hacerlo. Se pueden configurar específicamente el ancho de banda y límite de paquetes máximos (o profundidad de cola) para cada clase. El peso asignado a la cola de la clase es determinado mediante el ancho de banda asignado a dicha clase.

f) **Low Latency Queuing**. El Encolamiento de Baja Latencia (LLQ: Low-Latency Queueing, en inglés) es una mezcla entre Priority Queueing y Class-Based Weighted-Fair Queueing. Es actualmente el método de encolamiento recomendado para Voz sobre IP (VoIP) y Telefonía IP, que también trabajará apropiadamente con tráfico de videoconferencias. LLQ consta de colas de prioridad personalizadas, basadas en clases de tráfico, en conjunto con una cola de prioridad, la cual tiene preferencia absoluta sobre las otras colas. Si existe tráfico en la cola de prioridad, ésta es atendida antes que las otras colas de prioridad personalizadas. Si la cola de prioridad no está encolando paquetes, se procede a atender las otras colas según su prioridad. Debido a este comportamiento es necesario configurar un ancho de banda límite reservado para la cola de prioridad, evitando la inanición del resto de las colas.

2.5.- Redes Inalámbricas (WLAN).

Según Randall y col. (2003), una red inalámbrica de área local (WLAN, Wireless Local Area Network) es un sistema flexible de comunicación de datos implementado como extensión, o como alternativa, a una red LAN cableada, las redes WLAN transmiten y reciben datos por el aire mediante tecnología de radiofrecuencia, minimizando la necesidad de disponer de conexiones cableadas lo que, a su vez, combina la conectividad de datos con la movilidad de usuario.

Explican los autores, que las redes WLAN proporcionan toda la funcionalidad de las redes de área local, sin las correspondientes restricciones físicas, y las configuraciones disponibles abarcan desde topologías simples igualitarias a redes complejas que ofrecen conectividad distribuidas de datos y servicios de itinerancia. Además de ofrecer movilidad al usuario final dentro de un entorno de conexión de red, las redes WLAN permiten una portabilidad de la red física, lo que permite mover las redes de área local con los usuarios que las emplea.

Un usuario dentro de una red inalámbrica puede transmitir y recibir voz, datos y video dentro de edificios, entre edificios o campus universitarios, en áreas metropolitanas e incluso en áreas muy alejadas a velocidades de 11Mbps a 54 Mbps.

Las WLAN han surgido como una opción dentro de la corriente hacia la movilidad universal en base a una filosofía "seamless" o sin discontinuidades, es decir, que permita el paso a través de diferentes entornos de una manera transparente. Para ser considerada como WLAN, la red tiene que tener una velocidad de transmisión de tipo medio (el mínimo establecido por el IEEE 802.11 es de 1 Mbps, aunque las actuales tienen una velocidad del orden de 2 Mbps), y además deben trabajar en el entorno de frecuencias de 2,45 GHz. (UMAN, 2004).

2.5.1.- Topologías de redes

Según McQuerry (2008), el grado de complejidad de una red de área local inalámbrica es variable, dependiendo de las necesidades a cubrir y en función de los requerimientos del sistema que queramos implementar podemos utilizar diversas configuraciones de red. En la Imagen N º 7, se muestran ambas topologías.

* Ad hoc

La manera más simple de red inalámbrica se crea al conectar dos o más clientes inalámbricos en una red peer-to-peer. Una red inalámbrica establecida de esta manera se conoce como red ad-hoc y no incluye AP. Todos los clientes dentro de una red ad-hoc son iguales. El área cubierta por esta red se conoce como conjunto de servicios básicos independientes (IBSS, Independent Basic Service Set)[[1]](#footnote-2). Una red ad-hoc simple puede utilizarse para intercambiar archivos e información entre dispositivos sin el gasto ni la complejidad de comprar y configurar un AP.

* Modo de infraestructura

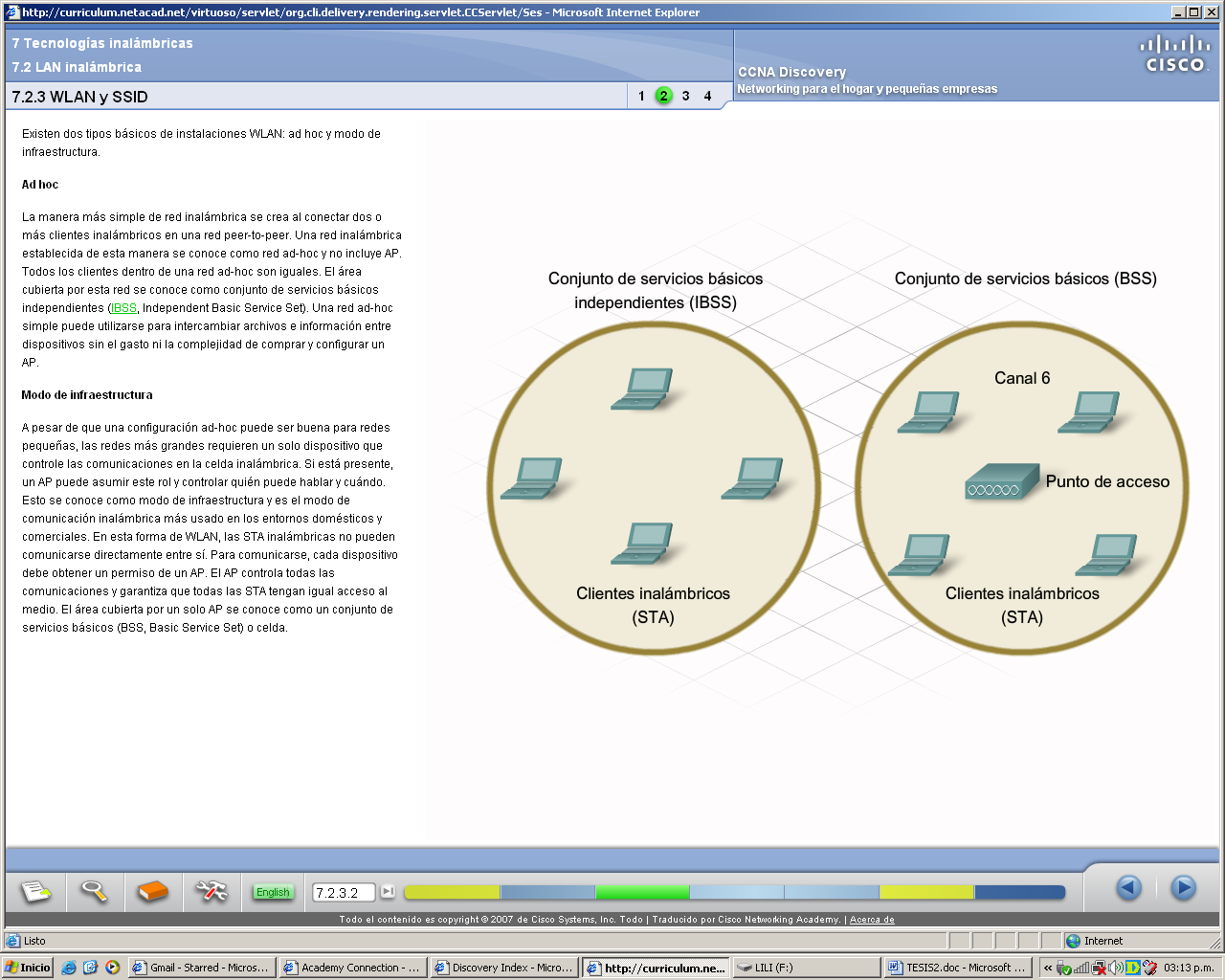
A pesar de que una configuración ad-hoc puede ser buena para redes pequeñas, las redes más grandes requieren un solo dispositivo que controle las comunicaciones en la celda inalámbrica. Si está presente, un AP puede asumir este rol y controlar quién puede hablar y cuándo. Esto se conoce como modo de infraestructura y es el modo de comunicación inalámbrica más usado en los entornos domésticos y comerciales. En esta forma de WLAN, las STA[[2]](#footnote-3) inalámbricas no pueden comunicarse directamente entre sí. Para comunicarse, cada dispositivo debe obtener un permiso de un AP. El AP controla todas las comunicaciones y garantiza que todas las STA tengan igual acceso al medio. El área cubierta por un solo AP se conoce como un conjunto de servicios básicos (BSS, Basic Service Set)[[3]](#footnote-4) o celda.

Imagen N° 7. Topologías de redes.

Fuente: Cisco (2007).

2.5.2.- Estándares WLAN

Según Mezquida (2004), sobre el mes de Junio de 1997 se concluyó el estándar IEEE 802.11, definido por la organización *Institute of Electrical and Electronics Engineers* (IEEE) para las transmisiones inalámbricas. Las primeras especificaciones eran relativamente lentas, siendo su velocidad de transmisión de 1 a 2 Mbps. Hacia el 1999, la IEEE facilito un nuevo estándar, IEEE 802.11b, en el que se aumentaba el rendimiento de las transmisiones a unos 11 Mbps.

A finales del 2002, apareció la marca registrada WI-FI (*Wireless Fidelity*), englobando el 802.11b y otros estándares más rápidos como el 802.11a. WI-FI es sinónimo del estándar IEEE "802.11b", protocolo de transmisión inalámbrica que logra alcanzar desde 2 Mbps hasta un máximo teórico de 11 Mbps. Este estándar fue creado por un grupo de fabricantes de dispositivos inalámbricos para mantener la compatibilidad entre sus productos y dar un grado de calidad a los productos *Wireless*.

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

**802.11b:** La revisión 802.11b del estándar original fue ratificada en 1999. 802.11b tiene una velocidad máxima de transmisión de 11 Mbit/s y utiliza el mismo método de acceso CSMA/CA definido en el estándar original. Debido al espacio ocupado por la codificación del protocolo CSMA/CA, en la práctica, la velocidad máxima de transmisión con este estándar es de aproximadamente 5.9 Mbit/s sobre TCP y 7.1 Mbit/s sobre UDP.

**802.11a:** La revisión 802.11a al estándar original fue ratificada en 1999. El estándar 802.11a utiliza el mismo juego de protocolos de base que el estándar original, opera en la banda de 5 GHz y utiliza 52 subportadoras orthogonal frequency division multiplexing (OFDM) con una velocidad máxima de 54 Mbit/s, lo que lo hace un estándar práctico para redes inalámbricas con velocidades reales de aproximadamente 20 Mbit/s.

La velocidad de datos se reduce a 48, 36, 24, 18, 12, 9 o 6 Mbit/s en caso necesario. 802.11a tiene 12 canales no solapados, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede interoperar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

**802.11g:** En Junio de 2003, se ratificó un tercer estándar de modulación: 802.11g. Este utiliza la banda de 2.4 GHz (al igual que el estándar 802.11b) pero opera a una velocidad teórica máxima de 54 Mbit/s, o cerca de 24.7 Mbit/s de velocidad real de transferencia, similar a la del estándar 802.11a. Es compatible con el estándar b y utiliza las mismas frecuencias. Buena parte del proceso de diseño del estándar lo tomó el hacer compatibles los dos estándares. Sin embargo, en redes bajo el estándar g la presencia de nodos bajo el estándar b reduce significativamente la velocidad de transmisión.

**802.11n:** En enero de 2004, la IEEE anunció la formación de un grupo de trabajo 802.11 (Tgn) para desarrollar una nueva revisión del estándar 802.11. La velocidad real de transmisión podría llegar a los 500 Mbps (lo que significa que las velocidades teóricas de transmisión serían aún mayores), y debería ser hasta 10 veces más rápida que una red bajo los estándares 802.11a y 802.11g, y cerca de 40 veces más rápida que una red bajo el estándar 802.11b.

**802.11e:** Con el estándar 802.11e, la tecnología IEEE 802.11 soporta tráfico en tiempo real en todo tipo de entornos y situaciones. Las aplicaciones en tiempo real son ahora una realidad por las garantías de Calidad de Servicio (QoS) proporcionado por el 802.11e. El objetivo del nuevo estándar 802.11e es introducir nuevos mecanismos a nivel de capa MAC para soportar los servicios que requieren garantías de Calidad de Servicio. Para cumplir con su objetivo IEEE 802.11e introduce un nuevo elemento llamado Hybrid Coordination Function (HCF) con dos tipos de acceso: (EDCA) Enhanced Distributed Channel Access y (HCCA) Controlled Channel Access.

**802.11i:** El estándar *802.11i* está destinado a mejorar la seguridad en la transferencia de datos (al administrar y distribuir claves, y al implementar el cifrado y la autenticación). Este estándar se basa en el *AES* (estándar de cifrado avanzado) y puede cifrar transmisiones que se ejecutan en las tecnologías 802.11a, 802.11b y 802.11g.

2.6.- Red de área amplia (WAN)

Una red de área amplia puede ser descripta como un grupo de redes individuales conectadas a través de extensas distancias geográficas. Las WAN interconectan las LAN, que a su vez proporcionan acceso a los computadores o a los servidores de archivos ubicados en otros lugares. Como las WAN conectan redes de usuarios dentro de un área geográfica extensa, permiten que las empresas se comuniquen entre sí a través de grandes distancias. Las WAN permiten que los computadores, impresoras y otros dispositivos de una LAN compartan y sean compartidas por redes en sitios distantes. Las WAN proporcionan comunicaciones instantáneas a través de zonas geográficas extensas. (Dye y col, 2007)

Conexiones seriales y enrutador

Los enrutadores son los responsables de enrutar paquetes de datos desde su origen hasta su destino en la LAN, y de proveer conectividad a la WAN. Dentro de un entorno de LAN, el enrutador contiene broadcasts, brinda servicios locales de resolución de direcciones, tal como ARP[[4]](#footnote-5), y puede segmentar la red utilizando una estructura de subred. Para brindar estos servicios, el enrutador debe conectarse a la LAN y a la WAN.

Además de determinar el tipo de cable, es necesario determinar si se requieren conectores DTE o DCE. El DTE es el punto final del dispositivo del usuario en un enlace WAN. El DCE en general es el punto donde la responsabilidad de enviar los datos se transfiere al proveedor de servicios.

Al conectarse en forma directa a un proveedor de servicios, o a un dispositivo como CSU/DSU que suministrará la señal de temporización, el enrutador actúa como DTE y necesita un cable serial DTE. (Imagen Nº 8).En general, esta es la forma de conectar los enrutadores. Sin embargo, hay casos en que los enrutadores tendrán que actuar como DCE. Al armar un escenario de enrutadores conectados espalda contra espalda en un ámbito de prueba, uno de los enrutadores debe ser DTE y el otro DCE (Imagen Nº 8).

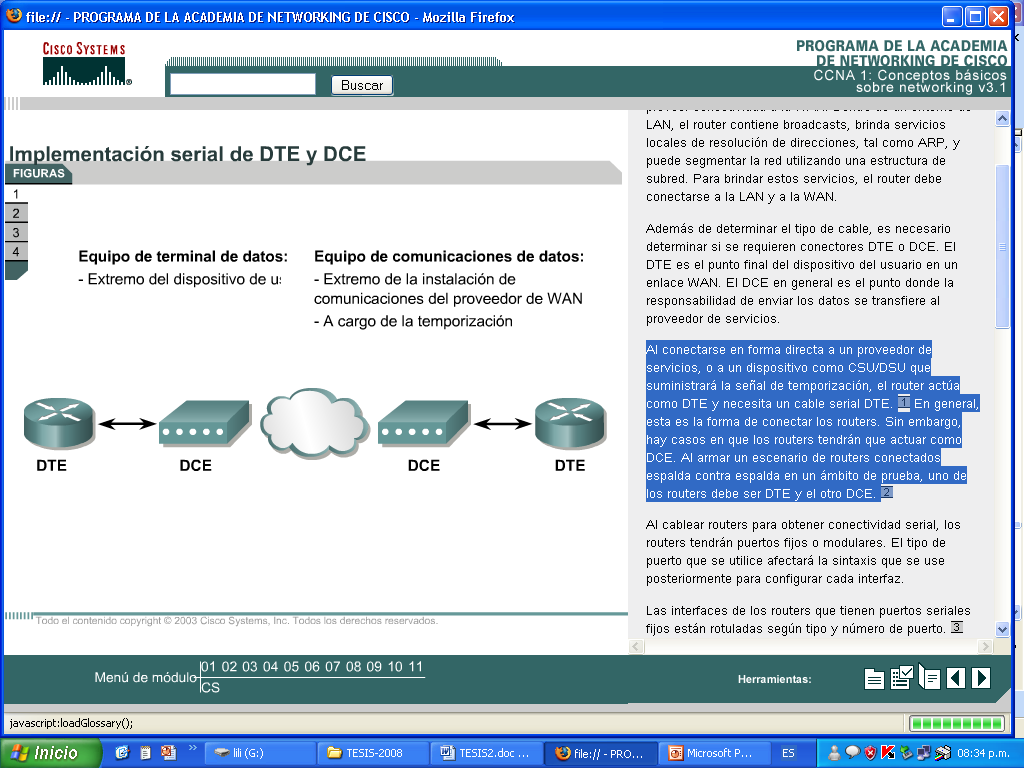


Imagen N° 8: Implementación serial de DTE y DCE.

Fuente: Cisco (2007).

Al cablear enrutadores para obtener conectividad serial, los enrutadores tendrán puertos fijos o modulares. El tipo de puerto que se utilice afectará la sintaxis que se use.

Imagen N° 9: Conexión serial interconectada.

Fuente: Cisco (2007).

Las interfaces de los enrutadores que tienen puertos seriales fijos están rotuladas según tipo y número de puerto. (Ver Imagen N º 10)

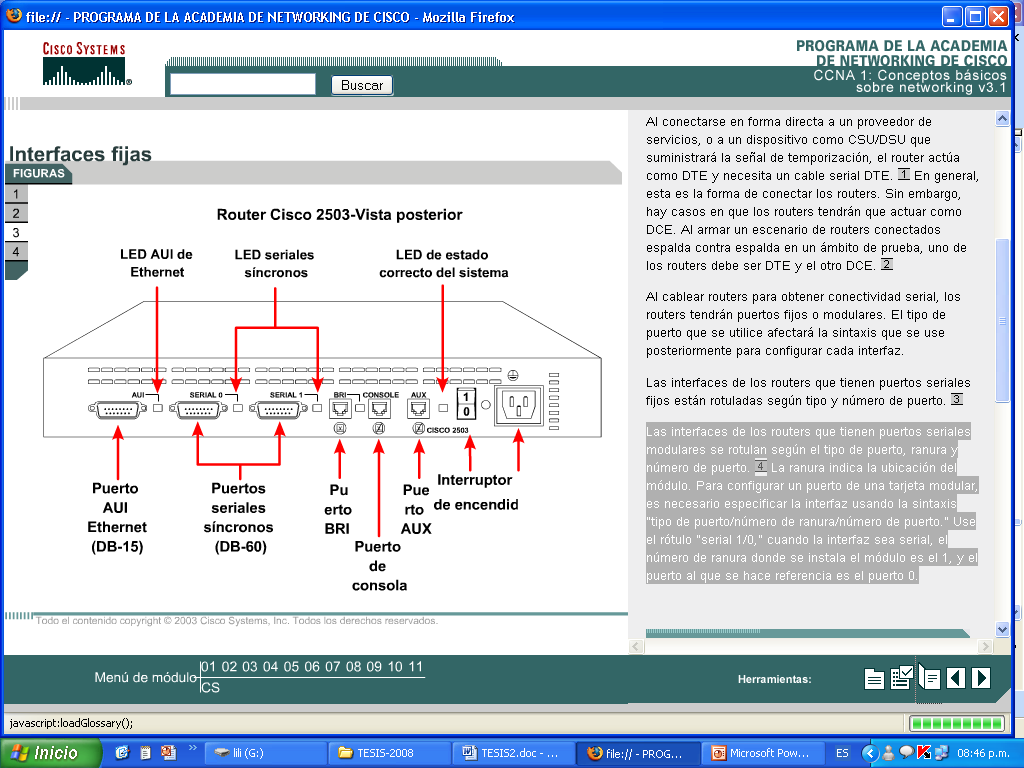


Figura Nº 10: Interfaces fijas.

Fuente: Cisco (2007).

Las interfaces de los enrutadores que tienen puertos seriales modulares se rotulan según el tipo de puerto, ranura y número de puerto (Imagen Nº 11).La ranura indica la ubicación del módulo. Para configurar un puerto de una tarjeta modular, es necesario especificar la interfaz usando la sintaxis "tipo de puerto/número de ranura/número de puerto." Use el rótulo "serial 1/0," cuando la interfaz sea serial, el número de ranura donde se instala el módulo es el 1, y el puerto al que se hace referencia es el puerto 0.

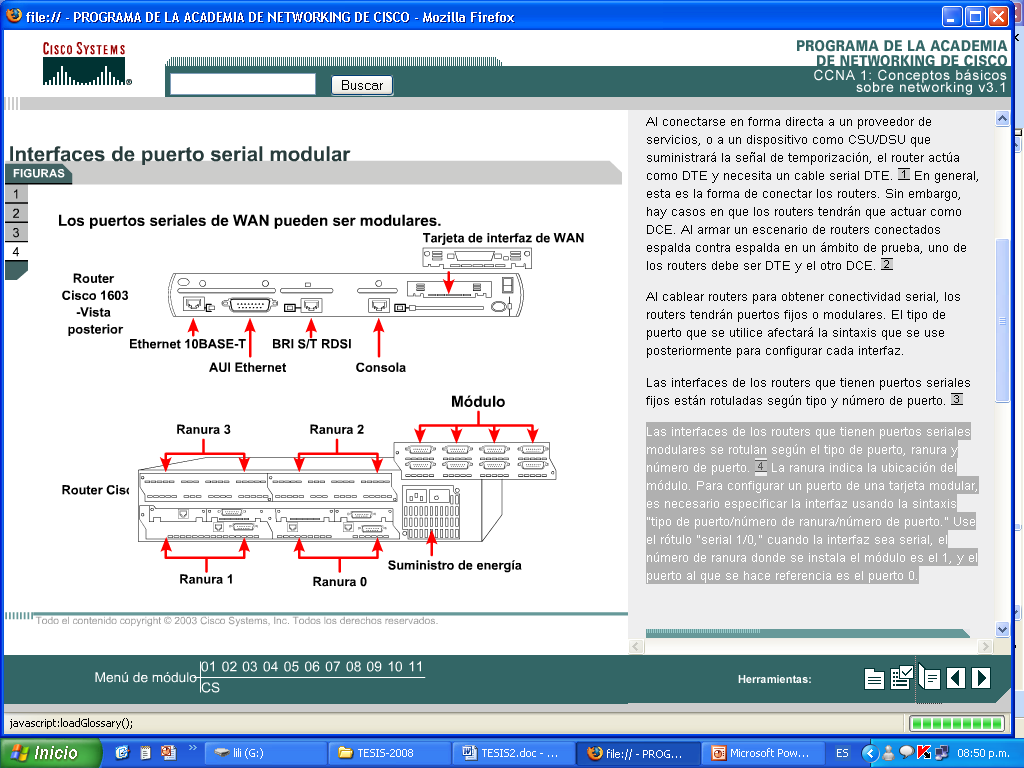


Imagen N° 11: Interfaces de puerto serial modular.

Fuente: Cisco (2007).

2.6.1.- Sistemas Autónomos

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



Imagen N° 12: Sistema Autónomo.

Fuente: Goitia (2003)

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

En Internet, la IANA es la organización que gestiona las direcciones IP y números de AS, teniendo en cuenta que cada Sistema Autónomo se identifica por un número inequívoco que no puede ser superior a 65535, teniendo en cuenta que la colección 65412-65535 son SA privados para ser utilizados entre los proveedores y los clientes. Así, podemos ponernos en contacto con RIPE, ARIN o APNIC para solicitar rangos de direcciones IP o números de AS.

2.6.2.- Protocolo de Enrutamiento de Pasarela Frontero: BGP

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

Es por eso que Stallings (2004) explicó que el protocolo de pasarela frontera (BGP) se desarrollo para su uso en conjunción con interconexiones en redes que empleen la arquitectura de protocolo TCP/IP, aunque los conceptos son aplicables a cualquier interconexión de redes. El protocolo de pasarela frontera se ha convertido en el protocolo de dispositivo de enrutamiento exterior preferido para Internet.

El protocolo de pasarela frontera (BGP, Border Gateway Protocol) se diseñó para permitir la cooperación en el intercambio de información de enrutamiento entre dispositivos de enrutamiento de diferentes sistemas autónomos (AS), llamado pasarelas en el estándar. El protocolo opera en términos de mensajes, que se envían utilizando conexiones TCP. El repertorio de mensajes se resume en el siguiente cuadro.

|  |  |
| --- | --- |
| Establecer | Utilizado para establecer una relación de vecindad con otro dispositivos de enrutamiento. |
| Actualizar | Utilizado para (1) transmitir información acerca de una única ruta y/o (2) enumerar rutas múltiples que se vallan a eliminar. |
| Mantener activa | Utilizado para (1) confirmar un mensaje “establecer” y (2) confirmar periódicamente la relación de vecindad. |
| Notificación | Se envía cuando se detecta una condición de error. |

Imagen N° 13: Mensajes de BGP.

Fuente: Stallings (2004).

2.6.2.1.- Procedimientos Funcionales del BGP:

Stallings (2004), menciona que el protocolo de pasarela frontera (BGP, Border Gateway Protocol) supone tres procedimientos funcionales, que son:

* Adquisición de vecino:

Se considera que son vecinos si están conectados a la misma subred. Si dos enrutadores se encuentran en sistemas autónomos diferentes, podrían desear intercambio de información de enrutamiento. Para este cometido, es necesario primero realizar la operación de adquisición de vecino. Básicamente, la adquisición de un vecino se produce cuando dos dispositivos de enrutamiento vecino de diferente sistema autónomo se ponen de acuerdo en intercambio regularmente información de enrutamiento. Para llevar a cabo la adquisición de vecino, un dispositivo de enrutamiento envía a otro un mensaje “establecer” (“Open”). Si el enrutador destino acepta la solicitud, devuelve un mensaje “mantener activa” (“Keepalive”) como respuesta.

* Detección de vecino alcanzable:

Una vez establecida la relación de vecino, se utiliza el procedimiento detección de vecino alcanzable para mantener la relación. Cada asociación necesita estar seguro de que el otro asociado existe y esta todavía comprometido con la relación de vecino. Con este propósito, ambos dispositivos de enrutamiento se envía periódicamente mensajes “mantener activa”.

* Detección de red alcanzable:

Cada dispositivo de enrutamiento mantiene una base de dato con las redes que puede alcanzar y la ruta preferida para ello. Siempre que se produzca un cambio en esta base de dato, el dispositivo de enrutamiento difunde un mensaje “actualizar” (“update”) a los otros dispositivo de enrutamiento que implemente BGP. Dado que el mensaje “actualizar” se envía por difusión, todos los enrutadores BGP pueden generar y mantener su información de enrutamiento.

2.6.2.2.- Formato de los Mensajes BGP:

Destaca Stallings (2004), que cada mensaje comienza con una cabecera de 19 bytes que contiene tres campos, como se indica en la parte sombreado de la Imagen No. 14.

* Marcador: reservado para autenticación. El emisor puede insertar un valor en este campo que se emplearía como parte de un mecanismo de autenticación para permitir al destino verificar la identidad del emisor.
* Longitud: longitud del mensaje en bytes.
* Tipo: tipo de mensaje: establecer, actualizar, notificación o mantener activa.



Imagen N° 14: Formato de los mensajes BGP.

Fuente: Stallings (2004).

2.7.- Términos básicos

**Ancho de banda:** cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. (Da Ros, 2006)

**Bitrate:** número de [bits](http://es.wikipedia.org/wiki/Bit) que se transmiten por unidad de tiempo a través de un [sistema de transmisión](http://es.wikipedia.org/wiki/Sistema_de_transmisi%C3%B3n) digital o entre dos dispositivos digitales. Así pues, es la velocidad de transferencia de datos. (Espina, 2007)

**Jitter**: es la variación en los retardos en la llegada de los paquetes entre su origen y el destino usualmente producida por congestión de tráfico en algún punto de la red o diferencia en el tiempo de transito de paquetes cuando estos viajan por diferentes rutas. (Certain, 2009)

**Latencia (Delay)**: es la cantidad de tiempo que le toma a un paquete viajar de un computador a otro y regresar al computador de origen, La latencia en la red debe ser lo más constante posible. (Raicu y Zeadally, 2003).

**Nodo Móvil:** es un terminal o enrutador que puede cambiar su punto de unión desde una red o subred a otra. (Millán, 2004).

**OSPF (Open Short Path First):** OSPF es un protocolo universal basado en el algoritmo de estado de enlace, desarrollado por el IETF para sustituir a RIP. Básicamente, OSPF utiliza un algoritmo que le permite calcular la distancia más corta entre la fuente y el destino al determinar la ruta para un grupo específico de paquetes. (Roldan, 2008.)

**Paquetes perdidos:** El porcentaje de paquetes que no llegan a su destino mide la pérdida de paquetes de la red. Esta pérdida puede producirse por errores en alguno de los equipos que permiten la conectividad de la red o por sobrepasar la capacidad de algún buffer de algún equipo o aplicación en momentos de congestión. (Certain A, 2009)

**RIPng (Routing Information Protocol next generation):** es un protocolo pensado para pequeñas redes, Se basa en el intercambio de información entre enrutadores, de forma que puedan calcular las rutas más adecuadas, de forma automática. (Valarezo, 2006.)

**UDP**: protocolo de nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión. (Garcia, 2002)

**CAPÍTULO III**

**CAPÍTULO III**

**MARCO METODOLÓGICO**

**1.- Tipo de investigación**

Según la naturaleza de los objetivos, el nivel de la investigación y la estrategia empleada por el investigador, la presente investigación se clasifica en exploratoria-descriptiva (Arias, 1999; Hernández y col, 2003):

Investigación Descriptiva: En esta se selecciona una serie de planteamientos y se mide o recolecta información sobre cada una de ellas, para así (válgase la redundancia) describir lo que se investiga. En esta investigación se establecieron diferentes pruebas repetitivas que permitieron describir o dar a conocer funcionalidades y características de Ipv6.

Investigación Exploratoria: Este tipo de estudio se genera cuando un problema en un área específica ha sido poco estudiado, se tiene muchas dudas acerca de él o no se ha abordado antes y las condiciones existentes no son aún determinantes. Se utiliza cuando la situación evidente que rodea al problema es poco determinante, de este modo sus resultados representan sólo una visión aproximada a dicho problema, lo cual se ajusta perfectamente al estudio ya que en el área de las telecomunicaciones y redes el nuevo protocolo IPv6 ha sido poco estudiado e implementado, y existen dudas respecto a si resuelve eficientemente las limitaciones nativas de Ipv4 en este caso referente a QoS y al comportamiento del mismo en la tecnología de conexiones inalámbricas.

**2.- Diseño de la investigación**

Según Hernández y col (2003), la precisión, la profundidad así como también el éxito de los resultados de la investigación dependen de la elección adecuada del diseño de investigación. La eficacia de cada uno de ellos depende de si se ajusta realmente a la investigación que se esté realizando.

Esta investigación se presenta mediante la manipulación de una variable no comprobada (IPv6 en Enlaces Inalámbricos), en condiciones rigurosamente controladas, con el fin de describir de qué modo y porqué causa se produce una situación o acontecimiento particular. En esta investigación se realizaron pruebas de confiabilidad de los datos a través de software estadístico y la repetición de las mismas.

**3.- Técnicas e instrumentos de Recolección de Datos**

Se recurrió al uso de fuentes secundarias como libros, trabajos de grado, artículos, revistas especializadas y consultas a diferentes sitios Web, para así recopilar la información básica sobre el tema y construir un marco teórico apropiado.

Las fuentes primarias también se usaron y fueron recolectadas mediante una observación simple indirecta. Según Méndez (2001), “La observación no directa o simple puede ser indirecta cuando se emplean elementos que registren aspectos visuales y auditivos del problema de investigación, entre otras)”. Para el caso de esta investigación se acudió a software estadísticos, software de generación y monitoreo de tráfico que recolectan datos por medios de variables asignadas en los mismos para así obtener datos que ayudaron a la investigación a determinar la influencia de Ipv6 con QoS en Sistemas Autónomos conectados por Enlace Inalámbrico a 5.7 Ghz.

**4.- Metodología**

Según Bisquerra (2000): “Todo método está compuesto por una serie de pasos para alcanzar una meta. De este modo los métodos de investigación describirían los pasos para alcanzar el fin de la investigación. Estos métodos o pasos determinaran como se recogen los datos y como se analizan, lo cual llevará a las conclusiones”.

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

Fase I: Recopilación de Información

Para el desarrollo de la investigación se recopiló información muy importante referente a los mecanismos, estructuras y configuración de calidad de servicio para cada protocolo IP, redes de área local inalámbrica, comandos de configuración de enrutadores, entre otros, utilizando los dos protocolos en comparación, Ipv6 e Ipv4, configuración de puntos de acceso y las características del protocolo Ipv6. Además de estos, se tuvo la necesidad de buscar y conocer software de monitoreo de red a fin de escoger el que mejor se adaptaba a la investigación. Así, entonces, fueron estudiados por medio de búsquedas en Internet, consultas de tesis, guías, revistas, libros, entre otras.

Fase II: Diseño y desarrollo de topologías y/o ambientes de pruebas de la red.

En esta se llevó a cabo la conexión total de los equipos pasivos y activos a través del diseño de una red WAN inalámbrica y nodos móviles.

Debido a que el modelo de enrutadores CISCO 1721 solo disponen de una interfaz Ethernet, y para este entorno de trabajo se requería un mínimo de dos interfaces Ethernet (Una para el Access Point y el otro para la Antena Ubiquiti), se tuvo que agregar un Switch CISCO 2924 en cada extremo y utilizar VLAN (Virtual LAN) para imitar que los enrutadores CISCO tuvieran más de dos puertos Ethernet. (Ver la Imagen N° 15)

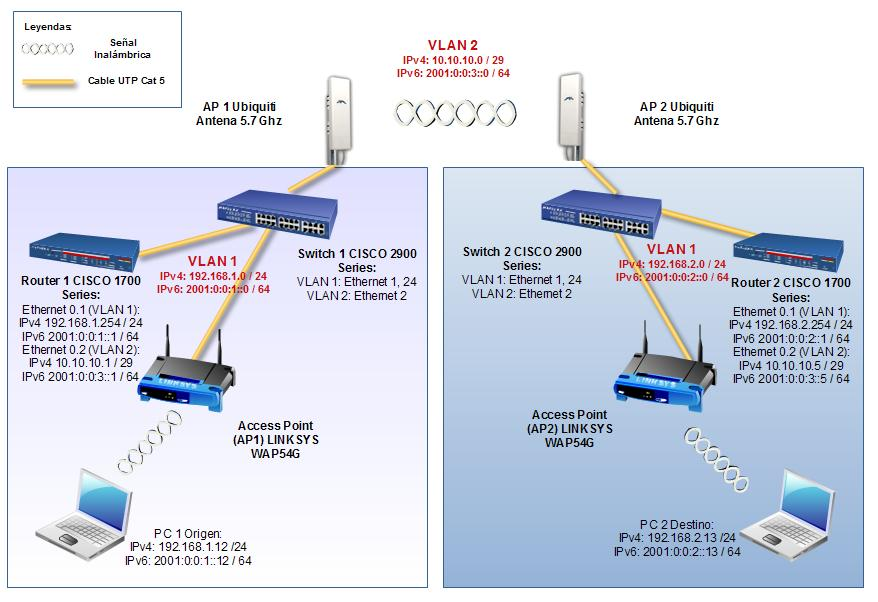


Imagen N° 15: Topología y/o ambiente de pruebas

Fuente: Propia (2011)

Luego, se procedió a conectar físicamente todas las interfaces Ethernet entre el AP, Switch y el enrutador mediante el cable UTP (Cat 5) para simular un Sistema Autónomo (SA). Así mismo, se hizo un procedimiento similar en el otro extremo para crear otro Sistema Autónomo. Posteriormente, se configuraron dos Antenas (AP Ubiquiti) en cada uno extremo de los dos Sistemas Autónomos creando un Enlace Inalámbrico a 5.7 Ghz. Seguidamente, se configuraron los dos APs de cada SA para formar dos redes inalámbricas en los extremos. Una vez finalizado esto, se inició la configuración de los distintos protocolos requeridos en este ambiente de pruebas, tales como RIPv2/RIPng, OSPF, BGP con IPv4 / IPv6. Dicha configuración se puede ver en las Figuras N° 16, 17 y 18.

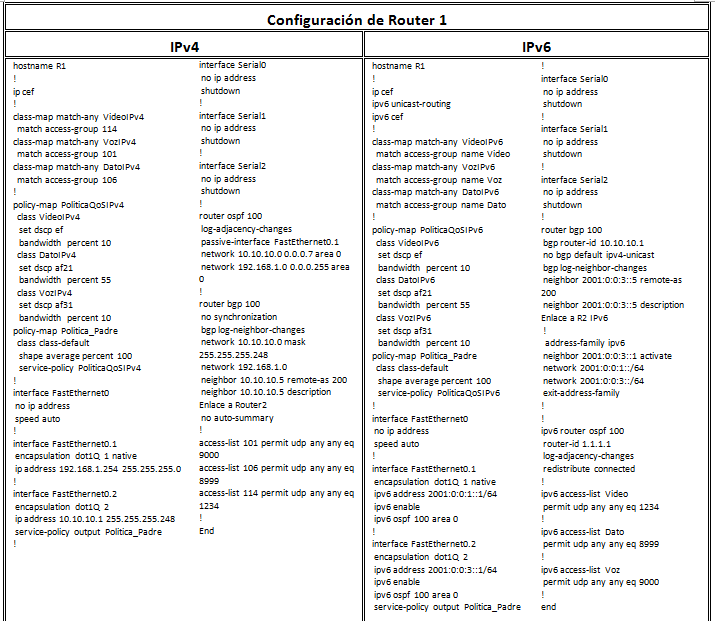


Imagen N° 16: Configuración del Router 1.

Fuente: Propia (2011)

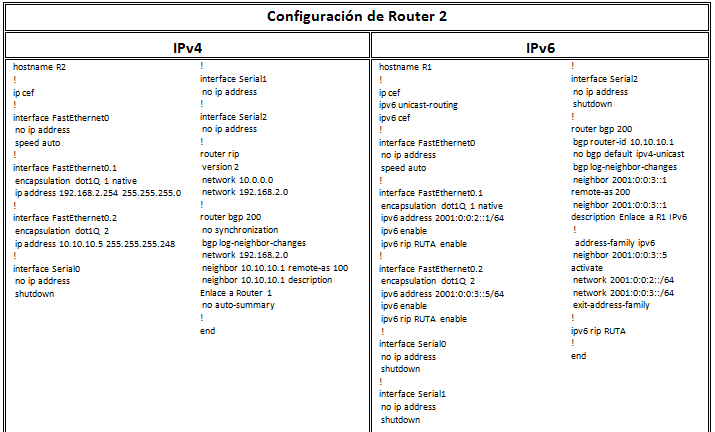


Imagen N° 17: Configuración del Router 2.

Fuente: Propia (2011)

Posterior a la configuración de los enrutadores Cisco, se procedió a configurar los Switches Cisco. En esta etapa, se crearon las Virtual LAN (VLAN) en cada una de los Switches para ayudar a los enrutadores a simular más de dos interfaces Ethernet y asignar los puertos o interfaces correspondientes a los VLAN creados. Tal configuración de los switches se pueden observar en la Imagen N° 18.

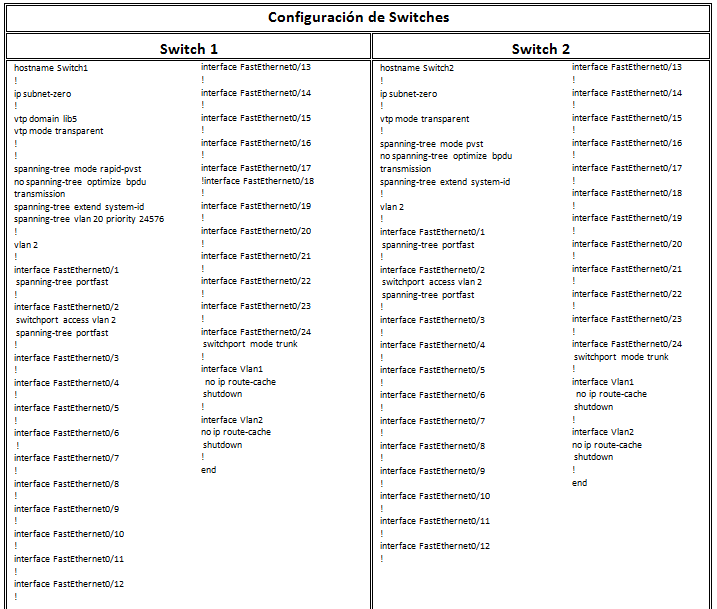


Imagen N° 18: Configuración de Switches 1 y 2.

Fuente: Propia (2011)

La comunicación y configuración con los enrutadores y switches CISCO se estableció por medio de un cable de consola a través de la interfaz de línea de comando de un programa de Terminal (Hyper Terminal). Finalmente, se procedió a configurar las PCs en cada extremo de los SA asignándoles direcciones IPv4 e IPv6 a través de la interfaz de red inalámbrica de Windows. El ambiente de pruebas y direccionamiento de la red se puede observar en la Imagen N° 15.

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

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

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

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

Fase IV: Análisis comparativo, tratamiento y análisis estadístico.

En esta Fase se trabajó con el software estadístico SPSS versión 15, utilizando la distribución Fisher y el procedimiento ANOVA en el cual se calculó el valor F y el valor P, dichos valores ayudaron a constatar estadísticamente los resultados obtenidos a través de las distintas pruebas.

5.- Herramientas utilizadas

Para el alcance de esta investigación de diseñaron topologías y/o ambientes de pruebas, las cuales necesitaron de las siguientes herramientas que fueron clasificadas según su tipo:

Dispositivos:

* Dos portátiles: Una con procesador Dual Core Intel de 2.0 Ghz, con 1 GB de memoria RAM y 80 GB de disco duro, y otra con procesador Intel Core i3 de 2.13 Ghz, con 3 GB de memoria RAM y 500GB de disco duro.
* Dos Enrutadores Cisco 1721 equipados con IOS 12.3 (24a) como sistema operativo del enrutador; en el cual se llevaron a cabo todas las configuraciones para el montaje de Ipv6 e IPv4 y la implementación de QoS en todas las pruebas.
* Dos Switches Cisco 2924 para simular que los Enrutadores tuvieran más de 2 puertos Ethernet.
* Dos Cables transpuestos de consola para enrutadores cisco.
* Dos puntos de acceso (APs) Ubiquiti Nano Station de 5.7 Ghz de frecuencia para crear el enlace inalámbrico entre los Sistemas Autónomos.
* Dos puntos de acceso (APs) o enrutador inalámbrico LINKSYS WAP54G v3.1 de 2.4 Ghz para la conexión con las redes locales en los extremos de los Sistemas Autónomos.

Software:

* Se utilizaron los Sistemas operativos Windows XP y Windows 7.
* Se utilizó un programa para acceder a la interfaz de línea de comando (CLI) del enrutador; el mismo es un software para la plataforma de Windows XP llamado Hyper Terminal.
* Se utilizó un Software de distribución libre para medir el ancho de banda de una red, denominado IPERF.
* Se usó un software de distribución libre, para la generación de tráfico y medición de los parámetros de la red, esta aplicación se denomina DITG (Distributed Internet Traffic Generator, en ingles) versión 2.6.1d para direccionamiento IPv4 e IPv6.
* Se usó el VLC VideoLAN para la transmisión de Video de un extremo a otro.
* Se usó el Wireshark para capturar los resultados de transmisión de Video.
* Paquetes estadístico SPSS v15 (Statistical Package of the Social Sciences, en inglés).

6.- Diseño del experimento

Esta fase se comenzó realizando pruebas con el programa IPERF para detectar el ancho de banda disponible desde una PC de un extremo a otra PC del otro extremo, arrojando como resultado óptimo 16.9Mbits/sec, tal como se puede apreciar en la Imagen N° 19.

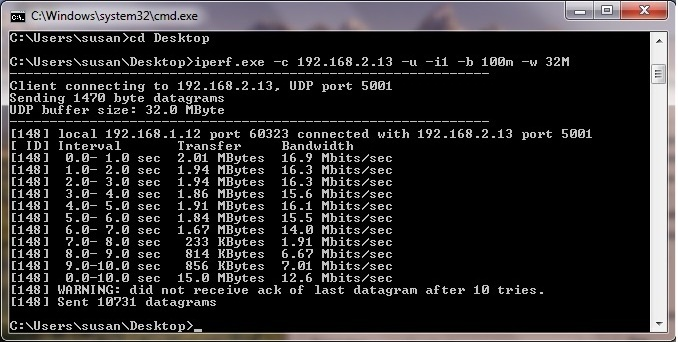


Imagen N° 19: Pruebas con IPERF para detectar el ancho de banda del ambiente

Fuente: Propia (2011)

Una vez conocido el ancho de banda disponible en el ambiente, y sabiendo que la QoS funcionaba sólo en caso de congestionamiento, se diseñaron tres tipos de Tráfico que se describen de la siguiente manera:

* Tráfico Datos: Este flujo de tráfico simula la transmisión de tráfico UDP, en las cuales se enviaron paquetes de tamaño 540 bytes, tamaño por defecto del programa DITG para representar una transmisión constante de datos.
* Tráfico Voz: Este flujo de tráfico también fue de UDP, en la cual se enviaron paquetes de tamaño 144 bytes, en el cual se utilizó el códec G.711 de flujo de voz con la técnica de codificación VAD (Propuesta por DITG).
* Tráfico Video: Este flujo de tráfico fue de RTP (Real Time Protocol, siglas en inglés), pero estos paquetes son de tamaño 1390 bytes para IPv6 y 1370 bytes para IPv4, estos valores fueron generados automáticamente por el VideoLAN y capturados por el Wireshark.

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

1. Tráfico Bajo:
   1. Datos: Se enviaron 200 paquetes por segundo durante 60 segundos, para un total de 12000 paquetes.
   2. Voz: Se enviaron 100 paquetes por segundo durante 60 segundos, para un total de 6000 paquetes.
   3. Video: Se enviaron 25874 paquetes.
2. Tráfico Medio:
   1. Datos: Se enviaron 2000 paquetes por segundo durante 60 segundos, para un total de 120000 paquetes.
   2. Voz: Se enviaron 500 paquetes por segundo durante 60 segundos, para un total de 30000 paquetes.
   3. Video: Se enviaron 25874 paquetes.
3. Tráfico Alto:
   1. Datos: Se enviaron 4000 paquetes por segundo durante 60 segundos, para un total de 240000 paquetes.
   2. Voz: Se enviaron 1000 paquetes por segundo durante 60 segundos, para un total de 60000 paquetes.
   3. Video: Se enviaron 25874 paquetes.

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

1. Condiciones de la red en IPv4 /IPv6 sin QoS enviando:

* Tráfico Bajo
* Tráfico Medio
* Tráfico Alto

1. Condiciones de la red en IPv4 / IPv6, con Calidad de Servicio y 55% del ancho de banda para Datos, 10% para el Video y 10% para la Voz, con envío de:

* Tráfico Bajo
* Tráfico Medio
* Tráfico Alto

1. Condiciones de la red en IPv4 / IPv6, con Calidad de Servicio y 10% del ancho de banda para Datos, 55% para el Video y 10% para la Voz, con envío de:

* Tráfico Bajo
* Tráfico Medio
* Tráfico Alto

1. Condiciones de la red en IPv4 / IPv6, con Calidad de Servicio y 10% del ancho de banda para Datos, 10% para el Video y 55% para la Voz, con envío de:

* Tráfico Bajo
* Tráfico Medio
* Tráfico Alto

Para la realización de las pruebas de los ambientes b, c y d, fue necesaria la configuración de QoS en el enrutador en base a:

* Clases de tráfico: encargadas de la clasificación de los distintos tráficos. Para este caso la clasificación se realizó mediante listas de acceso, como se muestra en la Imagen N° 20, se seleccionó el tráfico según protocolos, direcciones de origen o destino y puertos de origen o destino. Cada tipo de tráfico fue asociado con una clase. (Ver Imagen N° 21)

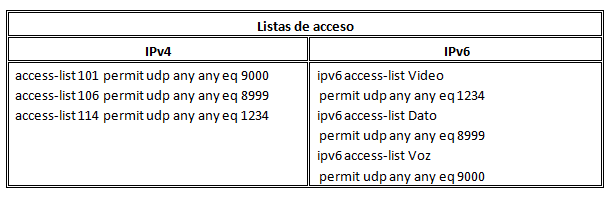


Imagen N° 20: Configuración de Listas de acceso de los protocolos IPv4 / IPv6

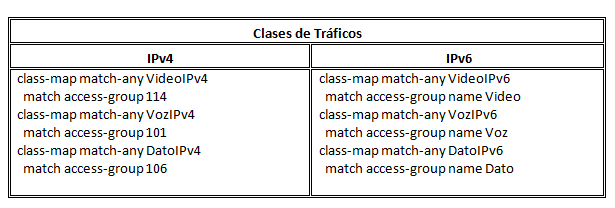
Fuente: Propia (2011)

Imagen N° 21: Configuración de Clases de Tráficos de los protocolos IPv4 / IPv6

Fuente: Propia (2011)

* Marcado: se basó en la información contenida en la cabecera de cada paquete. Para el marcado de los paquetes se utilizó el valor DSCP, el cual fue marcado con una determinada prioridad.
* Manejo de Congestión mediante Técnicas de Encolamiento: la técnica WFQ (Weighted Fair Queueing) permitió descartar paquetes cuando el tamaño de la cola excede los 64 paquetes, la misma fue colocada en la clase por defecto.
* Políticas de Tráfico: encargadas de asignar ciertas prioridades a los tráficos. En este caso, la prioridad se dio a través del porcentaje del ancho de banda el cual era de un 75% para el envío de tráfico, y un 25% para los protocolos que utilizan los enrutadores para negociar. (Ver Imagen N° 22)

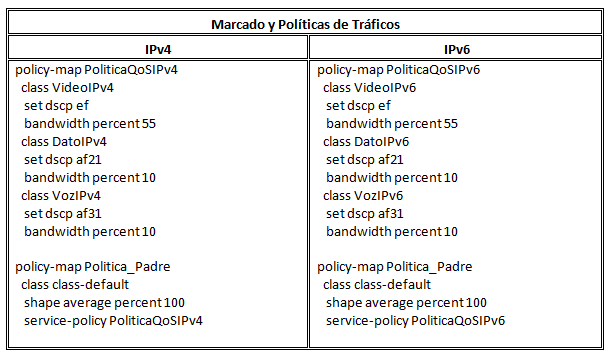


Imagen N° 22: Configuración de Marcado y Políticas de Tráficos en IPv4 / IPv6

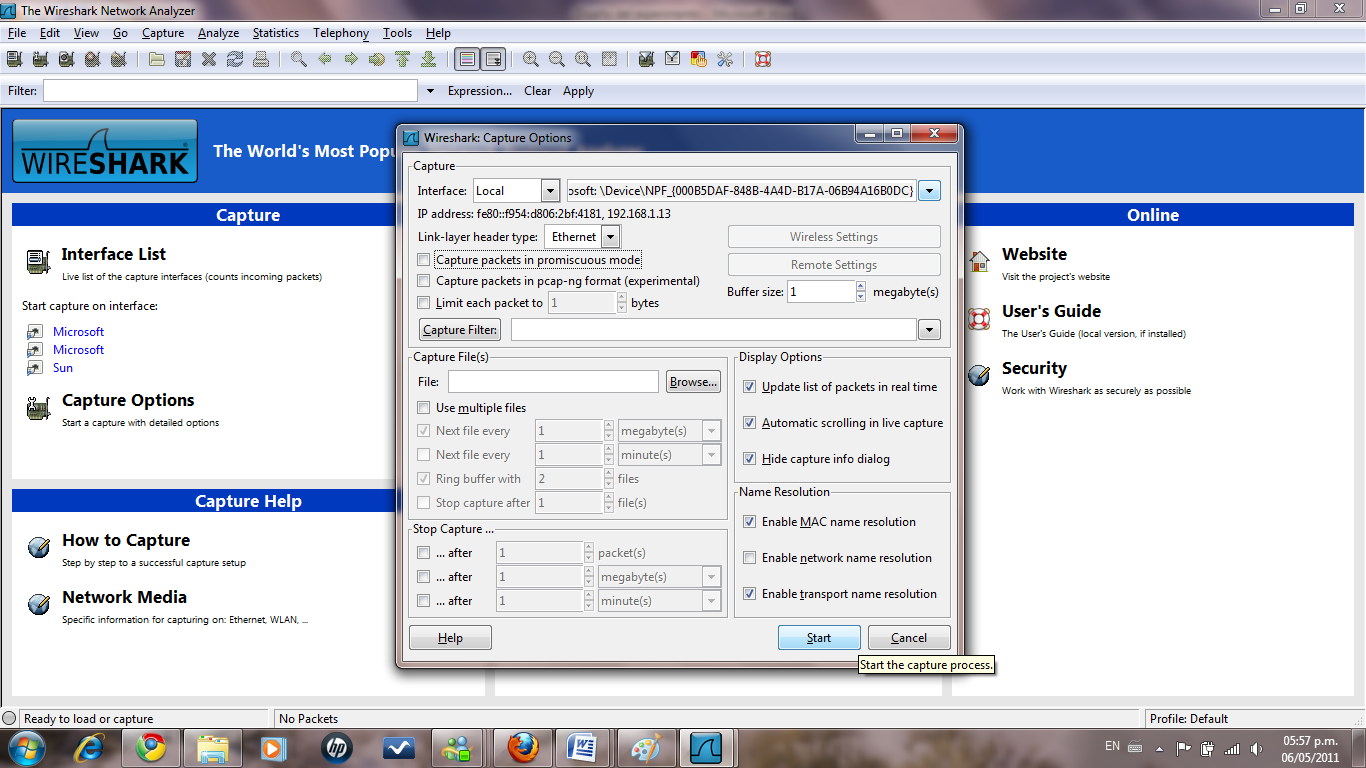
Fuente: Propia (2011)

Luego de realizar la configuración de QoS, se comprobó que las listas de acceso realizaran el filtrado apropiadamente. Esto se hizo enviando los tipos de tráfico uno por uno y mostrando, según el reporte del enrutador, los valores de la política aplicada a cada clase la cual estaba asociada con el tipo de tráfico.

Una vez terminada y probada la configuración de la QoS en los enrutadores, se dio inicio a las pruebas antes establecidas para llevar a cabo el experimento y se resumió en los siguientes pasos:

1.- Se verifican que todas las PCs estén operando de forma normal, con sus interfaces de red y los parámetros correctos.

2.- Se ejecuta Wireshark para iniciar la captura de transmisión tanto en las PC de origen como de destino. (Imagen N° 23). En esta investigación, el uso del Wireshark era necesario para obtener los distintos indicadores de QoS (% Paquetes Perdidos, Delay, Jitter y Bitrate) debido a que el VideoLAN no provee estos mismos valores. Además aplicó los filtros de paquetes para que mostraran solamente de Video, para esto, se colocó las direcciones IP de origen y destino y el puerto de destino (Imagen N° 24).

 Imagen N° 23: Captura de Transmisión por medio del Wireshark ver. 1.4.4

Fuente: Wireshark (2011)

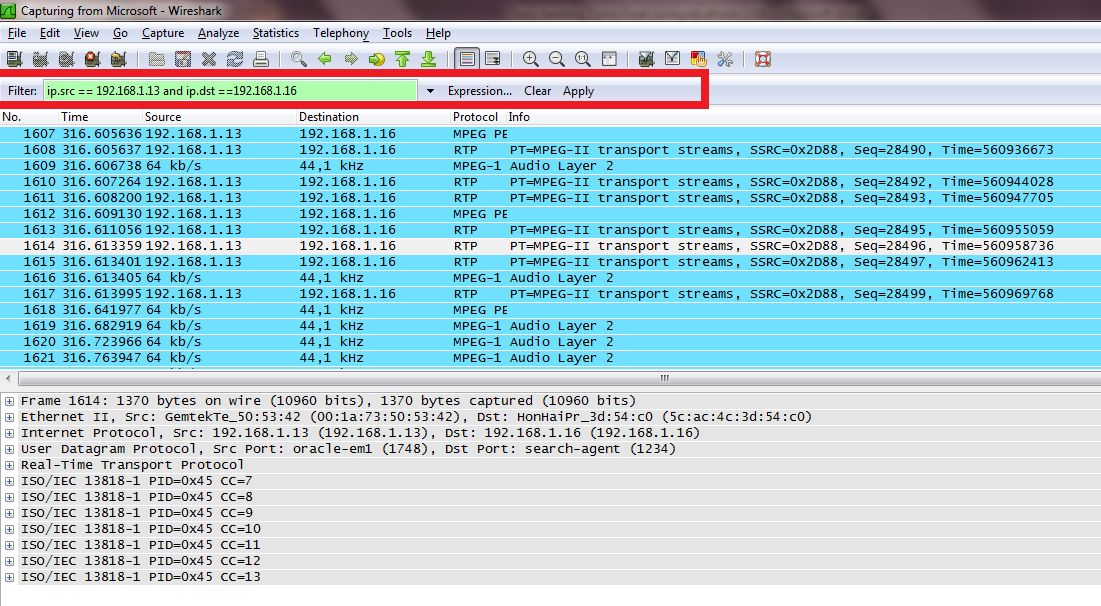


Imagen N° 24: Aplicación de Filtros en Wireshark ver. 1.4.4

Fuente: Wireshark (2011)

3.- Se ejecutan VideoLAN en las ambas PC. Se configura la PC de destino para dejar esperando la transmisión de video (Imagen N° 25), escribiendo la URL: **rtp://@[Direccion\_Destino]:Puerto\_Destino**

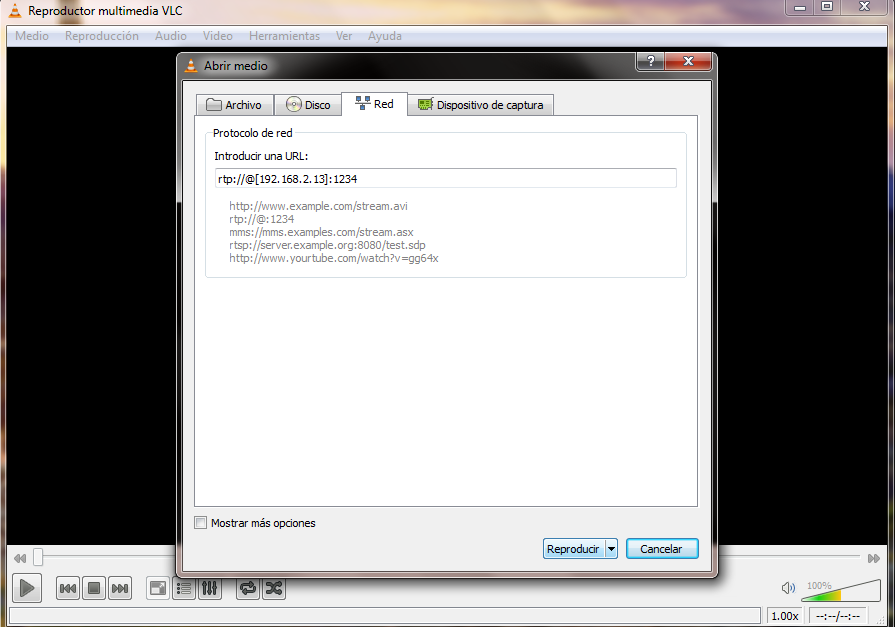


Imagen N° 25: Configuración de VideoLAN en la PC de Destino.

Fuente: VideoLAN (2011)

En la PC de origen se configura para transmitir el video. (Imagen N° 26).

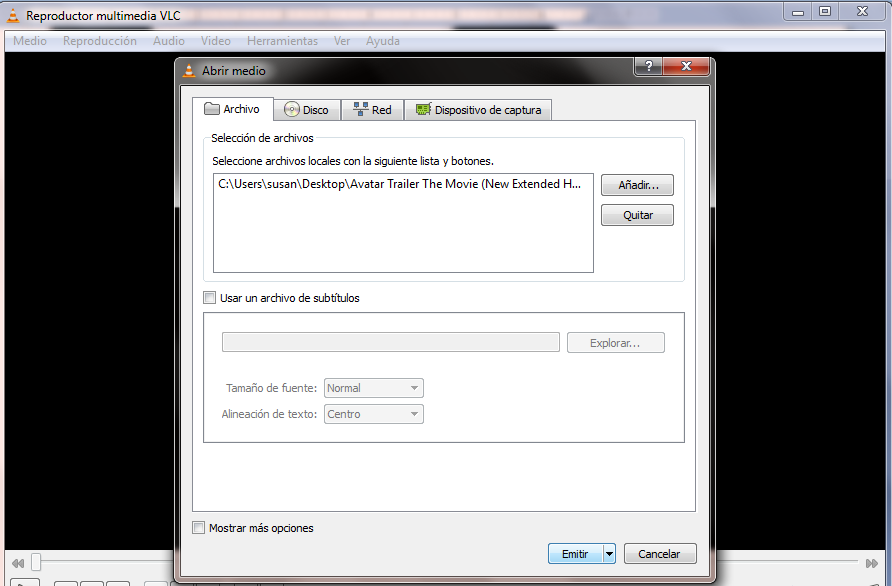


Imagen N° 26: Comienzo de la emisión de Video.

Fuente: VideoLAN (2011)

Luego, avanza hasta que llega a la pestaña OPCIONES y selecciona el protocolo RTP para emitir (Imagen N° 27), posteriormente le da a AÑADIR para colocar la dirección y el puerto de PC Destino (Imagen N° 28) y continúa en SIGUIENTE.

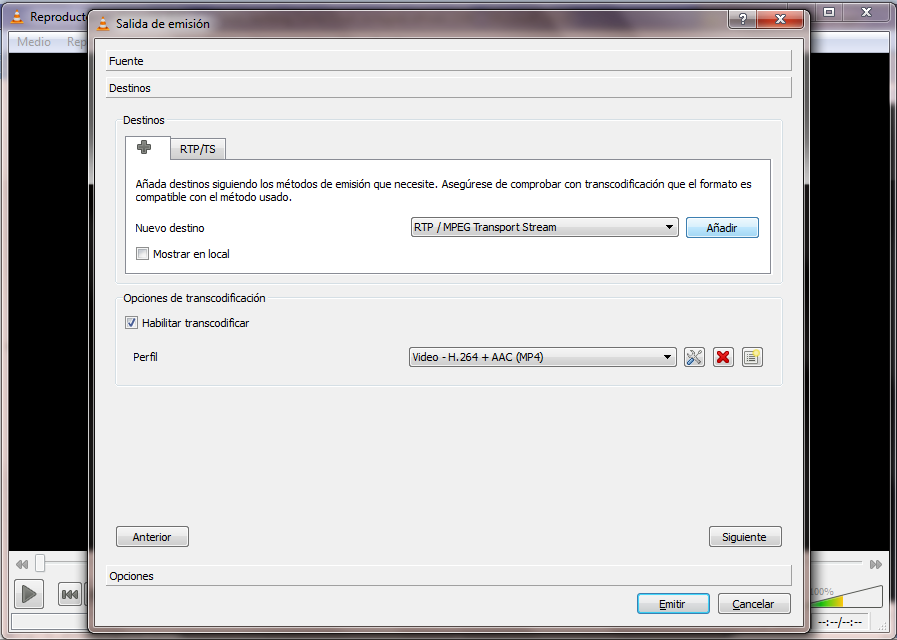


Imagen N° 27: Elección del protocolo RTP.

Fuente: VideoLAN (2011)

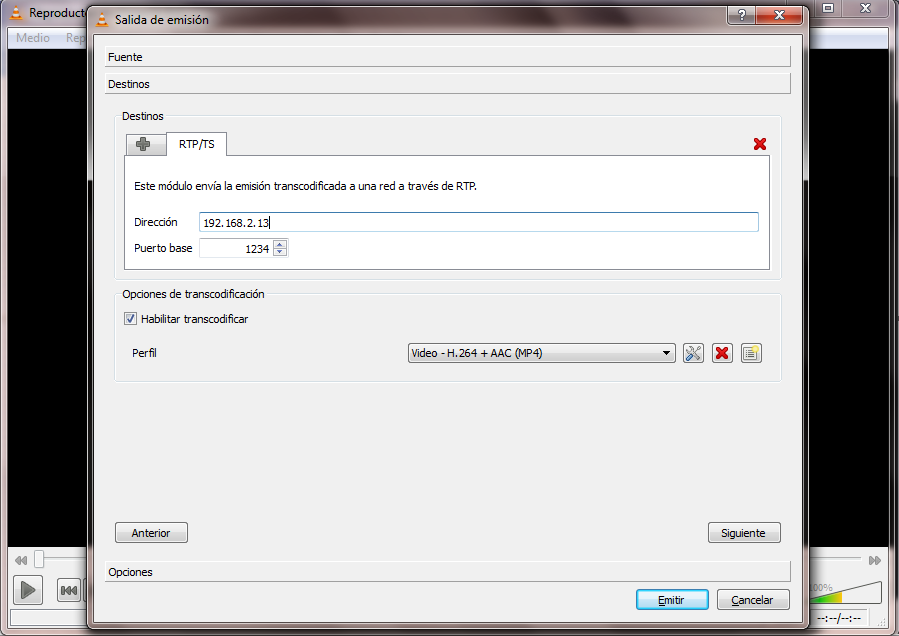


Imagen N° 28: Configuración de Dirección y Puerto de Destino.

Fuente: VideoLAN (2011)

Finalmente, presiona el botón EMITIR para iniciar la transmisión de Video. (Imagen N° 29)

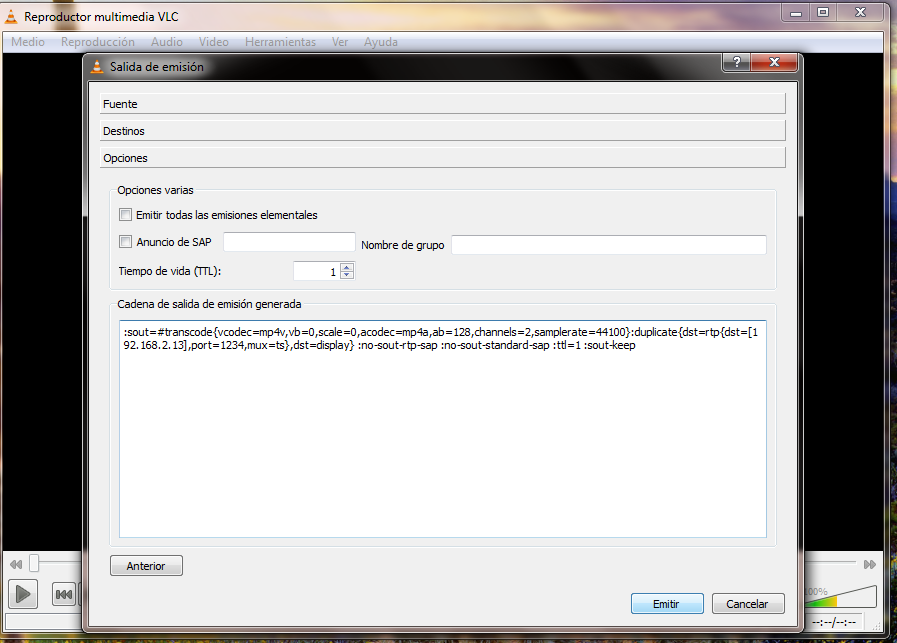


Imagen N° 29: Último paso para iniciar la transmisión.

Fuente: VideoLAN (2011)

4.- Se ejecutan DITG en ambas PCs. Se activa en la PC de destino el botón Receiver para recibir transmisiones de Datos y Voz (Imagen N° 30). Y en la PC de Origen se configura para transmitir el tráfico de Datos y de Voz y activa el botón Sender para iniciar la transmisión. (Imagen N° 31).

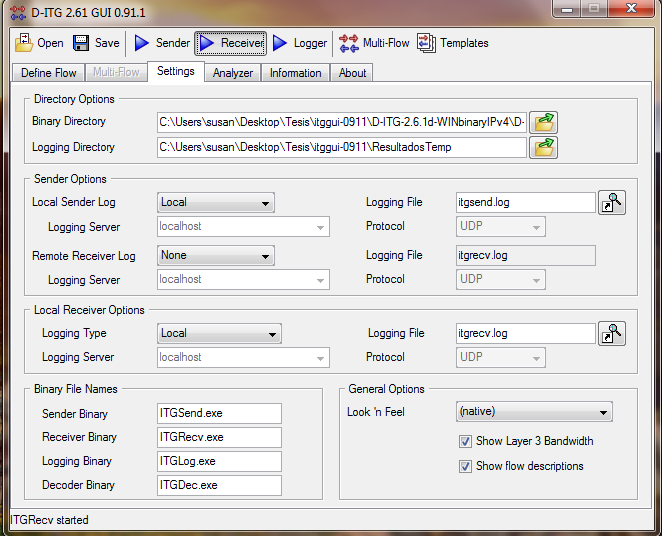


Imagen N° 30: Configuración de DITG en la PC de Destino en espera de transmisión.

Fuente: DITG (2011)

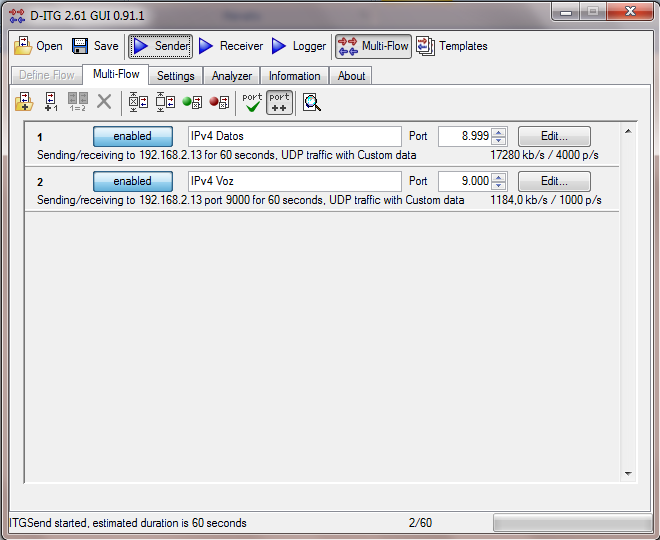


Imagen N° 31: Configuración de DITG en la PC de Origen para iniciar la transmisión.

Fuente: DITG (2011)

5.- Se empiezan a transmitir simultáneamente el tráfico de video por VideoLAN y los tráficos de Datos y Voz por DITG.

6.- Finalizado el tiempo de duración de la transmisión, se procede a detener la transmisión de video en VideoLAN y la captura de paquetes en DITG. (Imagen N° 32)

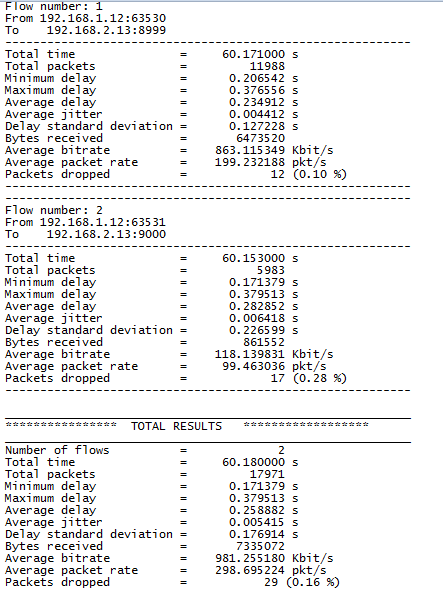


Imagen N° 32: Ejemplo de captura de resultados de DITG para Datos y Voz.

Fuente: DITG (2011)

7.- Para capturar los resultados de transmisión de Video, se utilizó el programa Wireshark. Para obtener el valor de Bitrate, se usó la opción Menu Statistics>Wireshark Protocol Hierarchy Statistics e identificó el flujo correspondiente a Video (Imagen N° 33).

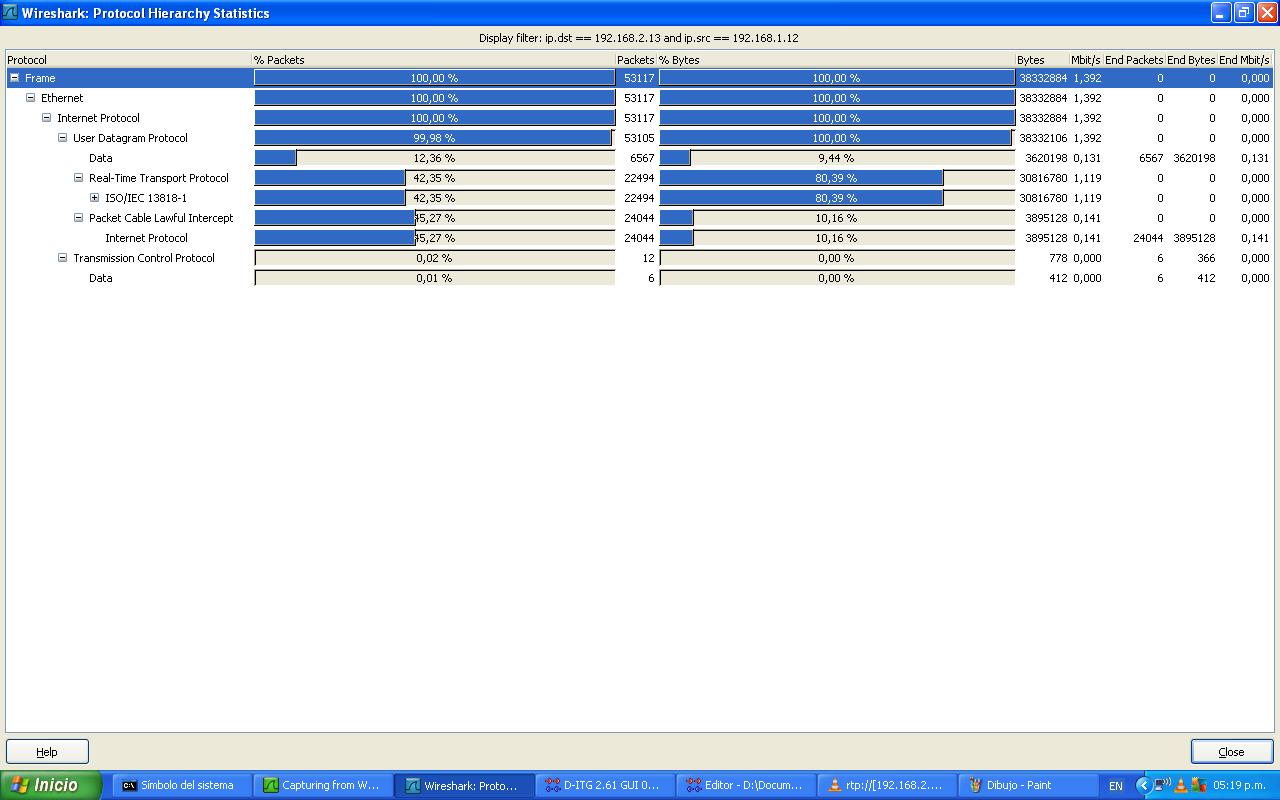


Imagen N° 33: Ejemplo de captura de Bitrate en Wireshark.

Fuente: Wireshark (2011)

Para conseguir los otros valores de QoS, se tuvo que decodificar los paquetes de Video en paquetes de Protocolo RTP para poder aplicar el analizador de flujo RTP de Wireshark.

Para lograr esto, se selecciona un paquete de Video del flujo capturado y activó la opción (Menu Analyze>Decode as) y escoge el protocolo a convertir RTP. (Imagen N° 34).

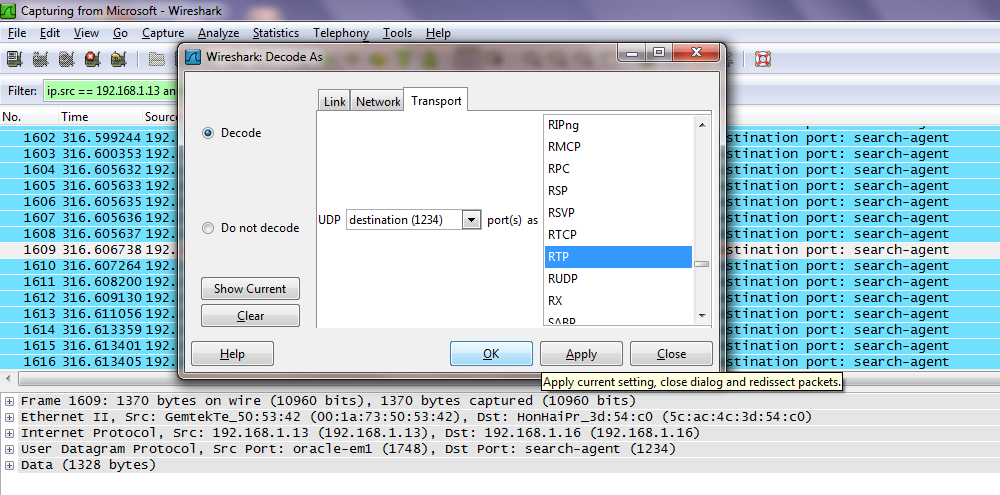


Imagen N° 34: Decodificación en Protocolo RTP de paquetes en Wireshark.

Fuente: Wireshark (2011)

A continuación, se utiliza el analizador RTP (Menu Telephony>RTP>Stream Analysis) para que mostraran el Delay y Jitter de cada paquete, y el porcentaje de paquetes perdidos de toda la transmisión (Imagen N° 35).

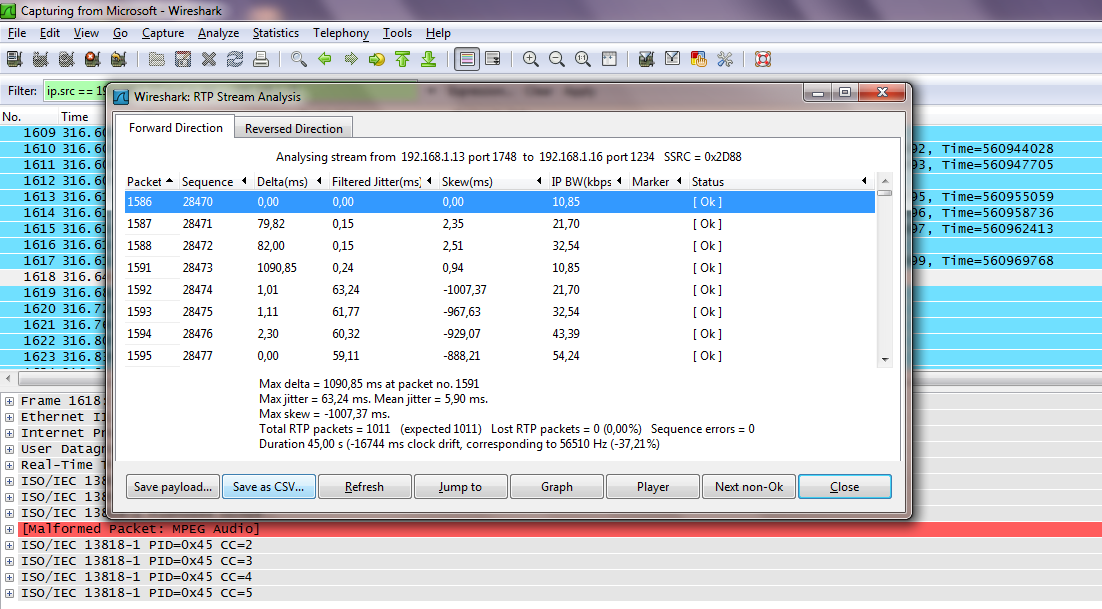


Imagen N° 35: Analizador de Flujo RTP en Wireshark.

Fuente: Wireshark (2011)

Luego, se exporta todo el flujo hacia un archivo .CSV donde posteriormente se calcula el Delay y Jitter promedio (Se calculó mediante Excel, Imagen N° 36).

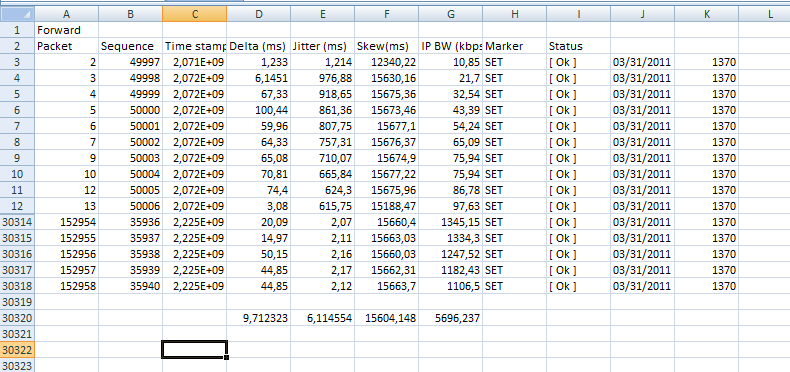


Imagen N° 36: Ejemplo de cálculo de delay y jitter usando Excel.

Fuente: Propia

8.- Luego, se procede a guardar los valores obtenidos como (% de Paquetes Perdidos, Delay, Jitter y Bitrate) de cada flujo (Datos y Voz por DITG, Video por Wireshark) con los tres (3) tipos de tráficos (Bajo, Medio y Alto) en los cuatros tipos de ambientes de Pruebas (**A.-** Sin QoS; **B.-** QoS 55% Dato 10% Video 10% Voz; **C.-** QoS 10% Dato 55% Video 10% Voz; y **D.-** QoS 10% Dato 10% Video 55% Voz). 12 Tablas en total.

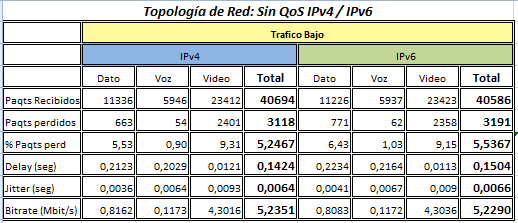


Tabla N° 1: Ejemplo de Consolidación de datos obtenidos de IPv4/IPv6 sin QoS Tráfico Bajo.

Fuente: Propia (2011).

9.- Finalmente, se resumen todas las tablas creadas en el Paso 8 utilizando las columnas “TOTAL” de ambos protocolos IP, en 4 tablas categorizadas por los indicadores de QoS (% de Paquetes Perdidos, (% de Paquetes Perdidos, Delay, Jitter y Bitrate). Estas tablas fueron utilizadas para generar los gráficos del esquema comparativo entre IPv4 e IPv6, de igual manera fueron introducidos posteriormente en el Programa estadístico SPSS para el análisis de la significancia de las diferencias observadas entre estos dos protocolos.

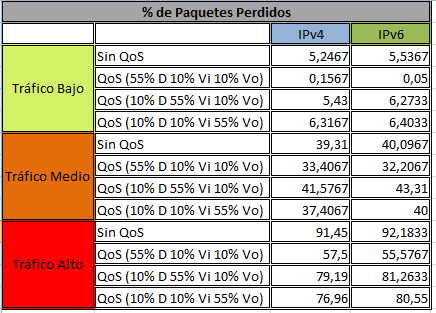


Tabla N° 2: Ejemplo de Resumen de Tablas categorizadas por los indicadores de QoS.

Fuente: Propia (2011).

Se aplicó el siguiente modelo estadístico: La variable independiente está conformada por cada Protocolo (IPv4 e IPv6), y las variables dependientes las integran el rendimiento de la red (% de Paq. Perdidos, Delay, Jitter, Bitrate).

El modelo estadístico utilizado es: *yij = µ + αi – εij*

*i=1,…,n j=1,…,m* Donde:

*n* es el número de repeticiones y m el número de casos

*y* = var dependiente: % de Paq. Perdidos, Delay, Jitter, Bitrate

*µ* = media del caso

*α* = var independiente: los dos protocolos (IPv4 e IPv6)

*εij* = error experimental

**CAPÍTULO IV**

**CAPÍTULO IV**

**ANALISIS Y DISCUSION DE LOS RESULTADOS**

1.- Análisis y descripción de los resultados

A continuación se describen y analizan los resultados obtenidos a partir de los ambientes y las pruebas descritas en el capitulo anterior, los cuales se resumen en cuatro (4) tablas categorizadas por Indicadores de QoS:

* **% de Paquetes Perdidos:**

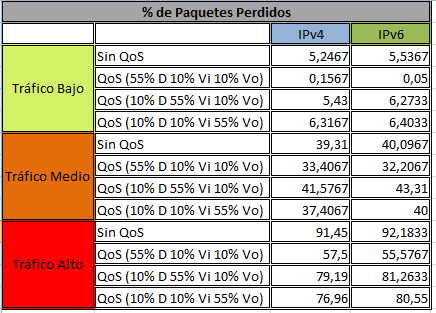
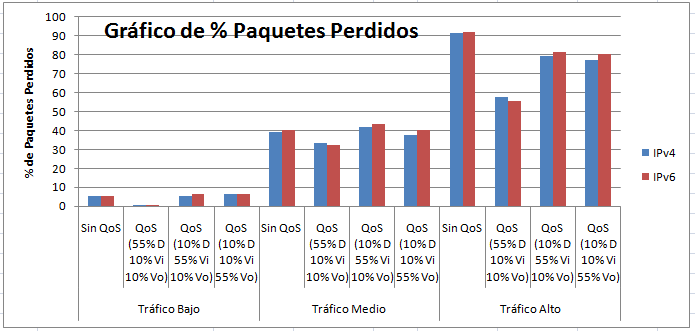


Tabla N° 3: Tabla de Resultados Totales del Porcentaje (%) de Paquetes Perdidos.

Fuente: Propia (2011).

Gráfica N° 1: Gráfico de Porcentaje de Paquetes Perdidos.

Fuente: Propia (2011).

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

* **Delay (Latencia):**

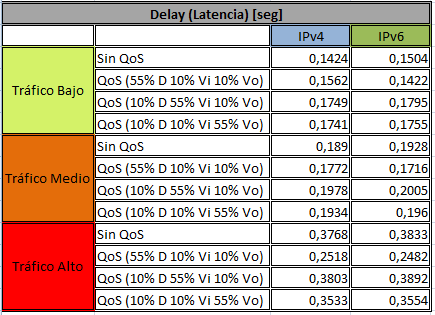
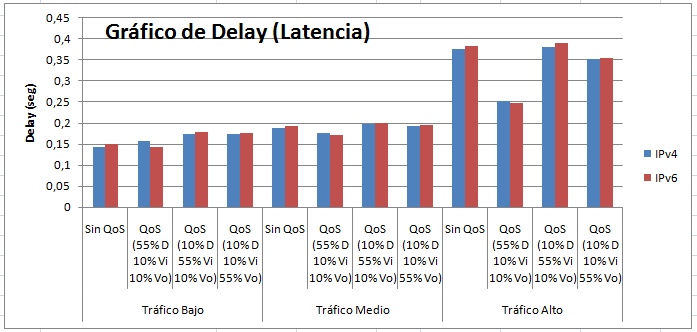


Tabla N° 4: Tabla de Resultados Totales en Delay (Latencia).

Fuente: Propia (2011).



Gráfica N° 2: Gráfico de Delay (Latencia).

Fuente: Propia (2011).

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

* **Jitter:**

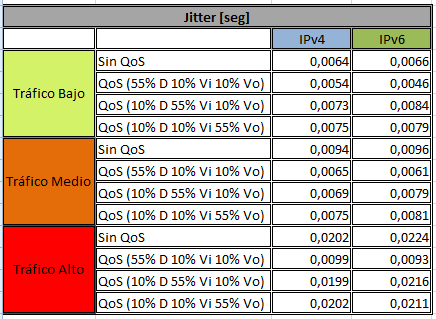
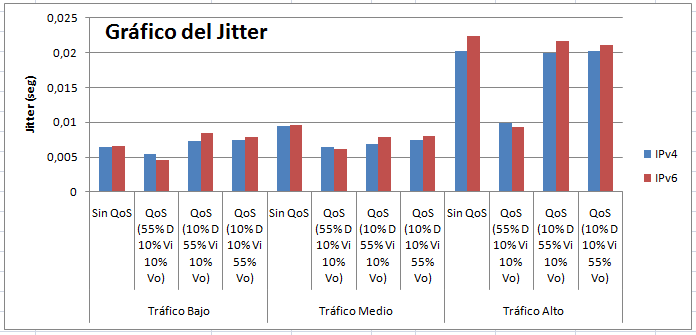


Tabla N° 5: Tabla de Resultados Totales en Jitter.

Fuente: Propia (2011).



Gráfica N° 3: Gráfico del Jitter.

Fuente: Propia (2011).

En este indicador, se hizo notar la mejora de IPv4 con respecto al IPv6 en la mayoría de los ambientes aunque sólo fue de baja proporción. No obstante, el IPv6 tuvo un contraste en los ambientes de QoS con la mayor prioridad de ancho de banda asignada en el flujo de DATOS, sobresaliendo con una pequeña ventaja frente al IPv4.

* **Bitrate:**

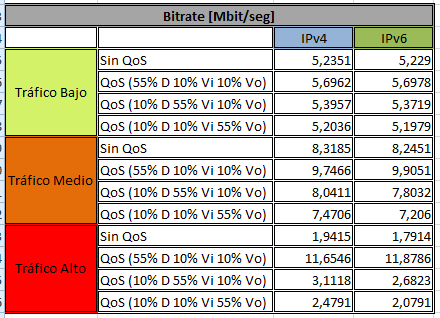


Tabla N° 6: Tabla de Resultados Totales en Bitrate.

Fuente: Propia (2011).

Gráfica N° 4: Gráfico del Bitrate.

Fuente: Propia (2011).

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

**2.- Sustentación Teórica de los Resultados:**

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

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

Así mismo, se comprueba que *“Cuanto más lejanos los dos radios, más pequeña la señal recibida debido a la pérdida en el espacio libre. Esto es independiente del medio ambiente, se debe solamente a la distancia. Esta pérdida se da porque la energía de la señal radiada se expande en función de la distancia desde el transmisor.”* (Flickenger, 2006)

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

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

**2.- Análisis estadístico de los resultados**

Para realizar el análisis estadístico se utilizó el procedimiento “Análisis of Variance" ANOVA de un factor. Según Massart y col (1997), este funciona para comparar si los valores de un conjunto de datos numéricos son significativamente distintos o no, a los valores de otro o más conjuntos de datos. El procedimiento para comparar estos valores está basado en la varianza global observada en los grupos de datos numéricos a comparar.

Asimismo ANOVA permite comparar dos o más medias poblacionales, partiendo de la hipótesis nula de que todas las medias son iguales y teniendo como hipótesis alternativa de que por lo menos una media es diferente.

Como el propósito de esta investigación fue comparar los resultados obtenidos entre IPv4 e IPv6, entonces el número de grupos a comparar es solamente de dos (2). Y según (Vallejo, 2011*), “Normalmente cuando tenemos dos muestras independientes utilizamos el contraste de medias (t de Student), pero podemos utilizar igualmente el análisis de varianza con idénticos resultados. En el caso de dos muestras independientes tenemos que t = √F; con ambos procedimientos llegamos a los mismos resultados y a las mismas conclusiones.”*

Por lo tanto, el tratamiento Post ANOVA llamado TUKEY no hizo falta en este proyecto, ya que según (Barón y col, 2008), el TUKEY se considera como una técnica de comparaciones múltiples y a la vez de rangos. Es un test que se suele utilizar cuando se quiere comparar cada grupo con todos los demás de par en par y el número de grupos es alto (6 o más), y partiendo del hecho de que la hipótesis nula arrojada por ANOVA es rechazada. Dicho esto, el análisis resultante del procedimiento ANOVA es suficiente para demostrar si las diferencias entre dos conjuntos de datos fueron significativas o no.

El valor estadístico F calculado (Fcal) arrojado por ANOVA nos indica que tan parecido son las medias que se están comparando. Si la significancia (Sig) asociada al valor estadístico F es menor al máximo o peor coeficiente de significancia (CoefS) 0.05, los resultados son significativos. Si el valor de Fcal es menor al valor de F tabulado (Ftab[[5]](#footnote-6))= 7,71 se acepta la hipótesis nula; de lo contrario se rechaza y se acepta la hipótesis alternativa, así se confirma que los grupos comparados difieren en sus medias. (Massart ,1997).

Gráficamente, se puede interpretar la aceptación de la Hipótesis Nula cuando la probabilidad de que existe tal valor esté fuera de la región sombreada α del Coeficiente de Significancia que este caso se asumió el peor de todos (0,05). De lo contrario, se rechaza la Hipótesis Nula y acepta la Hipótesis Alternativa. Se puede observar este comportamiento en el Anexo N° 2.

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

**- Porcentaje (%) de Paquetes Perdidos:**

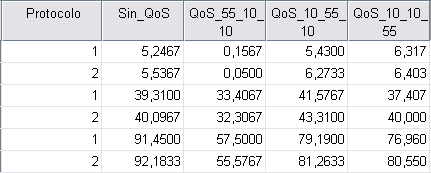


Tabla N° 7: Tabla de Valores de Porcentaje de Paquetes Perdidos en SPSS.

Protocolo 1: Protocolo IPv4; Protocolo 2: Protocolo IPv6.

Fuente: Propia

| **ANOVA** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | Sum of Squares | Df | Mean Square | F | Sig. |
| Sin\_QoS | Between Groups | ,546 | 1 | ,546 | ,000 | ,987 |
| Within Groups | 7574,979 | 4 | 1893,745 |  |  |
| Total | 7575,525 | 5 |  |  |  |
| QoS\_55\_10\_10 | Between Groups | 1,633 | 1 | 1,633 | ,002 | ,966 |
| Within Groups | 3213,169 | 4 | 803,292 |  |  |
| Total | 3214,801 | 5 |  |  |  |
| QoS\_10\_55\_10 | Between Groups | 3,604 | 1 | 3,604 | ,003 | ,962 |
| Within Groups | 5532,517 | 4 | 1383,129 |  |  |
| Total | 5536,121 | 5 |  |  |  |
| QoS\_10\_10\_55 | Between Groups | 6,552 | 1 | 6,552 | ,005 | ,947 |
| Within Groups | 5264,100 | 4 | 1316,025 |  |  |
| Total | 5270,652 | 5 |  |  |  |

Tabla N° 8: Tabla ANOVA del Porcentaje de Paquetes Perdidos.

Fuente: Propia

De la tabla N ° 14 se observa lo siguiente:

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

**- Delay (Latencia):**

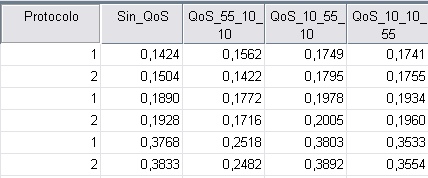


Tabla N° 9: Tabla de Valores de Delay.

Protocolo 1: Protocolo IPv4; Protocolo 2: Protocolo IPv6.

Fuente: Propia

| **ANOVA** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | Sum of Squares | Df | Mean Square | F | Sig. |
| Sin\_QoS | Between Groups | ,000 | 1 | ,000 | ,004 | ,955 |
| Within Groups | ,062 | 4 | ,015 |  |  |
| Total | ,062 | 5 |  |  |  |
| QoS\_55\_10\_10 | Between Groups | ,000 | 1 | ,000 | ,033 | ,866 |
| Within Groups | ,011 | 4 | ,003 |  |  |
| Total | ,011 | 5 |  |  |  |
| QoS\_10\_55\_10 | Between Groups | ,000 | 1 | ,000 | ,003 | ,957 |
| Within Groups | ,052 | 4 | ,013 |  |  |
| Total | ,052 | 5 |  |  |  |
| QoS\_10\_10\_55 | Between Groups | ,000 | 1 | ,000 | ,001 | ,981 |
| Within Groups | ,039 | 4 | ,010 |  |  |
| Total | ,039 | 5 |  |  |  |

Tabla N° 10: Tabla ANOVA del Delay.

Fuente: Propia

De la tabla N ° 16 se observa lo siguiente:

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

**- Jitter:**

****

Tabla N° 11: Tabla de Valores del Jitter.

Protocolo 1: Protocolo IPv4; Protocolo 2: Protocolo IPv6.

Fuente: Propia

| **ANOVA** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | Sum of Squares | Df | Mean Square | F | Sig. |
| Sin\_QoS | Between Groups | ,000 | 1 | ,000 | ,018 | ,899 |
| Within Groups | ,000 | 4 | ,000 |  |  |
| Total | ,000 | 5 |  |  |  |
| QoS\_55\_10\_10 | Between Groups | ,000 | 1 | ,000 | ,096 | ,772 |
| Within Groups | ,000 | 4 | ,000 |  |  |
| Total | ,000 | 5 |  |  |  |
| QoS\_10\_55\_10 | Between Groups | ,000 | 1 | ,000 | ,042 | ,848 |
| Within Groups | ,000 | 4 | ,000 |  |  |
| Total | ,000 | 5 |  |  |  |
| QoS\_10\_10\_55 | Between Groups | ,000 | 1 | ,000 | ,011 | ,922 |
| Within Groups | ,000 | 4 | ,000 |  |  |
| Total | ,000 | 5 |  |  |  |

Tabla N° 12: Tabla ANOVA del Jitter.

Fuente: Propia

De la tabla N ° 18 se observa lo siguiente:

En este ámbito, se pudo observar un comportamiento muy similar a los dos indicadores anteriores: en todos los ambientes a realizar, el F arrojado por ANOVA es mucho menor que el Ftab (7,71) y además la significancia (Sig) asociada en la tabla ANOVA también es mucho mayor que el coeficiente de significancia (0,05). Por lo que se pudo concluir que no hubo diferencias significativas entre IPv4 e IPv6 en esta categoría.

**- Bitrate:**

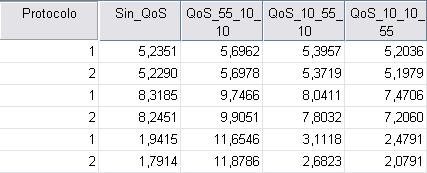


Tabla N° 13: Tabla de Valores del Bitrate.

Protocolo 1: Protocolo IPv4; Protocolo 2: Protocolo IPv6.

Fuente: Propia

| **ANOVA** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | Sum of Squares | Df | Mean Square | F | Sig. |
| Sin\_QoS | Between Groups | ,009 | 1 | ,009 | ,001 | ,978 |
| Within Groups | 41,195 | 4 | 10,299 |  |  |
| Total | 41,204 | 5 |  |  |  |
| QoS\_55\_10\_10 | Between Groups | ,025 | 1 | ,025 | ,003 | ,962 |
| Within Groups | 38,449 | 4 | 9,612 |  |  |
| Total | 38,474 | 5 |  |  |  |
| QoS\_10\_55\_10 | Between Groups | ,080 | 1 | ,080 | ,013 | ,916 |
| Within Groups | 25,294 | 4 | 6,323 |  |  |
| Total | 25,373 | 5 |  |  |  |
| QoS\_10\_10\_55 | Between Groups | ,075 | 1 | ,075 | ,012 | ,919 |
| Within Groups | 25,841 | 4 | 6,460 |  |  |
| Total | 25,915 | 5 |  |  |  |

Tabla N° 14: Tabla ANOVA del Bitrate.

Fuente: Propia

De la tabla N ° 20 se observa lo siguiente:

En esta indicador, se pudo observar un comportamiento equivalente a los todos indicadores anteriores: en todos los ambientes a realizar, el F arrojado por ANOVA es mucho menor que el Ftab (7,71) y además la significancia (Sig) asociada en la tabla ANOVA también es mucho mayor que el coeficiente de significancia (0,05). Por lo que se pudo afirmar que no hubo diferencias significativas entre IPv4 e IPv6 en este contorno.

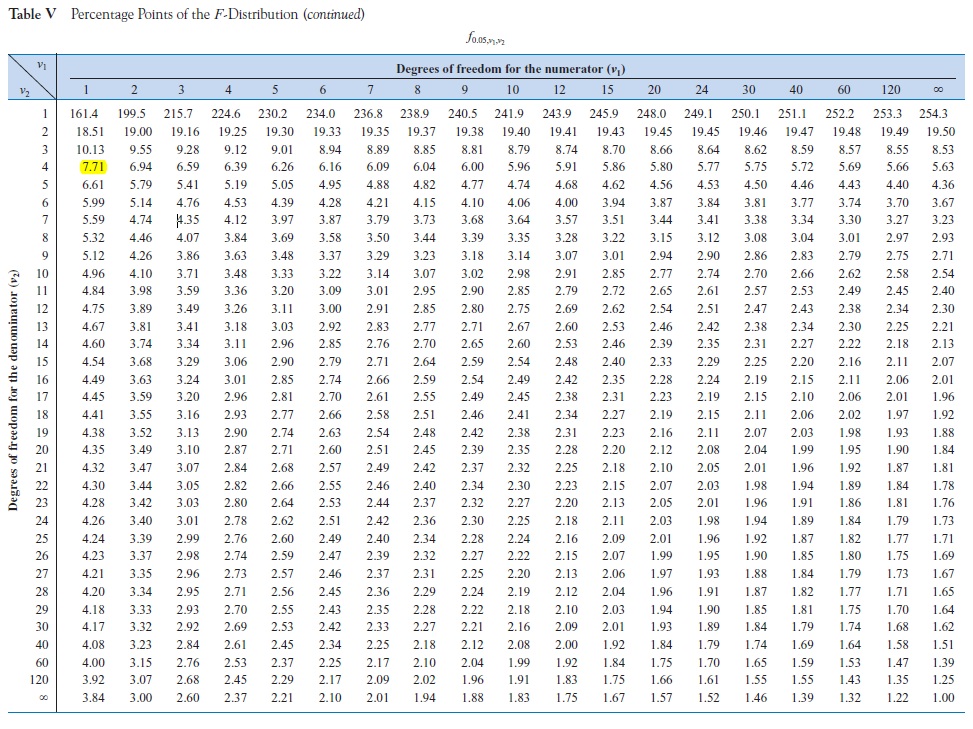
**CONCLUSIONES**

1. Cuando se establecen políticas de calidad de servicio donde la mayor prioridad es para tráficos que no son de tiempo real, IPv6 tiende a comportarse mejor que IPv4 observándose por medio de los gráficos en el Capítulo IV, aún cuando no es significativo estadísticamente. Esto se debe a los resultados arrojados por ANOVA, las cuales demostraron la aceptación de la Hipótesis Nula de que la media de los dos conjuntos de datos (IPv4 e IPv6) es igual.
2. El uso de una cabecera más grande en IPv6, influye en el aumento de los retardos y disminución del bitrate, debido al tiempo de procesamiento de los paquetes en los dispositivos activos como enrutadores, switches y Access Points.
3. La utilización del protocolo IPv6 en ambientes de producción con QoS similares a los utilizados en esta investigación, no influye significativamente en el desempeño de la red respecto a entornos IPv4 con las mismas características usadas, en cuanto a jitter, delay, porcentaje de paquetes perdidos y bitrate se refieren.
4. A pesar de que IPv6 presenta en general un menor desempeño frente a IPv4, esta diferencia puede considerarse no significativa, IPv6 aun está en su etapa de madurez, ya que IPv6 es un protocolo que fue construido en base a la experiencia obtenida con IPv4. Por lo tanto, puede concluirse que su uso no altera de manera significativa el desempeño de Sistemas Autónomos conectados por enlace inalámbrico a 5.7 GHz.
5. En vista de que las diferencias de rendimiento entre los protocolos IPv4 e IPv6 en este entorno de Sistemas Autónomos conectados por el enlace inalámbrico a 5.7 Ghz no fueron significativas, se puede concluir que este enlace inalámbrico fue estable bajo este ambiente de prueba.
6. El hecho de utilizar enlaces de 5.7 GHz genera una pérdida de paquetes superior a otros enlaces de otras frecuencias y enlaces cableados, debido al factor distancia, donde la pérdida de espacio libre puede aumentar, ya que la potencia de la señal tiende a disminuir. Por tanto, el estudio de las condiciones de los enlaces inalámbricos entre sistemas autónomos, es un factor determinante dada la envergadura de los sistemas a interconectar.

**RECOMENDACIONES**

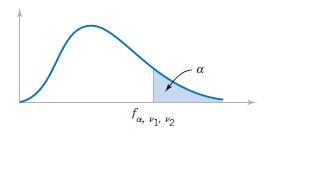
1. Implementar otros tipos de QoS, tal como la utilización de la estructura de servicios integrados, o continuar indagando en la manera de clasificar diferentes tipos de tráficos, o la utilización de otros parámetros que permitan aplicar prioridades a los distintos tráficos.
2. Por motivo de limitaciones de espacio físico en el laboratorio de pruebas, se conectaron las antenas Ubiquiti a una distancia de menos de 10 metros, lo cual es lejos de ser un trayecto de Conexión entre Sistemas Autónomos. Por este motivo, se recomienda en lo posible realizar pruebas con una distancia más cercana a lo real.
3. Implementar ambientes nativos IPv6 para afianzar los resultados obtenidos.
4. Incrementar el número de clientes inalámbricos y enrutadores para investigaciones con topologías similares.
5. Implementar otros estándares inalámbricos (802.11n por ejemplo) en investigaciones sobre QoS.

**ANEXOS**

****

Anexo N° 1: Tabla de Distribución F de Fisher con 0,05% de Coeficiente de Confianza.

Fuente: Montgomery (2002)



Anexo N° 2: Intervalo de Coeficiente de Confianza α.

Fuente: Montgomery (2002)

**Índice de Referencias**

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

**Arias, F. 1999. El proyecto de investigación: Guía para su elaboración. Caracas, Venezuela: Episteme.**

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

Barón López F.J., Téllez Montiel F, 2008. **Apuntes de Bioestadística**. [En Línea]: <http://www.bioestadistica.uma.es/baron/apuntes/ficheros/cap05.pdf>

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

Castro, Liliana. 2009. **Calidad de servicio de una WAN complementada con tecnología inalámbrica y el protocolo de Internet versión 6.** Proyecto de Trabajo Especial de Grado presentado para optar al título de Licenciada en Computación - La Universidad del Zulia. Edo. Zulia. Venezuela.

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

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

Cisco, 2007. **Cisco Networking Academy.** [En línea]. Disponible en: [http://cisco.netacad.net/cnams/course/CourseMaterial.jsp?.](http://cisco.netacad.net/cnams/course/CourseMaterial.jsp?.ç)

Danysoft, 2006. **Protocolo de Reservación de Recursos: RSVP.** [On-Line]. Dirección URL:  <http://www.danysoft.com/free/reservarecursos.pdf>

Da Ros Silvano, 2006. **Networking Fundamentals.** [On-Line]. Dirección URL: <http://www.ciscopress.com/bookstore/product.asp?isbn=1587052911>

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

Dye Mark, McDonald Rick, Rufi Antoon, 2007**. Network Fundamentals.** [On-Line]. Dirección URL: <http://www.ciscopress.com/bookstore/product.asp?isbn=1587132087>

Espina L, 2007. **Transmisión en redes ethernet bajo condiciones de interferencias generadas por campos electromagnéticos radiados**. Proyecto de trabajo presentado como requisito para optar al título de Licenciado en Computación, Universidad del Zulia, Venezuela.

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

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

Flickenger Rob, 2006. Creative Commons. **Redes Inalámbricas en los Países en Desarrollo.** Editorial Limehouse Book Sprint Team, 2007.

García J, 2002. **Redes de Comunicación: conceptos fundamentales y arquitecturas.** Madrid. Editorial: MC Graw Hill-Madrid. (P 443)

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

Granados Reyes Eduardo, 2010. **Transición de IPv4 a IPv6 en las Empresas.** [On-Line]. Dirección URL: <http://www.tlalpan.uvmnet.edu/oiid/download/Transici%C3%B3n%20IPV4-IPV6%20Gesti%C3%B3n_04_PO-ISC_PIT_E.pdf>

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

Hernández, R.; Fernández, C. y Baptista, P. (2003). **Metodología  
de la Investigación.** Caracas: McGrawHill. (p. 118)

Hurtado, Jorkey. 2009. **Medición de Calidad de Servicio bajo Protocolo BGP (Border Gateway Protocol) e IPv6 (Internet Protocol versión 6).** Proyecto de Trabajo Especial de Grado presentado para optar al título de Licenciado en Computación - La Universidad del Zulia. Edo. Zulia. Venezuela.

Julian-Bertomeu H., 2005. **Evaluación de los parámetros de QoS en entornos de Movilidad IP.** Tesis Doctoral presentada en la Universidad Politécnica de Cataluña, Barcelona.

Macías Esther, 2004. **IPv6, la transición necesaria.** [En línea]. Disponible en: <http://intechscialtda.com/IPv6/IPv6_computerworld_16012004.pdf>.

Majkowski J y Palacio F, 2003. **Calidad de servicio en WLAN considerando un escenario mixto IEEE 802.11e y IEEE 802.11b.** Investigación presentada en la Universidad Politécnica de Cataluña, Barcelona.

Massart D.L., B.M.G. Vandeginste, L.M.C. Buydens, S. de Jong, P.J. Lewi, J. Smeyers-Verbeke, **“Handbook of Chemometrics and Qualimetrics: Part A”,** Elsevier (1997), Amsterdam.

McQuerry Stephen, 2008. **Wireless LANs: Extending the Reach of a LAN.** [En línea]. Disponible en: <http://www.ciscopress.com/articles/article.asp?p=1156068&seqNum=4>

**Méndez, C. (2001). Metodología. Editorial McGraw-Hill Interamericana S.A, pp-155-160.**

## Mezquida C, 2004. (Página consultada el 13 de Mayo de 2009). [Diseño y optimización de una antena impresa para Wireless LAN.](http://www.carlosmezquida.com/word/2007/05/02/diseno-y-optimizacion-de-una-antena-impresa-para-wireless-lan/) Universidad Politécnica De Valencia - Gandia. Disponible en: <http://www.carlosmezquida.com/word/>.

Millán R, 2004. (Página consultada el 13 de Mayo de 2009). **Nueva** **estructura de direcciones en Internet, el protocolo ipv6**. [En línea]. Disponible en: <http://dialnet.unirioja.es/servlet/portadatesis>.

Montgomery, Douglas. 2002. **Applied Statistics and Probability for Engineers.** Third Edition. Editorial Limusa Wiley.

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

Odom Wendell, 2004. **Networking First-Step: How to Build a Local (Network) Roadway.** [On-Line]. Dirección URL:

<http://www.ciscopress.com/articles/article.asp?p=174105&seqNum=2>

Peralta L, 2002.(Página consultada el 13 de Mayo de 2009). **IPV6***.* [En Línea].Universidad Jaume I. España. Disponible en:<http://www.cu.ipv6tf.org/qos.htm>

Pezoa, Jorge. 2002. (Página consultada el 13 de Mayo de 2009). **Border Gateway Protocol (BGP).** [On-Line]. Dirección URL:

<http://cursos.die.udec.cl/~redes/apuntes/myapuntes/node178.html>

Raicu, I. y Zeadally, S. (2003). **Evaluating IPv6 on Windows and Solaris.** IEEE Computer Society. [En Línea]: <http://dx.doi.org/10.1109/MIC.2003.1200301>

Randall k. Nichols, Panos C. Lekkas, 2003. **Seguridad para comunicaciones inalámbricas.** Editorial: Mc GRAW HILL de España, S.A.U, pág. 357.

RFC1519. 1993. (Página consultada el 13 de Mayo de 2009). **RFC1519 - Classless Inter-Domain Routing (CIDR): an Address Ass.** [On-Line]. Dirección URL: <http://www.faqs.org/rfcs/rfc1519.html>

Roldan, Guillermo. 2008. (Página consultada el 24 de Julio de 2010). **Open Short Path First (OSPF).** [On-Line]. Dirección URL: <http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx>

Sendazo C, 2002. (Página consultada el 24 de Julio de 2010). **QoS** **y mecanismos de transición IPv4/IPv6.** Área de Ingeniería Telemática Universidad CARLOS III de Madrid. Disponible en: <http://www.it.uc3m.es/~fvalera/int_red/trabajos/>.

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

UMAN, 2004. (Página consultada el 24 de Julio de 2010). Universidad Nacional Autónoma de México. [En Línea]. Disponible en: <http://www.enterate.unam.mx/>.

Valarezo C, Iván R, 2006. **Autoconfiguración de direcciones stateless IPv6 y Enrutamiento dinámico en IPv6.** Universidad Técnica Particular de Loja. <http://www.utpl.edu.ec/telecomunicaciones/internetavanzado/index.php?btn=4>.

Valencia F, 2008. (Página consultada el 24 de Julio de 2010). **Cisco Certified Internetwork Expert.** [En Línea]. Disponible en: <http://francisco-valencia.es/Documentos/CCIE.pdf>.

Vallejo Pedro M, 2011. **Análisis de varianza para varias muestras independientes.** Universidad Pontificia Comillas, Madrid. [En Línea]. Disponible en: <http://www.upcomillas.es/personal/peter/analisisdevarianza/ANOVAIndependientes.pdf>

1. IBSS (Conjunto de Servicios Básicos Independientes). Red 802.11 formada por un conjunto de estaciones que se comunican entre sí, pero no con una infraestructura de red. [↑](#footnote-ref-2)
2. STA: abreviatura de Station (estación). Dispositivo de red básico. [↑](#footnote-ref-3)
3. BSS (Conjunto de servicios básicos): Grupo de dispositivos 802.11 conectados a un punto de acceso. [↑](#footnote-ref-4)
4. ARP (Protocolo de resolución de direcciones): Protocolo Internet que se usa para asignar una dirección IP a una dirección MAC. [↑](#footnote-ref-5)
5. Ftab.: Extraído de la tabla de distribución F, mediante los grados de libertad (gl) arrojados por ANOVA. Dicha tabla se muestra en el anexo N ° 1. [↑](#footnote-ref-6)