REPÚBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD DEL ZULIA

FACULTAD EXPERIMENTAL DE CIENCIAS

DIVISIÓN DE PROGRAMAS ESPECIALES

LICENCIATURA EN COMPUTACIÓN

**Influencia del protocolo IPv6 en redes basadas en MPLS (Multiprotocol Label Switching)**

Proyecto de Trabajo Especial de Grado presentado como requisito para optar   
al título de Licenciada en Computación

### Autor: Br. Angelis Meliana Carrasquero Urdaneta

Tutor**:** Msc.Alfredo Acurero

Maracaibo, Marzo de 2012

**Influencia del protocolo IPv6 en redes basadas en MPLS (Multiprotocol Label Switching)**

Angelis Carrasquero

C.I. No.: 20.280.333

Teléfono: 58-424-6959334

Urb. Las Amalias Calle 59 casa 78ª-144

Correo electrónico: angie\_88\_9@hotmail.com

Msc. Alfredo Acurero

C.I. No.: 9.783.996

Correo electrónico: [aacurero@gmail.com](mailto:aacurero@gmail.com)

Carrasquero Urdaneta, Angelis Meliana. “**Influencia del protocolo IPv6 en redes basadas en MPLS (Multiprotocol Label Switching).** Proyecto de Trabajo Especial de Grado. Universidad del Zulia. Facultad Experimental de Ciencias. División de Programas Especiales. Licenciatura en Computación. Maracaibo. Venezuela. 2012. 89 pág.

**RESUMEN**

La presente investigación se enfocó en la evaluación de redes basadas en MPLS regida por el uso del protocolo IPv6, empleando como diseño experimental pruebas de envío de datos y video sometidas a diversos tipos de tráfico (0%, 50% y 100%) en una topología totalmente cableada para obtener los parámetros de optimización de esta. Se utilizó una variación de la metodología planteada por Bisquerra (2000) efectuada en cuatro fases, en la primera fase se recopiló información teórica, la segunda fase se basó en la definición de pruebas e implementación de la topología, en la tercera fase se realizaron la pruebas definidas en la fase anterior, y por último se llevó a cabo la cuarta fase en donde se ejecutó las pruebas de medición mediante el uso del método estadístico ANOVA finalizando con el análisis comparativo-estadístico. Entre las conclusiones más relevantes, se tiene que el comportamiento de IPv6 en el rendimiento de redes MPLS con las condiciones estudiadas, no tiene diferencias significativas con respecto a IPv4 y que la saturación de tráfico no influyó negativamente en su desempeño.

**Palabras Clave:** IPv6, MPLS, Enrutamiento

**Dirección electrónica:** angie\_88\_9@hotmail.com

Carrasquero Urdaneta, Angelis Meliana. “**IPv6 protocol influence over MPLS (Multiprotocol Label Switching)** Proyecto de Trabajo Especial de Grado. Universidad del Zulia. Facultad Experimental de Ciencias. División de Programas Especiales. Licenciatura en Computación. Maracaibo. Venezuela. 2012. 89 pág.

**ABSTRACT**

This research are focused on the evaluation of MPLS-based under IPv6 use, implementing as an experimental design data and video transmission, subjected to many types of traffic (0%, 50% and 100%). A variation of Bisquerra (2000) methodology was used composed by four phases: theoretical information gathering, test definition and topologies implementation, test implementation and statistical analysis. Among the most important conclusions, was determined that IPv6 behavior over MPLS-based networks performance under studied conditions, it is not significantly different with respect IPv4 protocol

**Keywords:** IPv6, MPLS, QoS, routing.

**E-mail:** angie\_88\_9@hotmail.com

**ÍNDICE GENERAL**

|  |  |
| --- | --- |
|  | **Pág.** |
| **RESUMEN**……………………………………………………………………………….….  **ABSTRACT**…………………………………………………………………………………  **ÍNDICE DE ILUSTRACIONES**……………………………………………………………  **INTRODUCCIÓN**…………………………………………………………………….……. | 3  4  8  12 |
| **CAPÍTULO I**………………………………………………………………………………...  **PLANTEAMIENTO DEL PROBLEMA**…………………………………………………..  1. Planteamiento del Problema…..………………………………...…...……………......  2. Formulación 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……………………………………………......…….  2.1.1. Características de Ipv6………………...………………………………………..…  2.1.2 Ventajas de IPv6……….………………….…………………….………….……….  2.1.3. Direccionamiento IPv6….………………………………………………….………  2.1.4. Representación del direccionamiento IPv6 …….................…………..………  2.1.5 Representación de los prefijos de las direcciones............................................  2.1.6. Estructura de un paquete IPv6.........................................................................  2.2. Multiprotocol Label Switching (MPLS).................................................................  2.2.1. Antecedentes históricos……………………………………………………….…..  2.2.2. Arquitectura MPLS………................................................................................  2.2.2.1. Elementos.………..........................................................................................  2.2.2.2. Estructura………...........................................................................................  2.2.3. Operaciones con etiquetas...............................................................................  2.2.4. Características del MPLS…….……………………………………………………  2.2.5. Funcionamiento MPLS……….…………………………...………………………  2.2.6. Operación de MPLS………….………….…………………………………………  2.2.7 Ventajas específicas de MPLS ………..…………………………………………..  2.2.8. Manejo de colas y etiquetas……………………………………………………….  2.2.9. Enrutamiento convencional Vs conmutación de etiquetas MPLS…………….  2.2.10. Componentes de una red MPLS.………………………………………………..  2.2.11. Arquitectura MPLS y calidad de servicio (QoS) en una red IP……………….  2.3. 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……………………………………………………………………………….  ANÁLISIS 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**……………………………………………………………………  **ÍNDICE DE REFERENCIAS**………………………………………………………………  **ANEXO**……………………………………………………………………………………… | 14  15  15  18  18  18  18  18  19  20  20  20  21  22  22  24  25  26  27  28  30  30  31  32  34  35  35  36  36  38  39  40  41  43  44  46  47  47  47  48  48  50  51  72  73  73  79  81  86  88  89  92 |
|  |  |

|  |  |  |
| --- | --- | --- |
| **Figura** | **Título** | **Pág.** |
| 1  2  3  4  5  6  7  8  9 | Estructura de un paquete IPv6.........…………………………………...  Estructura de un paquete IPv4 e IPv6...………………...…………….  Modelo OSI con MPLS........................................................………….  Etiquetas MPLS ..………………………………………………………...  Estructura MPLS…….............…….……………………………………..  Funcionamiento MPLS ...............……………...………………………..  Colas y Etiquetas MPLS.................................................................…  Comparación de Enrutamiento Convencional y Conmutación de Etiquetas.............................................................................................  Componentes de control y Datos de un nodo .......…………………. | 28  29  31  33  34  37  39  40  42 |
| 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  37 | Configuración IPv4..................................………………………………  Configuración de las computadoras IPv4.............................…………  Configuración IPv6.............................…………………………………..  Configuración de las computadoras IPv6..........……………………….  Ambiente de Pruebas ...........................................…………………….  Pruebas con IPERF para detectar el Ancho de banda ................……  Comando para el servidor en DITG....................................................  Comando para el servidor en DITG....................................................  Comando para visualizar el resultado en el DITG..............................  TFTP Cliente.......................................................................................  TFTP Servidor....................................................................................  Filtro del Wireshark para el tráfico generado por el TFTP en IPv4....  Filtro del Wireshark para el tráfico generado por el TFTP en IPv6....  Filtro de wireshark para el tráfico generado por el VideoLan en IPv4  Filtro de wireshark para el tráfico generado por el VideoLan en IPv6.....................................................................................................  Configuración de VideoLAN en el computador receptor.....................  Configuración de VideoLAN en el computador emisor.......................  Elección del protocolo RTP...............................................................  Asignación de la dirección del receptor, el puerto y el tipo de video..  Último paso para empezar a emitir.....................................................  Paso para observar los resultados......................................................  Resultado de la captura del cliente....................................................  Resultado de la captura del servidor...................................................  Tipo de Archivo CSV.........................................................................  Pasos para calcular el promedio.........................................................  Decodificación para el protocolo RTP................................................  Analizador del RTP...........................................................................  Resultado de la captura de RTP usando Excel................................. | 52  53  53  54  55  55  57  57  58  60  60  61  61  62  62  63  63  64  64  65  66  67  67  68  68  70  70  71 |
| **Tabla** | **Título** | **Pág.** |
| 1 | Tráfico 0% enviando Datos................................................................. | 73 |
| 2 | Tráfico 50% enviando Datos............................................................... | 74 |
| 3 | Tráfico 100% enviando Datos............................................................. | 75 |
| 4 | Tráfico 0% enviando Video................................................................. | 76 |
| 5 | Tráfico 50% enviando Video............................................................... | 77 |
| 6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21 | Tráfico 100% enviando Video.............................................................  Tabla de valores del tráfico al 0%, 50% y 100% enviando datos……  Tabla ANOVA Delay con el tráfico 0%, 50% y 100% enviando datos ……………………………………………………………………….  Tabla ANOVA Bitrate con el tráfico 0%, 50% y 100% enviando datos ……………………………………………………………………….  Tabla ANOVA PaquetesE con el tráfico 0%, 50% y 100% enviando datos ……………………………………………………………………….  Tabla ANOVA PaquetesP con el tráfico 0%, 50% y 100% enviando datos ……………………………………………………………………….  Tabla de valores del tráfico al 0%, 50% y 100% enviando datos……  Tabla ANOVA Delay con el tráfico 0%, 50% y 100% enviando video ……………………………………………………………………….  Tabla ANOVA Bitrate con el tráfico 0%, 50% y 100% enviando video ……………………………………………………………………….  Tabla ANOVA PaquetesE con el tráfico 0%, 50% y 100% enviando video ……………………………………………………………………….  Tabla PaquetesP Delay con el tráfico 0%, 50% y 100% enviando video ……………………………………………………………………….  Protocolo IPv4, Tráfico 0%, 50% y 100% enviando datos……………  Protocolo IPv4, Tráfico 0%, 50% y 100% enviando video……………  Protocolo IPv6, Tráfico 0%, 50% y 100% enviando datos……………  Protocolo IPv4, Tráfico 0%, 50% y 100% enviando video……………  Tabla de Distribución F de Fisher con probabilidad de 0.05………… | 78  81  82  82  82  83  83  84  84  84  85  92  93  94  95  96 |
| **Gráficos** | **Título** | **Pág.** |
| 1 | Tráfico 0% enviando Datos……………………………………………… | 73 |
| 2 | Tráfico 50% enviando Datos…………………………………………….. | 74 |
| 3 | Tráfico 100% enviando Datos............................................................. | 75 |
| 4 | Tráfico 0% enviando Video ………………………..…………………... | 76 |
| 5 | Tráfico 50% enviando Video …………………………………………... | 77 |
| 6 | Tráfico 100% enviando Video………………………………………….... | 78 |

**INTRODUCCIÓN**

La evolución tecnológica en el sector de las telecomunicaciones ha sido muy violenta a partir de los años ochenta; en donde los medios tradicionales de comunicación, mensajería, telefonía entre otros, han convergido hacia esta única red de comunicación.

Estos crecimientos han dejado en descubierto las limitaciones del Protocolo de Internet Versión cuatro (IPv4) como lo ha sido, su reducido número de direcciones disponibles junto a problemas de arquitectura que han restringido y limitado el desarrollo de nuevas aplicaciones y tecnologías. Por tal motivo, se desarrollo el Protocolo de Internet Versión seis (IPv6) como solución a los problemas fundamentales de IPv4 y entregar una base para futuros desarrollos y avances.

Esta investigación se baso en estudiar e implementar el Protocolo de Internet Versión seis (IPv6) en redes basadas en MPLS para conocer sus funcionalidades y características beneficiosas al ser comparado con el Protocolo de Internet Versión cuatro (IPv4). Para tal efecto, la investigación se ha estructurado en cuatro capítulos:

Para el primer capítulo se plantea el problema, la justificación de la investigación, el objetivo específico y los objetivos generales en el cual se basó el desarrollo de la presente investigación.

En el segundo capítulo se llevó a cabo el desarrollo del marco teórico conformado a su vez por los antecedentes teóricos, donde se investigaron las bases u orígenes del tema.

Para el tercer capítulo se definió el tipo y diseño de la investigación, la metodología implementada y cómo se realizaron las pruebas.

Por último, en el cuarto capítulo se realizaron los análisis comparativos y estadísticos de las pruebas.

**CAPÍTULO I**

**CAPÍTULO I**

**PLANTEAMIENTO DEL PROBLEMA**

1. Planteamiento del problema

Los avances logrados en el área de telecomunicaciones, han permitido que el hombre se desempeñe de una manera más eficiente y esta eficiencia es lo que en gran medida, ha motivado a empresas nuevas a exigir mayores retos a quienes lo desarrollan. De esta forma, se ha llegado a logros de avances tecnológicos creando alternativas de gran impacto.

Uno de los grandes avances que se utiliza en la actualidad es la versión cuatro (4) del Protocolo de Internet; el aumento de usuarios, aplicaciones, servicios y dispositivos provocaron la creación, así como la migración hacia una nueva versión seis (6) del protocolo de internet (IP por sus siglas en inglés, Internet Protocol) llamada Ipv6, que nos proporciona un espacio de direcciones que se ha ampliado enormemente, lo que permitirá a la Internet crecer en el futuro.  (NRO, 2010)

La génesis de este nuevo protocolo no ha venido sólo propiciada por la escasez de direcciones; si no que introduce un número de mejoras sobre la versión actual como la identificación de paquetes perteneciente a cierto “Flujo” en particular, como por ejemplo el tráfico multimedia, el cual debe llegar en “Tiempo real” y se le puede proporcionar una mayor calidad de servicio (Quality of Service) con respecto a otros clientes. Además, incluye características que serán necesarias para algunos nuevos servicios como la flexibilidad en el direccionamiento y seguridad mediante la autentificación y la privacidad, posibilidad de paquetes con carga útil (datos) de más 65535 bytes, características de movilidad, entre otras (Ferrer-Rocas, 2001).

La creciente demanda de aplicaciones multimedia por parte de los clientes ISP (Internet Service Providers, en inglés), con altas necesidades de ancho de banda, con garantía de Calidad de Servicio, propiciaron la introducción de ATM (Asyncronous Transfer Mode, en inglés). Aún cuando este modelo de IP sobre ATM satisfacía los requisitos de las nuevas aplicaciones, ofreciendo un encaminamiento inteligente de

nivel 3 de los enrutadores IP en la red de acceso y un aumento del ancho de banda y rendimiento de los conmutadores de nivel 2, la arquitectura presentaba ciertas limitaciones en cuanto a costo de los equipos y la dificultad de operar e integrar redes basándose en dos tecnologías muy distintas (Moya y Millán, 2002).

Motivado por estas limitaciones el [IETF (Internet Engineering Task Force, en inglés)](http://www.ietf.org/) establece el grupo de trabajo MPLS (MultiProtocol Label Switching, en inglés) para producir un estándar que unificase las soluciones propietarias de conmutación de nivel 2. Por lo tanto, MPLS es un protocolo de red que simplifica la retransmisión de los paquetes, al utilizar etiquetas de longitud fija en vez de direcciones, proporcionando los beneficios de la ingeniería de tráfico como una mayor escalabilidad, entre otras. Esta tecnología puede ser aplicada a cualquier tipo de red y está diseñado para operar sobre cualquier tecnología en el nivel de enlace (Moya y Millán, 2002).

Al relacionar los criterios de uso de MPLS con respecto a las bondades que puede brindar Ipv6, surge la inquietud de determinar si estas nuevas características pueden afectar el desempeño de una red con los servicios descritos, debido a los escasos estudios realizados a la fecha. El análisis exhaustivo que se realiza de la cabecera IP durante el etiquetado de paquetes en MPLS, así como el proceso de encaminamiento IP y MPLS, según lo refiere Boada y otros (2005), podrían crear un aumento en las latencias de la red, y por consiguiente una degeneración en la red.

Asimismo, dado que los mecanismos de traducción (Ipv6-Ipv4) dependen normalmente del proceso de conmutación de paquetes, pueden experimentarse limitaciones significativas en el rendimiento. En la mayoría de estos mecanismos deberían tenerse en cuenta cuando estos se integren en un despliegue planificado del Ipv6, tal y como lo afirma Boada y otros (2005).

En relación a lo antes expuesto, esta investigación buscó implementar una topología de servicio de red basada en MPLS (MultiProtocol Label Switching, en inglés) a fin de evaluar la influencia del nuevo protocolo de Internet Ipv6 en su rendimiento, en condiciones aplicables a métodos de traducción ya definidos, con el propósito de promover el uso de Ipv6 en ambientes similares y generar métricas para su implementación a otros niveles.

2. Formulación del problema

¿Podrá determinarse la influencia del protocolo Ipv6 en redes basadas en MPLS (Multiprotocol Label Switching)?

3. Objetivos de la Investigación

3.1 Objetivo general

Evaluar la influencia del protocolo Ipv6 en redes basadas en MPLS (Multiprotocol Label Switching) y la aplicación de políticas de Calidad de Servicio.

3.2 Objetivo específico

* Profundizar teóricamente todo lo concerniente al Protocolo Ipv6 y redes MPLS.
* Analizar los parámetros que definen la QoS en una red MPLS.
* Diseñar la topología de red para el estudio de Ipv6 con la red basada en MPLS.
* Definir los tipos de pruebas que permitan evaluar redes MPLS, bajo el protocolo Ipv6.
* Implementar los ambientes y tipos de pruebas variando parámetros de medición tales como la versión del IP y el tráfico de red.
* Evaluar estadísticamente los resultados obtenidos de las pruebas.

4. Justificación e Importancia de la Investigación

El pequeño “pool” de direcciones IP existentes marca un momento crítico en el agotamiento de direcciones IPv4 lo que contribuye a promover la implementación de direcciones IPv6. Un poco más del 90% de direcciones ya fueron asignadas, quedando menos del 10% de direcciones por asignar. La implantación de este nuevo protocolo es un desarrollo de infraestructura clave, que permitirá que la red sustente los miles de millones de personas y dispositivos que se conectarán en los próximos años. Aunque el protocolo IPV6 brinda muchas funcionalidades y características que favorecen el envío del tráfico, éstas no son suficientes para poder hacer un uso correcto de los recursos de la red Doménico y García (2011), nos explica que a pesar de haberse definido dos arquitecturas de Calidad de Servicio, ninguna de estas llega a satisfacer las necesidades actuales de las aplicaciones. En la primera arquitectura, Servicios Integrados, se reservan recursos en los nodos de la red haciendo uso de señalización, lo cual deteriora el rendimiento de la misma. En la segunda arquitectura, Servicios Diferenciados, se tiene un comportamiento en base a los bits DS pero no de forma garantizada ya que no se especifican las necesidades del tráfico a cursar, sin mencionar que los enrutadores no intercambian información sobre los tráficos.

MPLS surge como la mejor opción que se puede encontrar actualmente para el manejo del troncal de Internet por sus diferentes características: ingeniería de tráfico, bajo costo de implementación, así como adaptación con tecnologías de capa de Enlace y de Red, y su fusión con IPv6 representa un gran aporte en el despliegue del mismo. Doménico y García (2011).

Estos conocimientos han sido respaldados con datos obtenidos en redes MPLS, que permitieron cuantificar la calidad de la red ante ciertas topologías y eventos que puedan ocurrir en ella. Por último, esta investigación representa un aporte teórico y metodológico en el uso de IPv6 asociado al uso de MPLS, mediante la difusión de los resultados que se han generado.

5. Delimitación de la investigación.

El transcurso de la investigación y de las pruebas, 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 Julio del 2011 hasta Enero del 2012.

**CAPÍTULO II**

**CAPÍTULO II**

**MARCO TEÓRICO**

En este capítulo se explican de forma detallada las bases teóricas que sustentaron la ejecución de esta investigación. De esta forma, se explican las características de las tecnologías, los beneficios que posee cada una, así como los problemas que se pretenden superar en la Internet actual.

1.- Antecedentes de la investigación

Actualmente se presentan muchos problemas con el protocolo IPv4 a nivel de capa de red. Si bien en sus comienzos resultó ser un esquema adecuado y robusto dado que las aplicaciones no necesitaban un gran ancho de banda, no requerían una ingeniería de tráfico; solo se tenían pocos nodos capaces de generar tráfico en la red; pero con el pasar del tiempo, el desarrollo y la convergencia a la que tienden los múltiples servicios clásicos y los nuevos servicios que han aparecido, en su mayoría servicios interactivos, hace que el escenario inicial en el que se planteó IPv4 no sea suficiente para satisfacer la demanda actual de QoS.

Rodríguez y Zambrano (2010) realizaron un proyecto de investigación titulado “Análisis y diseño de una reingeniería organizativa de la red del campus de la Universidad técnica de Manabí mediante la utilización de IPv6 y su implementación en la Facultad de Ciencias Informáticas en el laboratorio de redes” donde realizaron estudios y análisis de la migración del protocolo IPv4 a IPv6 Concluyendo que la red permitió conectar a las distintas unidades administrativas y departamentos directamente a Internet mediante IPv6, sin necesidad de utilizar túneles o traducción de protocolos. Este trabajo aporto información teórica sobre el rendimiento de los protocolos IPv4 e IPv6 y sobre la migración de IPv4 a IPv6.

Por su parte, Doménico y García (2011) realizaron un proyecto de investigación que se titula “Medición y Análisis de tráfico en redes MPLS” siendo el objetivo general realizar un estudio profundo y detallado del protocolo MPLS, donde una de sus primeras conclusiones fue que gracias a este protocolo se pueden afrontar problemas como la migración de IPv4 a IPv6 de manera progresiva sin los problemas citados. Mediante este trabajo, se pudo obtener conocimiento teórico así como también, se pudo comprobar que la migración de IPv4 con MPLS a IPv6 con MPLS fue de manera sencilla, esto se debe a que la configuración de MPLS en IPv4 es igual para Ipv6.

También, Subía y otros (2006) realizaron un estudio que se titula “Comunicaciones IPv6 con MPLS” donde enfocaron su investigación en MPLS y las aplicaciones de esta misma. Una de sus conclusiones fueron que utilizaron routers marca cisco debido a que cumple con las especificaciones técnicas mínimas requeridas como: velocidad de transmisión, soporte para transmitir datos y video, Calidad de servicio, protocolo de direccionamiento IPv6, entre otros. Esta Investigación contribuyó a la elección de los equipos que se utilizaron, los cuales también fueron marca cisco y de esta manera también cumplir las especificaciones técnicas mínimas requeridas.

Por último, Rubiano y Urbano (2006) realizaron un proyecto de investigación que se titula “Investigación de la arquitectura MPLS ventajas y servicios.” Teniendo como objetivo describir las ventajas y servicios fundamentales que abarcan la Conmutación de Etiquetas Multiprotocolo (MPLS) llegando a la conclusión que MPLS triunfó como única solución para aumentar el desempeño de las redes actuales, ya que ha sido la solución a los inconvenientes del enrutamiento clásico que van desde los problemas con la velocidad, el retardo y la escalabilidad hasta el manejo de la calidad de servicio (QoS) e ingeniería de tráfico. Mediante este trabajo, fue posible crear el marco teórico de todo lo referente al protocolo MPLS.

2.- Bases Teóricas

Estas representan la sustentación teórica, que se basó en un conjunto de conceptos y proposiciones que constituye un enfoque determinado para el desarrollo de la presente investigación.

2.1.- Protocolo de Internet versión 6.

En el año 1990, tras la primera voz de alerta sobre el posible agotamiento de direcciones IP el IETF promueve un grupo de trabajo que se encargarían de crear el nuevo protocolo de Internet llamado IPV6, removiendo aquellas características que son poco utilizadas en la práctica y manteniendo los conceptos principales de IPv4, considerando el protocolo una evolución más que una revolución según Rodríguez y Zambrano (2010).

2.1.1.- Características de IPv6

Deering y Hiden (1998) explican que los cambios de Ipv4 a Ipv6 recaen en las siguientes características:

* Capacidades de Direccionamiento

IPv6 aumenta el tamaño de la dirección IP de 32 a 128 bits lo que se traduce alrededor de 3,4x10^38 direcciones posibles. Esto permite asegurar que cada dispositivo conectado a una red pueda contar con una dirección IP pública.

* Nuevo formato de encabezado

Aun cuando el tamaño de la cabecera en IPv6 es mayor que en IPv4, el formato de ella se ha simplificado. Se han eliminado campos que en la práctica eran poco usados, de forma de hacer más eficiente el manejo de paquetes. Con la incorporación de cabeceras adicionales, IPv6 permite futuras expansiones.

## Infraestructura de direcciones y enrutamiento eficaz y jerárquica

Las direcciones globales están diseñadas para crear una infraestructura eficaz, jerárquica y que se puede resumir y que tiene en cuenta la existencia de múltiples niveles de proveedores de servicios Internet. En la red Internet IPv6, los enrutadores de red troncal tienen tablas de enrutamiento mucho más pequeñas.

* Seguridad integrada

La compatibilidad con IPSec es un requisito del conjunto de protocolos IPv6. Este requisito proporciona una solución basada en estándares para las necesidades de seguridad de red y aumenta la interoperabilidad entre diferentes implementaciones de IPv6.

* Mejora de la compatibilidad para la calidad de servicio (QoS)

Los nuevos campos del encabezado IPv6 definen cómo se controla e identifica el tráfico. La identificación del tráfico, mediante un campo Flow Label (etiqueta de flujo) en el encabezado, permite que los enrutadores identifiquen y proporcionen un control especial de los paquetes que pertenecen a un flujo dado. Un flujo es un grupo de paquetes entre un origen y un destino. Dado que el tráfico está identificado en el encabezado IPv6, la compatibilidad con QoS se puede obtener de forma sencilla incluso si la carga del paquete está cifrada con IPSec.

* Capacidad de ampliación

IPv6 se puede ampliar con nuevas características al agregar encabezados de extensión a diferencia del encabezado IPv4, que sólo admite 40 bytes de opciones, el tamaño de los encabezados de extensión IPv6 sólo está limitado por el tamaño del paquete IPv6.

* Movilidad

Es la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.

* Autoconfiguración

IPv6 incorpora un mecanismo de auto configuración de direcciones, “stateless address configuration”, mediante el cual los nodos son capaces de auto asignarse una dirección IPv6 sin intervención del usuario.

2.1.2.- Ventajas del Protocolo IPv6

De acuerdo al trabajo de Investigación de Wallid (2004) titulado “Transición a IPv6 en un departamento Universitario” hace referencia a las ventajas que nos proporciona el protocolo de Internet 6 como lo es:

* El desarrollo de mecanismos que permiten gestionar de forma automática el traslado de los dispositivos de unas redes a otras, permitiendo así la conexión automáticas a su red de origen de dispositivos que se encuentran temporalmente en redes de acceso remotas. A estos procedimientos, englobados bajo el nombre de IPv6 Mobility, se les ha concedido una gran importancia dado que permiten gestionar nuevos servicios hasta ahora el participio a la Internet tradicional.
* IPv6 se ha diseñado teniendo en mente las nuevas necesidades de calidad de servicio (QoS) que estarán presentes en los nuevos servicios proporcionados a los clientes de la nueva red.
* Este nuevo protocolo también ha sido pensado para hacer uso de las técnicas de cifrado (IPSec) con el fin de dar mayor privacidad a las comunicaciones de usuario.
* La amplitud de direcciones disponibles permitirá que virtualmente cualquier dispositivo electrónico disponga de una conexión a la red.

Se han diseñado técnicas de asignación automática de direcciones a los dispositivos, con el fin de evitar que cada dispositivo de red haya de ser configurado manualmente. También se ha proporcionado mecanismos que permiten detectar y resolver colisiones de direccionamiento en el caso de que varios dispositivos intenten utilizar la misma dirección IPv6.

2.1.3.- Direccionamiento IPv6

Según Deering y Hinden (2003) las direcciones IPv6 son identificadores de 128 bits y conjuntos de interfaces donde hay 3 tipos de direcciones:

* Unicast: Identificador de una interfaz. Un paquete enviado a una dirección unicast es entregado a la interfaz identificada por esa dirección.

En IPv6 las direcciones Unicast pueden pertenecer a uno de los tres contextos existentes:

* Local al enlace (“link - local”): Identifica a todos los nodos dentro de un enlace (Capa 2).
* Local único (“unique - local”): Identifica a todos los dispositivos dentro de una red interna o sitio, compuesta por varios enlaces o dominios capa 2.
* Global: Identifica a todos los dispositivos ubicables a través de Internet.
* Anycast: Identificador para un conjunto de interfaces (típicamente perteneciente a diferentes nodos). Un paquete enviado a una dirección anycast se entrega a una de las interfaces identificadas por esa dirección (la “más cercana”, de acuerdo a la ruta protocolos de medida “de la distancia”).
* Multicast: Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección de multidifusión se entrega a todas las interfaces identificadas por esa dirección.

Donde el tipo específico de dirección IPv6 es 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.

2.1.4.- Representación del direccionamiento IPv6

Según RAU (2005), existen tres formas de representar las direcciones IPv6 como Strings de texto.

x:x:x:x:x:x:x:x donde cada x es el valor hexadecimal de 16 bits, de cada uno de los 8 campos que definen la dirección. No es necesario escribir los ceros a la izquierda de cada campo, pero al menos debe existir un número en cada campo.

Ejemplos:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210

1080:0:0:0:8:800:200C:417A

Como será común utilizar esquemas de direccionamiento con largas cadenas de bits en cero, existe la posibilidad de usar sintácticamente :: para representarlos. El uso de **::** indica uno o más grupos de 16 bits de ceros. Dicho símbolo podrá aparecer una sola vez en cada dirección. Por ejemplo:

1080:0:0:0:8:800:200C:417A     unicast address   
          FF01:0:0:0:0:0:0:101                multicast address   
          0:0:0:0:0:0:0:1                         loopback address   
          0:0:0:0:0:0:0:0                         unspecified addresses

 podrán ser representadas por:

   1080::8:800:200C:417A       unicast address   
         FF01::101                                multicast address   
         ::1                                           loopback address   
         ::                                             unspecified addresses

Para escenarios con nodos IPv4 e IPv6 es posible utilizar la siguiente sintaxis:  
x:x:x:x:x:x:d.d.d.d, donde x representan valores hexadecimales de las seis partes más significativas (de 16 bits cada una) que componen la dirección y son valores decimales de los 4 partes menos significativas (de 8 bits cada una), de la representación estándar del formato de direcciones IPv4:

Ejemplos:   
                   0:0:0:0:0:0:13.1.68.3   
                   0:0:0:0:0:FFFF:129.144.52.38   
  
  o en la forma comprimida   
                 ::13.1.68.3   
                 ::FFFF:129.144.52.38

2.1.5.- Representación de los prefijos de las direcciones

Los prefijos de identificadores de subredes, enrutador y rangos de direcciones IPv6 son expresados de la misma forma que en la notación CIDR utilizada en IPv4.

Un prefijo de dirección IPv6 se representa con la siguiente notación:

dirección-ipv6/longitud-prefijo, donde:

* dirección-ipv6: es una dirección IPv6 en cualquiera de las notaciones mencionadas anteriormente.
* longitud-prefijo: es un valor decimal que especifica cuantos de los bits más significativos, representan el prefijo de la dirección.

2.1.6.- Estructura de un paquete IPv6

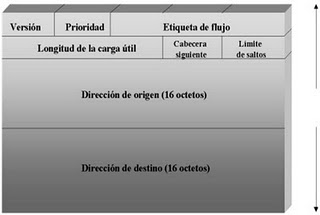


Imagen N° 1: Estructura de un paquete IPv6.

Fuente: Rodríguez y Zambrano (2010)

De acuerdo a la Investigación realizada por Rodríguez y Zambrano (2010) un paquete IPv6 tiene una cabecera de tamaño fijo a 40 [byte], el doble de la cabecera de IPv4. Este aumento se debe a que tamaño de los campos “Source Address” y “Destination Address” aumentaron su tamaño de 32 a 128 [bit] cada uno. La cabecera posee los siguientes 8 campos:

Versión (“Version”): Indica la versión del protocolo IP, en este caso su valor es igual a 6.

Clase de tráfico (“Traffic Class”): Incluye información que permite a los “enrutador” clasificar el tipo de tráfico al que el paquete pertenece, aplicando distintas políticas de enrutamiento según sea el caso. Realiza la misma de función que el campo “Type of Service” de IPv4.

Etiqueta de Flujo (“Flow Label”): Identifica a un flujo determinado de paquetes, permitiendo a los “Enrutador” identificar rápidamente paquetes que se deben ser tratados de la misma manera.

Tamaño de la carga útil (“Payload Length”): Indica el tamaño de la carga útil del paquete. Las cabeceras adicionales son consideradas parte de la carga para este cálculo.

Próximo encabezado (“Next Header”): Indica cual es el siguiente cabecera es la siguiente adicional presente en el paquete. Si no se utilizan, apunta hacia la cabecera de protocolo capa 4 utilizado.

Limite de saltos (“Hop Limit”): Indica el máximo número de saltos que puede realizar el paquete. Este valor es disminuido en uno por cada “router” que reenvía el paquete. Si el valor a cero, el paquete es descartado.

Dirección de origen (“Source Destination Address”): Indica la dirección de Ipv6 del nodo que género el paquete.

Dirección de origen (“Source Destination Address”): Indica la dirección deldestino final del paquete.

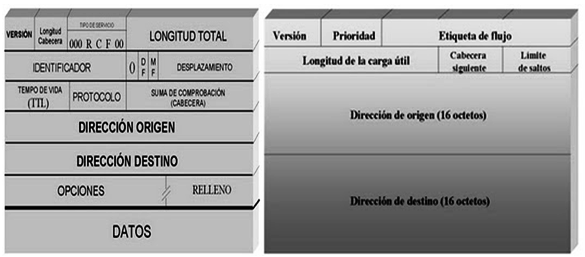


Imagen N° 2: Estructura de un paquete IPv4 e IPv6.

Fuente: Rodríguez y Zambrano (2010)

En la Imagen N° 2 podemos apreciar los cambios de la cabecera IPv6 respecto a la cabecera IPv4.

El protocolo IPv6 reemplaza el campo “options” de IPv4 por las denominadas cabeceras adicionales. Estas cabeceras permiten expandir el funcionamiento de IPv6, sin verse restringidas a un campo de tamaño fijo como el presente en IPv4. Las cabeceras adicionales se ubican inmediatamente depuse de la cabecera IPv6 y antes de la cabecera del protocolo superior (UDP o TCP).

2.2.- Multi-Protocol Lable Switching (MPLS)

Jara (2004) realizó una investigación titulada docencia en QoS orientada a redes MPLS. Donde afirma que MPLS es una tecnología híbrida que hace uso de una técnica conocida como Label Switching, que codifica una etiqueta en la cabecera del paquete que se usa para retransmitir el mismo (forwarding). Cuando un router que soporta MPLS recibe un paquete, decide la interfaz de transmisión según la etiqueta, en vez de hacerlo mediante un algoritmo de ruteo.

2.2.1.- Antecedentes históricos

Según Rubiano y Urbano (2006) nos explica que cuando se comenzó a utilizar Internet, los backbones IP de los proveedores estaban construidos por enrutadores conectados entres sí, lo cual generó saturación de las redes y provocó la falta de ancho de banda en las transmisiones. Debido a eso se aumentó el rendimiento de los enrutadores, dándose a conocer los conmutadores ATM con ciertas capacidades de control IP.

Se generaron entonces varios tipos de problemas que tenían que ver con el rendimiento óptimo y para lo cual se implementaron soluciones de integración de niveles que fueron conocidos como conmutación IP. Sin embargo, estas soluciones causaban congestionamiento y no eran operativas entre las distintas tecnologías de capa 2 y 3 que se conocían.

Es por esto que para los administradores de red el buen desempeño de la red siempre ha sido un reto, generando un continuo surgimiento de protocolos de enrutamiento teniendo siempre como objetivo principal diseñar el camino más corto para la ruta que un paquete debe seguir por la red, más sin embargo no se ha tenido en cuenta parámetros que afecten el desempeño de la red como lo son retardo, QoS, congestión de tráfico, etc.

El surgimiento de MPLS se da a mediados del año 90 siendo un gran avance cuando hablamos de eficiencia en la toma de decisiones de enrutamiento y conmutación debido a que opera entre la capa de enlace y capa de red permitiendo una conmutación más rápida, dado que la cabecera de capa de enlace se encuentra antes de la capa de red.

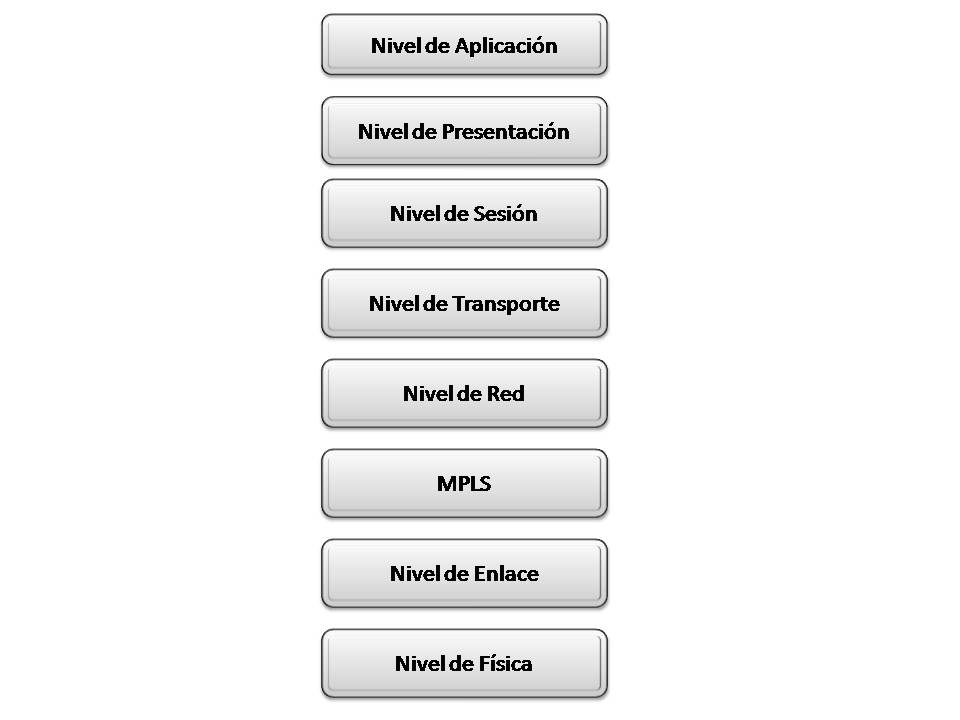


Imagen N° 3: Modelo OSI con MPLS

Fuente: Doménico y García (2011)

2.2.2.- Arquitectura MPLS

Según Doménico y García (2011) los elementos y estructura del protocolo MPLS se clasifican de la siguiente manera:

2.2.2.1.- Elementos

* LER: Label Edge Router

Es el nodo que conecta un dominio de conmutación de etiquetas con un nodo externo al dominio, bien porque no soporta la conmutación de etiquetas o por que pertenece a otro dominio de conmutación de etiquetas.

* FEC Forwarding Equivalence Class

Conjunto de paquetes pertenecientes a determinado flujo que ingresan en la red MPLS a través de un mismo Router Ingress LER, a los cuales se les asigna la misma etiqueta y por tanto circulan por un mismo camino a través de la backbone hasta su destino. Normalmente se trata de paquetes que pertenecen a un mismo flujo correspondiente a una aplicación los que reciben la misma etiqueta. La FEC para la red especifica los recursos que se asignarán al tráfico que lleve la etiqueta a lo largo del camino LSP cuando este circule en la red MPLS. Cabe resaltar que un FEC puede agrupar varios flujos de diferentes aplicaciones según lo crea conveniente el administrador de la red y/o según lo estipulado en el contrato de arrendado con el ISP, pero un mismo flujo no puede pertenecer a más de una FEC al mismo tiempo ya que no se pueden asignar diferentes tipos de recursos a un mismo tráfico.

* LSP Label Switched Path

Camino por el cual el tráfico con FEC asignada será enviado a través de la red MPLS. Este camino es equivalente a un circuito virtual en la tecnología. En este trayecto que seguirá el tráfico, los recursos son asignados según el LSA. Además, si hubiese alguna falla de algún nodo intermedio en la red MPLS, el camino LSP puede conmutar de manera estática o dinámica según lo crea más conveniente el administrador de la red MPLS y/o lo estipulado en el contrato con el ISP.

* LSR Label Switching Router

El router que puede conmutar paquetes en función a la etiqueta asignada MPLS según los diferentes parámetros del tráfico. Estos enrutador se encuentran en el interior de la red MPLS y solo se encargan de la tarea de conmutar los paquetes etiquetados.

* LDP Label Distribution Protocol

Para el correcto funcionamiento de la arquitectura MPLS se necesita que el camino o LSP, así como los requerimientos del tráfico, sean anunciados a los nodos por los cuales este tráfico será enviado. Este protocolo recibe el nombre de LDP y es usado por los enrutador LSR y/o del tipo LER (Ingress o Egress).

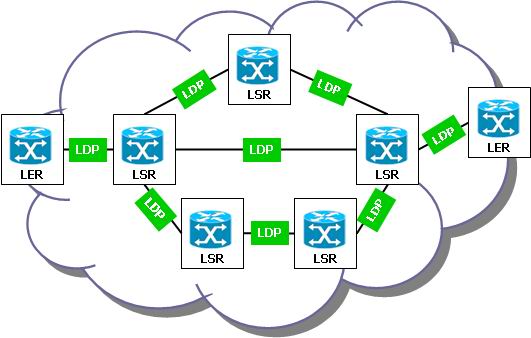


Imagen N° 4: Etiquetas MPLS

Fuente: Fuente: Doménico y García (2011)

2.2.2.2.- Estructura

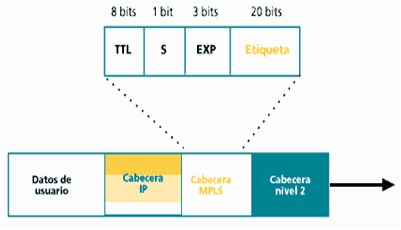
****

Imagen N° 5: Estructura MPLS

Fuente: Fuente: Doménico y García (2011)

* Campo TTL Time to Live (8 bits)

Al igual que en el protocolo IP, este campo sirve como un contador del número de saltos para poder evitar la creación de bucles o loops que se puedan generar en el envío de los paquetes etiquetados. Este campo reemplaza al TTL de la cabecera IP durante el viaje del datagrama por la red MPLS y es disminuido en una unidad por cada nodo por el que pasa; si llegase a cero en algún LSP, será descartado.

* Campo Stacking (1 bits)

Gracias a este campo, se tienen jerarquías de etiquetas. MPLS tiene la capacidad de etiquetar tráfico MPLS de una red vecina con lo que se forma una pila o stack. Toma el valor 1 para la primera entrada en la pila, y cero para el resto.

* Campo Experimental EXP (3 bits)

Campo para uso experimental, pero actualmente se utiliza para transmitir información DiffServ por la creciente demanda de prioridades en el protocolo IP con lo que se tendrían ocho niveles de prioridad incluyendo el esquema de Best Effort.

* Campo Label o Etiqueta (20 bits)

En base a este campo, los LSR pueden efectuar la conmutación. Esta etiqueta es asignada por el Ingress LER según parámetros descritos en el LSA. Como se indicó antes, los LSP son los que cambian la etiqueta a lo largo de su recorrido para poder formar un túnel LSP y la última etiqueta es extraída por el Egress LER. Doménico y García (2011)**.**

2.2.3.- Operaciones con etiquetas**:**

Según Boada y otros (2005) las operaciones con etiquetas de MPLS son las siguientes:

* PUSH
* Imposición de etiqueta al paquete de nivel de red
* Apilamiento de etiquetas según LIFO (Last-In, Firt – Out)
* SWAP
* Intercambio de etiquetas
* Según la etiqueta de entrada se obtiene la etiqueta de salida y se cambia el valor en el paquete
* POP
* Retirada de la etiqueta.

2.2.4.- Características MPLS

También Boada y otros (2005) nos especifican las características que presentan las redes basadas en MPLS.

* Flexibilidad
* Escalabilidad
* Accesibilidad
* Eficiencia
* Calidad de servicio y clases de servicios
* Administración
* Monitoreo

2.2.5.- Funcionamiento MPLS

Morales (2006), plantea que una red MPLS consiste de un conjunto de enrutadores de conmutación de etiquetas (LSR) que tiene la capacidad de conmutar y rutear paquetes en base a la etiqueta que se ha añadido a cada paquete. Cada etiqueta define un flujo de paquetes entre dos puntos finales. Cada flujo es diferente y es llamado clase de equivalencia de reenvió (FEC), así como también cada flujo tiene un camino específico a través de los LSR de la red, es por eso que se dice que la tecnología MPLS es “orientada a conexión”. Cada FEC, además de la ruta de los paquetes contiene una serie de caracteres que definen los requerimientos de QoS del flujo. Los enrutadores de la redes MPLS no necesitan examinar ni procesar el encabezado IP, solo es necesario reenviar cada paquete dependiendo el valor de su etiqueta. Esta es una de las ventajas que tienen los enrutador MPLS sobre los enrutador IP, en donde el proceso de reenvió es más complejo.

En un router IP cada vez que se escribe un paquete se analiza su encabezado IP para comprarlo con la tabla de enrutamiento (routing table) y ver cuál es el siguiente salto (next hop). El hecho de examinar estos paquetes en cada uno de los puntos de transito que deberán recorrer para llegar a su destino final significa un mayor tiempo de procesamiento en cada nodo y por lo tanto, una mayor duración en el recorrido.

2.2.6.- Operación de MPLS

De la misma manera Morales (2006) nos plantea el siguiente diagrama de operación:

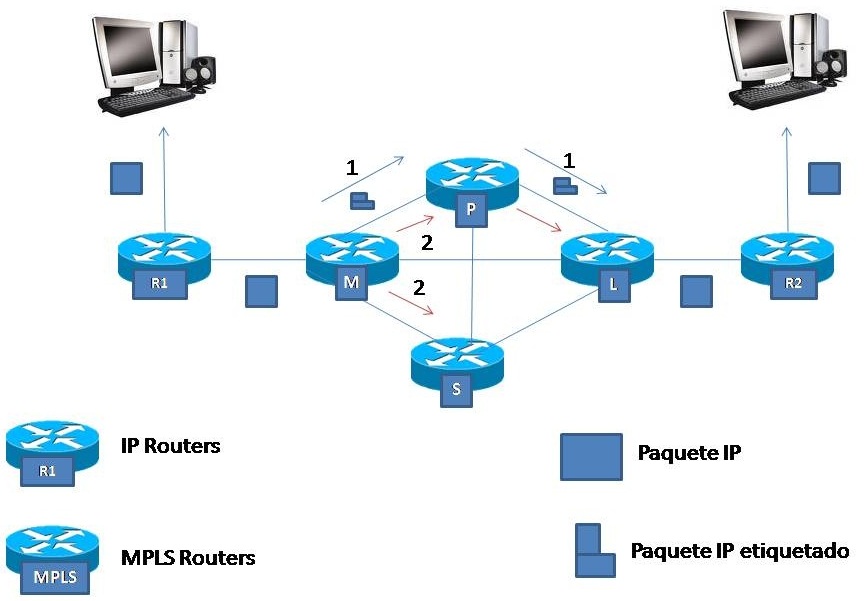


Imagen N° 6: Funcionamiento MPLS

Fuente: propia (2011)

Primero antes de mandar la información por el flujo es necesario establecer un camino de conmutación de etiquetas (LSP) entre los enrutador que van a transmitir la FEC. Dichos LSP sirven como túneles de transporte a lo largo de la red MPLS e incluyen los parámetros QoS específicos del flujo. Estos parámetros sirven para determinar dos cosas:

La cantidad de recursos a reservar a LSP

Las políticas de desechado y la cola de procesos en cada LSR.

Para lograr los puntos anteriores se utilizan dos protocolos para intercambiar información entre los enrutador de la red.

Luego se le asignan etiquetas a cada flujo FEC particular para evitar el uso de etiquetas globales que dificultan el manejo y la cantidad de las mismas. Por esta razón las etiquetas solo hacen referencia al flujo específico. La asignación de nombres y rutas se puede realizar manualmente o bien se puede utilizar el protocolo de distribución de etiquetas (LDP).

En esta sección el paquete entra al dominio MPLS mediante un LSR frontera que determina que servicios de red requiere, definiendo así su QoS. Al terminar dicha asignación el LSR asigna el paquete a una FEC y a un LSP particular, lo etiqueta y los envía. Si no existe ningún LSP, el router frontera trabaja en conjunto con los demás LSRs para definirlo.

En este momento el paquete ya está dentro del dominio MPLS, cuando los enrutador contiguos del LSR reciben el paquete se llevan a cabo los siguientes procesos:

* Se desecha la etiqueta de entrada y se le añade la nueva etiqueta de salida al paquete.
* Se envía el paquete al siguiente LSR dentro de LSP.

El LSR de salida “abre” la etiqueta y lee el encabezado IP para enviarlo al destino final.

2.2.7.- Ventajas especificas de MPLS

Según Morales (2006), en este momento ya es posible identificar algunas de las ventajas internas más importantes que MPLS presenta:

* Un domino MPLS consiste de una serie de enrutador habilitados con MPLS continuos. El tráfico puede entrar por un punto final físicamente conectado a la red, o por otro router que no sea MPLS y que esté conectado a una red de computadoras sin conexión directa a la nube MPLS.
* Se puede definir un comportamiento por salto (PHB) diferente en cada router de la FEC. El PHB (Per Hop Behaviour) define la prioridad en la cola y las políticas de desechado de los paquetes.
* Para determinar el FEC se pueden utilizar varios parámetros que define el administrado de la red.
* Dirección IP fuente o destino y/o las direcciones IP de la red.
* Utilizar el id del protocolo IP.
* Etiqueta de flujo IPv6
* Número de puerto de la fuente o del destino.
* El punto de código (codepoint) de los servicios diferenciados (DSCP).
* El reenvió de información se lleva a cabo mediante una búsqueda simple (LOOKUP) en una tabla predefinida que enlaza los valores de las etiquetas con las direcciones del siguiente salto (next hop).
* Los paquetes enviados de mismos endpoint pueden tener diferentes FEC, por lo que las etiquetas serán diferentes y tendrán un PHB distinto en cada LSR. Esto puede generar diferentes flujos en la misma red.

2.2.8.- Manejo de colas y etiquetas

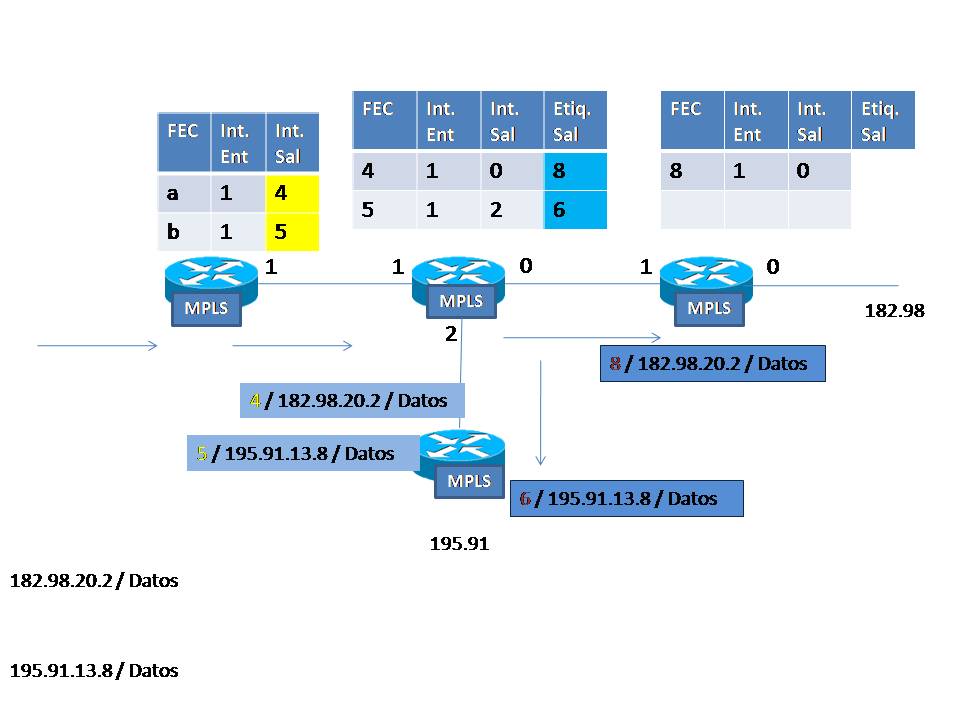
****

Imagen N° 7: Colas y Etiquetas MPLS

Fuente: Morales (2006)

Como se puede observar en la figura cada LSR tiene una tabla de reenvió para cada LSP que pasa por sus interfaces. Dichas tablas manejan diferentes tipos de datos, la tabla del LSR de entrada maneja la FEC, la interfaz de salida y etiqueta de salida, los LSR siguientes manejan etiqueta e interfaz ambas de entrada y de salida.

Posteriormente se muestra como llegan los datos (a y b) sin etiqueta al LSR de entrada, el cual les asigna una etiqueta de salida y lo manda al siguiente LSR (next hop LSR). El LSR siguiente correspondientes, es aquí donde se ve la escalabilidad de la tecnología, ya que las etiquetas solo tienen significado local.

Otra de las funciones de LSR de entrada es asignarle una FEC a cada paquete sin etiquetar que entra, y en base a esto asigna cada paquete a un LSP particular. En la figura (NÚMERO DE LA FIGURA) tenemos dos FERCs (a y b) cada uno con su LSP particular.

2.2.9.- Enrutamiento convencional Vs Conmutación de etiquetas MPLS

Con MPLS se generan cierta cantidad de ventajas, las cuales son reflejadas en la siguiente imagen:

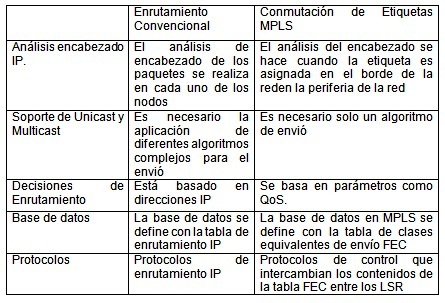


Imagen N° 8: Comparación de Enrutamiento Convencional y Conmutación de Etiquetas

Fuente: Rubiano y Urbano (2006)

2.2.10.- Componentes de una red MPLS

La conmutación por etiquetas se puede describir principales:

* Componente de Control

La componente de control es la que se encarga de crear y mantener la información de etiquetas asignadas entre un grupo de LSR interconectados, por esto cada nodo de MPLS utiliza los protocolos de encaminamiento como lo son: OSPF, IS-IS y BGP-4, realizando un intercambio de información con los enrutadores para la construcción y mantenimiento de las tablas de encaminamiento. El componente de control es responsable de configurar los LSP entre rutas IP y también mantiene actualizado el sistema cuando existe algún cambio en la topología de la red.

La idea de separar estas dos componentes, es que cada una de estas se puede implementar y modificar independientemente, teniendo en cuenta que la componente de control deben mantener la comunicación con la componente de datos mediante envío de paquetes y actualización de información.

* Componente de Datos

Esta componente es la encargada del transporte de paquetes entre dos LSR o entre un enrutador que se encuentra fuera del dominio de MPLS y que no posee etiquetas (LER). En esta componente se manejan dos tipos de bases de datos de etiquetas (Label Forwarding Table) y para los enrutadores de borde (LER) está la tabla de forwardeo IP tradicional de todo enrutador (Forwarding Information Base), donde la primera se utiliza para el transporte de paquetes que contienen etiquetas y la segunda lo que permite es transportar paquetes de datos desde o hacia dispositivos que no manejan etiquetas.

Así que la componente de datos se basa en el intercambio de etiquetas, es decir que cuando un paquete llega a la componente de datos, esta se encarga de examinar la información que la etiqueta del paquete contiene y busca en la tabla de envió para tomar la decisión de encaminamiento, es decir que busca para cada paquete la entrada y dirige el paquete desde el interfaz de entrada al de salida a través del correspondiente hardware de conmutación, según Rubiano y Urbano (2006).



Imagen N° 9: Componentes de control y Datos de un nodo

Fuente: Rubiano y Urbano (2006)

Antes de iniciar con la explicación del funcionamiento de esta tecnología, es importante conocer algunos términos que serán indispensables para su entendimiento.

2.2.11.- Arquitectura MPLS y calidad de servicio (QoS) en una red IP

Según Doménico y García (2011), la arquitectura MPLS nos provee de un circuito virtual o LSP a través de los diferentes nodos que conforman la red MPLS. Gracias a este tipo de funcionamiento, el circuito virtual creado provee de un trato igualitario a los diferentes tráficos que se envían bajo a un mismo túnel LSP bajo una etiqueta FEC en particular. Estudios relacionados a la calidad de servicio en diferentes escenarios son de interés actualmente dado que, a comparación con las demás arquitecturas, MPLS ofrece escalabilidad, simplicidad, velocidad, entre otros. Las facilidades que ofrece esta arquitectura para la implementación de calidad de servicio son las que se explicaran a continuación:

* Velocidad frente al esquema de enrutamiento IP. En efecto, la conmutación de etiquetas es más rápida y eficiente en primer lugar porque se produce en la capa inmediatamente anterior a la capa de red. En segundo lugar, el envió o forwarding se hace en base a un campo específico de la cabecera de la tecnología de conmutación.
* Procesamiento más rápido de la cabecera MPLS. En el caso particular de MPLS solo se necesita tener en cuenta los campos Label, TTL para el envió de tráfico y en ciertos casos dependiendo del tipo de SLA que se haga, los campos correspondientes a Stacking para envió interdominio y el campo experimental EXP para implementar prioridades.
* Facilidad de implementación. Cualquiera de las formas que existe para el correcto funcionamiento de la arquitectura MPLS requiere de poca señalización entre los nodos. Las contramedidas que se pueden tomar en caso de fallas, protocolos de enrutamiento, entre otras tecnologías de capas superiores y/o inferiores no afecta el funcionamiento de la arquitectura, es decir, para cualquier cambio en cualquier capa la arquitectura se amolda a los posibles cambios sin la intervención del administrador de la red MPLS.
* Adaptabilidad frente a la capa de red como a la capa de enlace. La arquitectura MPLS se localiza entre la capa de red y la capa de enlace, se vale de la conmutación para el envió del tráfico y de los protocolos de enrutamiento para la creación de la tablas de conmutación y de rutas alternas para diferentes fines.
* El cambio que se da en el software y no en el hardware. Los nodos que conformarían la red MPLS necesitan solo los procesos correspondientes a los manejos de MPLS independientemente de las tecnologías y funcionamiento de la capa de enlace y la capa de red. Para equipos actuales basta con una actualización al sistema operativo de los enrutador que conforman la backbone.
* Permite la implementación de Ingeniería de tráfico. Gracias a nuevos protocolos de enrutamiento como a mejoras a otros protocolos de capas superiores, MPLS tiene la capacidad de cambiar dinámicamente de ruta. Las nuevas rutas pueden ser generadas por protocolos de capa de red destinados a crear la tabla de enrutamiento bajo ciertas métricas, así también se aplicaran ciertas políticas en estos mismos protocolos para una mejor evaluación de los recursos de la red.
* Reserva de recurso de intradominio MPLS. Gracia al túnel LSP que se crea para el envió de los tráficos correspondientes, se asegura que la red pueda soportar los requerimientos solicitados dado que si fuese el caso contrario, el túnel no puede establecerse.

2.3.- Términos Básicos.

* ATM: "Modo de transferencia asíncrono", es una tecnología de red de alta velocidad que soporta el transporte de señales de voz, datos y vídeo a través de una sola corriente. (McQuerry y otros; 2001).
* Calidad de servicio (QoS): es un mecanismo de control que puede dar diferente prioridad a distintos usuarios o flujos de datos, o garantizar un determinado nivel de rendimiento a un flujo de datos de acuerdo con solicitudes del programa de aplicación. (Cisco; 2011).
* Dirección IP: Número exclusivo que utilizan los dispositivos a fin de identificar y comunicarse entre ellos en una red de computadoras utilizando el estándar de protocolo de internet (IP). (Cisco; 2011).
* IETF (Internet Engineering Task Force): es una gran comunidad internacional abierta de diseñadores, operadores, vendedores, e investigadores interesados ​​en la evolución de la arquitectura de Internet y el buen funcionamiento de la Internet. (IETF; 2011).
* Paquetes: agrupación lógica de información que incluye un encabezado que contiene información de control y (generalmente) datos de usuario. (Cisco; 2011).
* Protocolo: Es un conjunto de reglas de comunicaciones entre dispositivos (computadoras, teléfonos, enrutadores, switchs, etc). Los protocolos gobiernan el **formato, sincronización, secuencia** y**control de errores**. (Eveliux; 2011).

**CAPÍTULO III**

**CAPÍTULO III**

**MARCO METODOLÓGICO**

1.- Tipo de investigación

Según el grado de profundidad con el que se aborda los objetivos, el nivel de la investigación y la estrategia empleada por el investigador, la presente investigación se clasifica en exploratoria-descriptiva. (Arias; 1999).

Se puede decir que esta clasificación usa como criterio lo que se pretende con la investigación, sea explorar un área no estudiada antes y describir una situación.

“La investigación descriptiva busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice” Hernández y otros (2003).

Para el análisis de esta investigación se establecieron diferentes pruebas repetitivas que permitieron describir o dar a conocer las propiedades, características y rasgos de IPv6 conjuntamente con MPLS.

Por su parte, “la investigación exploratoria se efectúa normalmente cuando el objetivo es examinar un tema o un problema de investigación poco estudiado, del cual tienen muchas dudas o no se ha abordado antes” Hernández y otros (2003).

En el Área de Redes y Telecomunicaciones existen temas que ameritan ser estudiados e investigados, en este caso se trabajó con el nuevo protocolo de internet Versión 6 con MPLS debido a que su implementación ha sido poca, y con respecto a ipv6 existen dudas sobre su efectividad al resolver las limitaciones nativas que se tienen con IPv4.

2.- Diseño del Investigación

“El diseño de investigación es la estrategia general que adopta el investigador para responder al problema planteado (Arias; 1999)”.

Su objetivo es proporcionar un modelo de verificación que permita contrastar hechos con teorías, y su forma es la de una estrategia o plan general que determina las operaciones necesarias para hacerla. (Sabino; 2000).

El Diseño de esta Investigación ha sido planteado de forma experimental debido a la manipulación de la variable independiente (Protocolo IP =IPv4 e Ipv6) para medir su rendimiento con una variable dependiente (Rendimiento=Delay, Bitrate y % Paquetes perdidos), mediante una serie de pruebas sucesivas como modelo de verificación con el fin de describir de qué modo y porqué causa se produce una situación o acontecimiento particular.

3.- Técnicas e instrumentos de Recolección de Datos

Para efectuar el desarrollo de la presente Investigación se hizo 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 e 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 medio de variables que al obtenerlos, ayudaron a la investigación a determinar la influencia del protocolo IPv6 en redes basadas en MPLS (Multiprotocol Label Switching).

4.- Metodología Utilizada

Para determinar cómo influye el protocolo IPv6 en redes basadas en MPLS (Multiprotocol Label Switching), la investigación se rigió por una variación de la metodología experimental planteada en Bisquerra (2000) donde explica que “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 determinarán como se recogen y analizan los datos, lo cual llevará a las conclusiones”. Esta investigación se llevó a cabo, a través de las siguientes fases:

Fase 1. Recopilación de Información:

Esta fase se basó en la recopilación teórica utilizando fuentes periódicas, electrónicas, publicaciones científicas, libros entre otras. Entre los aspectos a considerar, se estudiará la implementación de IPv6 en redes WAN, proceso de etiquetado en redes MPLS, análisis y comparación de métodos de medición de tráfico, entre otros.

Fase 2. Definición de pruebas y diseño e implementación de topologías y ambientes de prueba:

Para esta fase se realizó el diseño de la topología en un ambiente controlado, donde se garantizó el uso de los servicios MPLS. Se dispuso físicamente de los equipos de enrutamiento, y se configuraron de acuerdo con las especificaciones de la investigación

Fase 3. Pruebas de medición y recopilación de información de las mismas:

En esta fase se realizaron las pruebas definidas en la fase anterior, el tipo de tráfico IP, las topologías que se desprendan de los resultados preliminares, y finalmente se organizaron y tabularon los datos obtenidos.

Fase 4. Análisis comparativo, tratamiento y análisis estadístico:

En esta última fase se analizaron comparativamente los resultados detectando diferencias básicas observables y finalmente se sometió a un tratamiento estadístico que permitió detectar las diferencias significativas en los diferentes casos, determinando causas y consecuencias para generar las conclusiones de la investigación.

5.- Herramientas Utilizadas

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

* Dispositivos:
* Dos Enrutadores Cisco 2800 equipados con IOS 12.4 (13r)T 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 MPLS en todas las pruebas.
* Dos Computadoras Lenovo con las siguientes características: Pentium (R) Dual-Core CPU, 2 GB de RAM, HHDD 120 GB.
* Dos cables de consola para enrutadores Cisco.
* Tres Cables seriales para enrutadores Cisco.
* Software:
* Sistema operativo Windows XP.
* Se utilizó un programa para acceder a la interfaz de línea de comando (CLI) del enrutador; el mismo es HyperTerminal.
* 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.
* Capturador de paquetes Wireshark versión 1.4.3, antes conocido como Ethereal, es un [analizador de protocolos](http://es.wikipedia.org/wiki/Analizador_de_protocolos) utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de [software](http://es.wikipedia.org/wiki/Software) y [protocolos](http://es.wikipedia.org/wiki/Protocolo).
* TFTP32 es un software para la transmisión de datos de un extremo a otro.
* Se usó el VLC VideoLAN para la transmisión de Video de un extremo a otro.

6.- Diseño del experimento

La presente investigación dio inicio con la Fase Uno, donde se investigó detalladamente sobre las variables independientes IPv4 e IPv6 con MPLS, las ventajas de IPv6 con respecto a IPv4, la configuración tanto de IPv4 con MPLS como IPv6 con MPLS, la búsqueda del sistema operativo de los enrutadores que soportaría simultáneamente Ipv6 con MPLS y los software que se utilizarían para realizar las pruebas.

Se continúo con la Fase Dos, donde se realizó el diseño de la Topología, luego se realizaron las conexiones físicas de los equipos de la siguiente manera:

* Se hizo la conexión de los tres enrutadores Cisco por medio de los tres cables seriales v35.
* Se conectaron los enrutadores uno y dos a las computadoras por medio de la FastEthernet con cables cruzados.
* Se utilizaron dos cables de consola para la configuración de los enrutadores.

Una vez establecidas todas las conexiones físicas y de forma correcta se procedió a configurar los enrutadores de la siguiente manera:

Para IPv4:

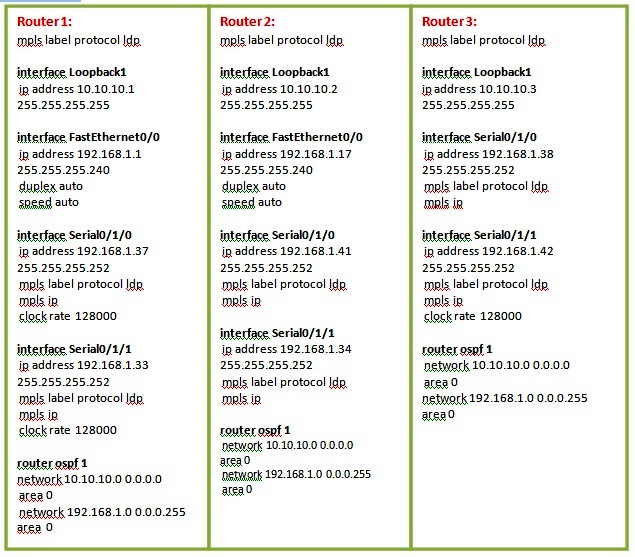


Imagen N° 10: Configuración IPv4

Fuente: Propia (2011)

Teniendo configurado los enrutadores se realizaron pruebas de conexión entre ellos por medio del comando Ping seguido de la dirección IP por ejemplo:

En el router 1 se realizó un ping a la dirección 192.168.1.34, obteniendo la respuesta de conexión esperada. Del mismo modo se realizó en el router 2, sólo que la dirección cambiaba a 192.168.1.33 así sucesivamente entre los enrutadores (R1-R2, R1-R3, R2-R1, R2-R3, R3-R1, R3-R2).

Ya configurado los enrutadores correctamente se procedió a la configuración de las computadoras asignándoles las siguientes direcciones IP:

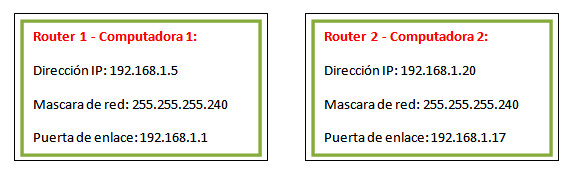


Imagen N° 11: Configuración de las computadoras IPv4

Fuente: Propia (2011)

En el mismo orden de ideas, se realizaron pruebas de conexión pero ahora de un host a otro, esta vez se ejecutaba el símbolo de sistema (Consola) y se ejecutaba la instrucción ping seguido de la dirección IP del otro computador.

Para IPv6:

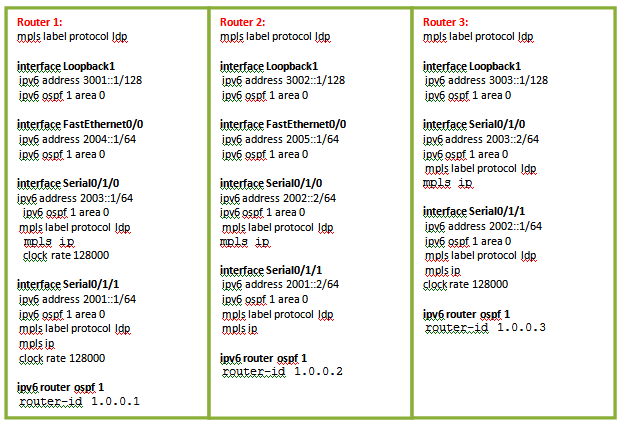


Imagen N° 12: Configuración IPv6

Fuente: Propia (2011)

De la misma manera que en IPv4, una vez configurado los enrutadores se realizaron pruebas de conexión entre los enrutadores por medio del comando ping de la siguiente manera:

En el Router 1 se coloco pin 2001::2 obteniendo la respuesta de conexión esperada, del mismo modo se realizo en el router 2, solo que la dirección cambiaba a 2001::1 así sucesivamente entre los enrutadores (R1-R2, R1-R3, R2-R1, R2-R3, R3-R1, R3-R2).

Ya configurados los enrutadores se continuaba con la configuración de las computadoras asignándoles las siguientes direcciones IP:

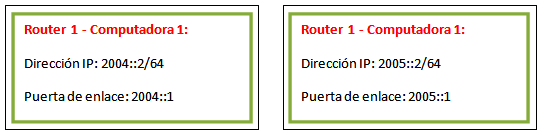


Imagen N° 13: Configuración de las computadoras IPv6

Fuente: Propia (2011)

De manera semejante a Ipv4 se realizaron pruebas de conexión entre las computadoras, ejecutando el símbolo de sistema (consola) y se ejecutaba la instrucción ping seguido de la dirección IP de otro computador.

En ese mismo sentido, el ambiente de pruebas y el direccionamiento de la red quedaron establecidos de la siguiente manera:

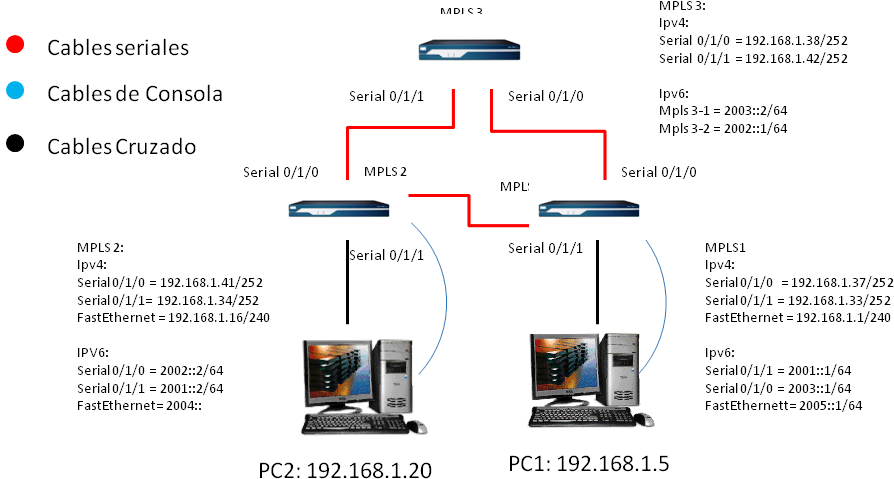


Imagen N° 14: Ambiente de Pruebas

Fuente: Propia (2011)

La **fase Tres,** dio inicio realizando pruebas con el programa IPERF, que se utilizó para medir el ancho de banda real de la red, mostrando como resultado 124kbits/s como se puede observar en la imagen siguiente:



Imagen N° 15: Pruebas con IPERF para detectar el Ancho de banda

Fuente: IPERF (2011)

Una vez teniendo conocimiento del ancho de banda real de la red, se necesitaba el tamaño y número de paquetes que se transmitiría por el Ditg.

Para calcular el tamaño y número de paquetes, se realizaron unas las operaciones que se explican a continuación:

1.- El ancho de Banda se convirtió a bytes debido que el DITG maneja el tamaño de los paquetes en bytes.

124 kbits 🡪 15500 bytes

Fórmula para convertir Kbits 🡪 Bytes

124 kbits \* 1000 = 124000 bits

124000 / 8 = 15500 bytes

2.- Se estipuló el tamaño de los paquetes

Tamaño del Paquete 🡪 512 bytes (valor por defecto del ditg)

3.- Para calcular el número de paquetes máximo que se podía transmitir, se dividió el ancho de banda entre el tamaño de los paquetes.

15500/512 = 30 paquetes.

Las pruebas se realizaron por un tiempo de 3 minutos debido a que después de ese tiempo el proceso no se alteraba. Luego fueron convertidos a 180.000 milisegundos y el tipo de protocolo que se utilizó fue UDP.

Sobre las bases de las consideraciones anteriores, los comandos utilizados en el Ditg para generar tráfico fueron los siguientes:

ITGSend: Es el componente emisor, este se encarga de enviar los paquetes hasta el receptor. Se utiliza de la siguiente manera:

ITGSend –a (Dirección Destino) –rp (puerto destino) –T (Tipo de Protocolo) –t (tiempo de duración) –C (Numero de paquetes) –c (tamaño del paquete) –l (nombre de la prueba)

ITGRecv: Es el componente Receptor, este se encarga de recibir los paquetes que el emisor envía. Se utiliza de la siguiente manera:

ITGRecv -l (nombre de la prueba)

ITGDec: Es el Decodificador, este se encarga de procesar la información que envió el emisor y recibió el receptor. Se utiliza de la siguiente manera.

ITGDec (nombre de la prueba)

Los comandos fueron ejecutados en el siguiente orden:

1.- Se ejecuta el comando ITGRecv (Imagen N° 16), cuando se muestra el mensaje Press Ctrl-C to terminate, enseguida se ejecuta el comando ITGSend (Imagen N° 17).

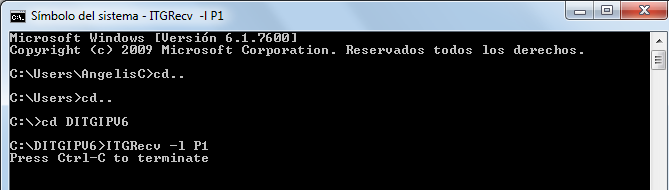


Imagen N° 16: Comando para el servidor en DITG

Fuente: DITG (2011)

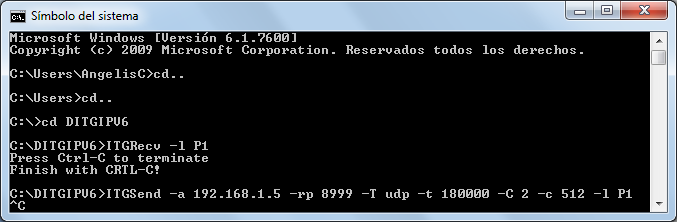


Imagen N° 17: Comando para el servidor en DITG

Fuente: DITG (2011)

2.- Pasado lo 3 minutos, el servidor muestra un mensaje de que ha finalizado la prueba, luego se ejecuta el comando ITGDec (Imagen N° 18) para visualizar los resultados.

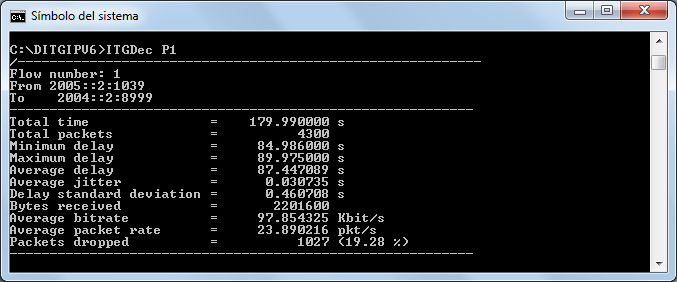


Imagen N° 18: Comando para visualizar el resultado en el DITG

Fuente: DITG (2011)

Ante el escenario planteado, se realizaron pruebas variando los parámetros del número de paquetes para generar tráfico de congestión al 0%, 50% y 100% con Ipv4 e Ipv6.

* Con el Tráfico al 0% se manejaron los parámetros de la siguiente manera:

Tamaño del paquete: 512,

Numero de paquetes: 2 paquetes

Tipo de protocolo: UDP

Tiempo: 180000

ITGSend –a 192.168.1.5 –rp 8999 –T udp – t 180000 –C 2 –c 512 –l P1

ITGRecv –l P1

ITGDec P1

Para Saber el total de paquetes que debe recibir el receptor, Multiplicamos el número de paquetes por el tiempo de la prueba en segundos:

2 x 180= 360 paquetes

* Con el Tráfico al 50% se manejaron los parámetros de la siguiente manera:

Tamaño del paquete: 512,

Numero de paquetes: 15 paquetes

Tipo de protocolo: UDP

Tiempo: 180000

ITGSend –a 192.168.1.5 –rp 8999 –T udp – t 180000 –C 15 –c 512 –l P1

ITGRecv –l P1

ITGDec P1

Total de paquetes que debe recibir 15 x 180= 2700 paquetes

* Con el Tráfico al 100% se manejaron los parámetros de la siguiente manera:

Tamaño del paquete: 512,

Numero de paquetes: 30 paquetes

Tipo de protocolo: UDP

Tiempo: 180000

ITGSend –a 192.168.1.5 –rp 8999 –T udp – t 180000 –C 30 –c 512 –l P1

ITGRecv –l P1

ITGDec P1

Total de paquetes que debe recibir 30 x 180= 5400 paquetes

Para el envío de Data se utilizó TFTP que es un protocolo de transferencia de datos que funciona de la siguiente manera:

1.- En un computador se ejecuta el Tftp Client donde se coloca la dirección IP del otro computador (host), el número de puerto (port), la dirección del archivo que se va a enviar (Local File), y el tamaño de los bloques (Block Size). Ejemplo:

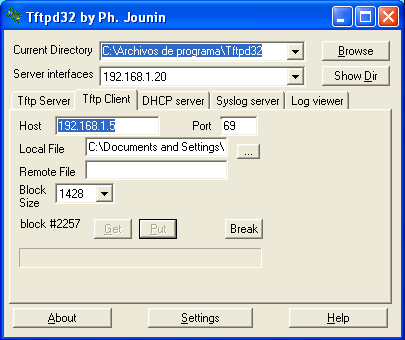


Imagen N° 19: TFTP Cliente

Fuente: TFTP32 (2011)

2.- En el Otro computador solo se ejecuta el Tftp Server Ejemplo:

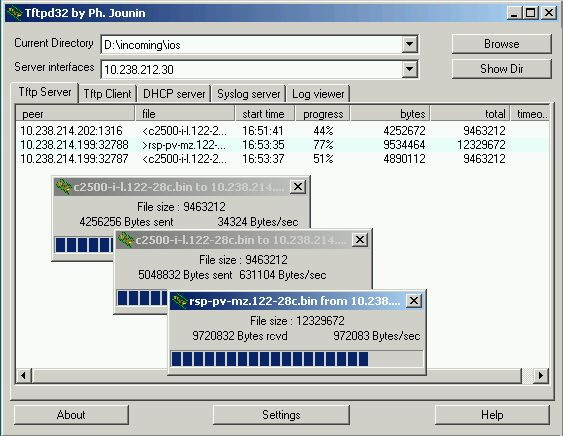


Imagen N° 20: TFTP Servidor

Fuente: TFTP32 (2011)

3.- Cuando se encuentren listos el Cliente y el Servidor, se oprime PUT y empieza la transmisión del archivo de un host a otro.

Ahora bien, para la captura del tráfico se utilizo el Wireshark ya que el uso de esta es apropiado para obtener los distintos indicadores (%paquetes Perdidos, delay, bitrate) debido a que ni el TFTP ni el VideoLAN proporciona estos valores.

El Wireshark se ejecuta en las dos computadoras en el Cliente para capturar el número de paquetes que se enviaban y en el servidor para saber el número de paquetes que llegaban, el bitrate, delay entre otros valores. También proporcionó la facilidad de filtrar el tráfico que requería verse (TFTP o VideoLAN) colocando las direcciones IP de origen, IP destino y el puerto de destino.

Para ver el tráfico de paquetes de TFTP en Ipv4, se tiene:

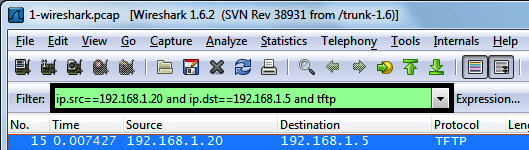


Imagen N° 21: Filtro del Wireshark para el tráfico generado por el TFTP en IPv4

Fuente: Wireshark (2011)

Para ver el tráfico de paquetes de TFTP en Ipv6:

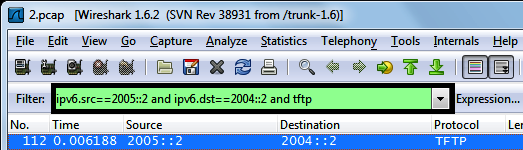


Imagen N° 22: Filtro del Wireshark para el tráfico generado por el TFTP en IPv6

Fuente: Wireshark (2011)

Para ver el tráfico de paquetes de VideoLAN en Ipv4, se tiene:

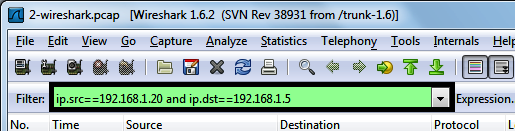


Imagen N° 23: Filtro de wireshark para el tráfico generado por el VideoLan en IPv4

Fuente: Wireshark (2011)

Para ver el tráfico de Paquetes de VideoLAN en Ipv6:

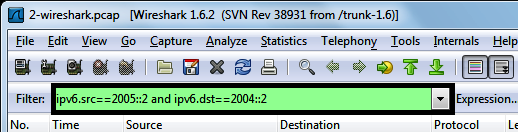


Imagen N° 24: Filtro de wireshark para el tráfico generado por el VideoLan en IPv6

Fuente: Wireshark (2011)

Para el envío de video como se ha dicho anteriormente se utilizó VideoLAN, que es una solución de software completa para transmisión de vídeo y se utilizó de la siguiente manera:

1.- Se ejecuta VideoLan en ambas Computadoras

2.- Se establece una como Receptor: Medio, Abrir volcado de Red e introducir URL (rtp://@[DireccionIP]:1234).

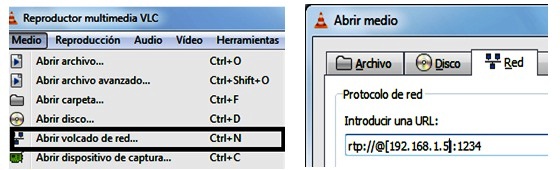


Imagen N° 25: Configuración de VideoLAN en el computador receptor

Fuente: VideoLAN (2011)

3.- Y el otro computador como Emisor: Se presiono Medio, Emitir, Añadir luego emitir nuevamente.

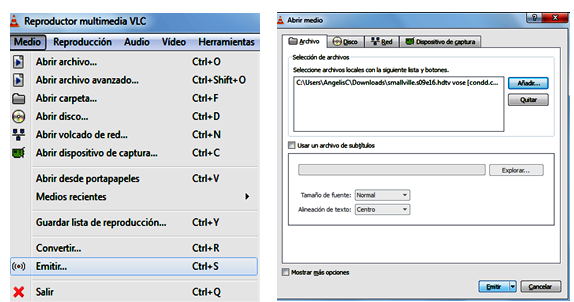


Imagen N° 26: Configuración de VideoLAN en el computador emisor

Fuente: VideoLAN (2011)

4.- Luego se avanza hasta la pestaña opciones y se selecciona el protocolo RTP para emitir (Imagen N° 27) posteriormente se oprime añadir para colocar la dirección y el puerto de la computadora Destino (Imagen N° 28) y continúa en siguiente.

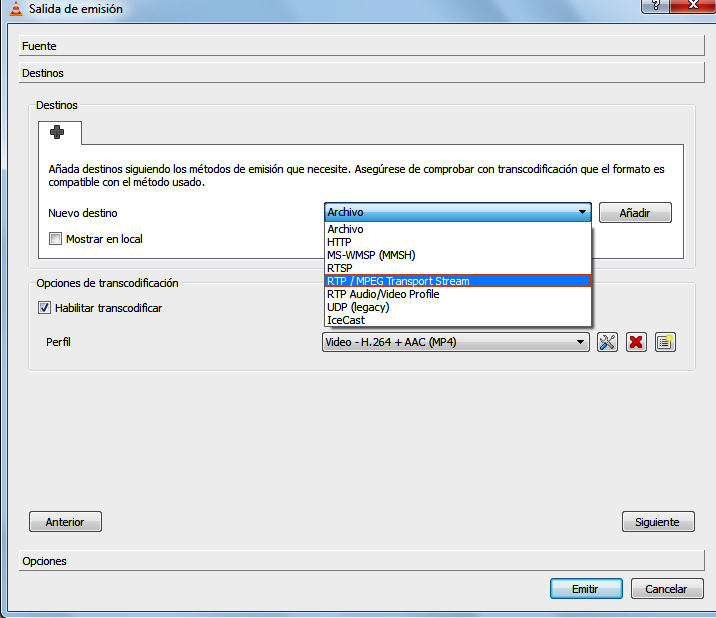


Imagen N° 27: Elección del protocolo RTP

Fuente: VideoLAN (2011)

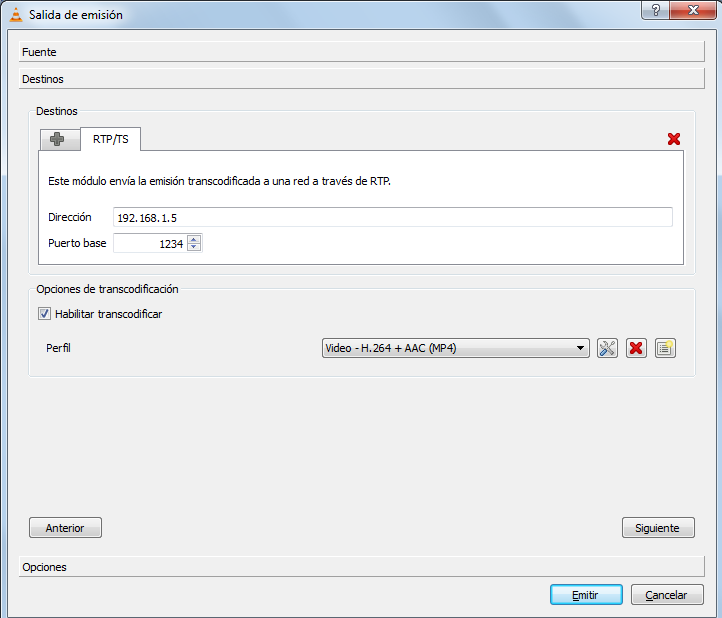


Imagen N° 28: Asignación de la dirección del receptor, el puerto y el tipo de video

Fuente: VideoLAN (2011)

5.- Finalmente, se presiona el botón emitir para iniciar la transmisión de Video.

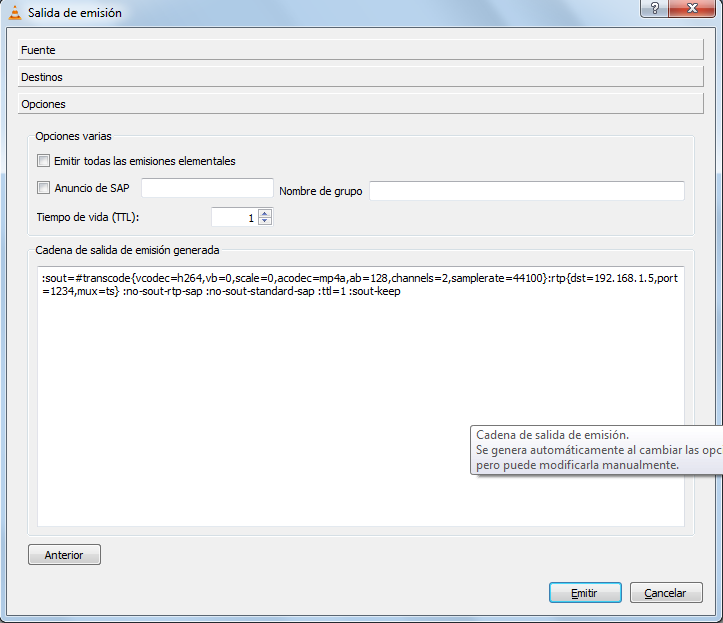


Imagen N° 29: Último paso para empezar a emitir

Fuente: VideoLan (2011)

Hecha todas las consideraciones anteriores se realizaron pruebas de Datos y video; para cada caso se realizaron tres (3) repeticiones, para los tres tipos de tráficos 0%, 50% y 100%, esto fue necesario para conseguir un análisis representativo en cada protocolo, de tal forma que se pudiera 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.

Se realizó un total de 36 pruebas: 18 pruebas para cada protocolo, basadas en 2 tipos de ambientes que consistían en transmisión de data y video.

Para el desarrollo de las pruebas se trabajó como Cliente la computadora dos (2) y como Servidor la computadora (1), (ver Imagen N° 14).

Pruebas de Datos:

Para las pruebas de Datos se utilizaron los siguientes Software DITG, TFTP32 y Wireshark en Ipv4 y en Ipv6.

1.- Se ejecutó el wireshark en las dos computadoras con sus respectivos filtros para la captura de tráfico de los paquetes transmitidos por TFTP.

2.- Se abrió el TFTP en el computador cliente y el TFTP Server en el computador servidor.

3.- Se abrió el sistema de símbolos (Consola) en los dos computadores, en el cliente se configuró los comandos de ITGSend y en el Servidor los comandos de ITGRecv.

4.- Se ejecuto ITGRecv enseguida ITGSend, luego en el TFTP Cliente se oprimió PUT y el wireshark tanto el de cliente como el del servidor comenzó a capturar tráfico.

5.- Luego de 3 minutos en el DITG servidor se oprimió Ctrl-c y en el wireshark cliente y servidor se oprimió stop al mismo tiempo para detener la captura.

6.- Luego se ejecutó ITGDec para guardar los resultados y en el wireshark cliente y servidor se oprimía Statistics, Protocol Hierarchy (Imagen N° 30) para observar los valores y proceder a guardar los resultados.

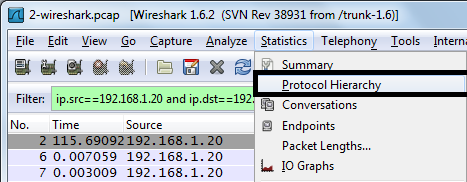


Imagen N° 30: Paso para observar los resultados

Fuente: Wireshark (2011)

Ahora bien, para conocer la cantidad de Paquetes que se envió y la cantidad de paquetes que se perdió, se restaba el número de paquetes que había enviado el Cliente y el número de paquetes que había recibido el servidor y para el bitrate simplemente nos fijamos en la columna Mbits/s que es la cantidad de Megabits por segundos que se enviaron durante el tiempo de captura de la prueba.

Wireshark Cliente:

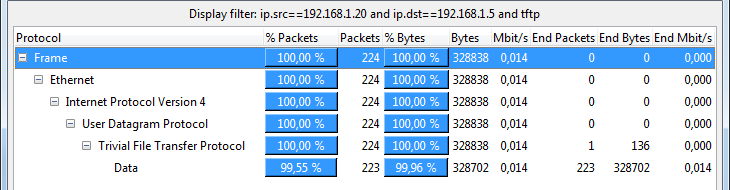


Imagen N° 31: Resultado de la captura del cliente

Fuente: Wireshark (2011)

Wireshark servidor:

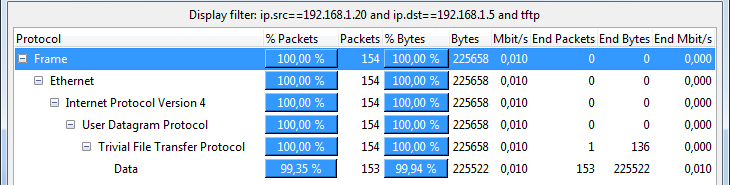


Imagen N° 32: Resultado de la captura del servidor

Fuente: Wireshark (2011)

Paq. Perdidos = Paq. Enviados - Paq. Recibidos

Paq. Perdidos = 224 - 154

Paq. Perdidos = 70

Para calcular el porcentaje de los paquetes perdidos, se utilizó la siguiente fórmula:

% Paq. Perdidos = (Paq. Perdidos/Paq. Enviados) \* 100

% Paq. Perdidos = (70 / 224) \* 100

% Paq. Perdidos = 31,25%

Para calcular el Bitrate de la prueba debemos convertir los Mbits/s que nos da el Wireshark en Kbits/s

Bitrate = 0,010 Mbits \* 1000

Bitrate = 10 Kbits/s.

7.- Se procede a guardar la prueba de la siguiente manera para luego hallar el Delay: file, export, file se abrirá la siguiente ventana (ver Imagen N° 33).

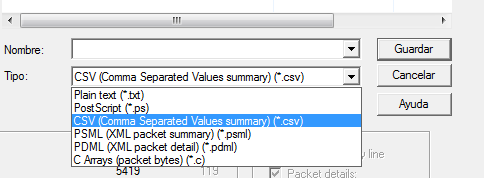


Imagen N° 33: Tipo de Archivo .CSV

Fuente: Wireshark (2011)

Se exporta el archivo a .CSV, luego lo abrimos en Excel y se mostrará el archivo. Para hallar el delay sombreamos la columna de time, en el menú de Excel seleccionamos fórmulas, autosuma y calculamos el promedio total (Imagen N° 34).

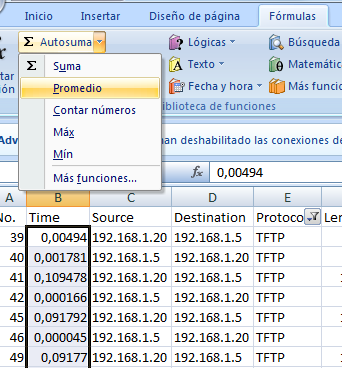


Imagen N° 34: Pasos para calcular el promedio

Fuente: Wireshark (2011)

Pruebas de Video:

Para las pruebas de Video se utilizaron los siguientes Software DITG, VideoLAN y Wireshark en Ipv4 y en Ipv6.

1.- Se ejecutó el wireshark en las dos computadoras con sus respectivos filtros para la captura de tráfico de video.

2.- Se abrió el VideoLan en ambas computadoras, en la computadora cliente se emitió el video y en la computadora servidor se abría el Volcado de red para que fuera el receptor.

3.- Se abrió el sistema de símbolos (Consola) en los dos computadores, en el cliente se configuraron los comandos de ITGSend y en el Servidor los comandos de ITGRecv.

4.- Se ejecutó ITGRecv enseguida ITGSend, luego en la computadora Cliente se oprimió emitir del VideoLan y de una vez en la computadora servidor se oprimió reproducir del VideoLan.

5.- Pasado los 3 minutos en el DITG servidor se oprimia Ctrl-c y en el wireshark cliente y servidor se oprimió stop al mismo tiempo para detener la captura.

6.- Posteriormente se ejecutó ITGDec para poder guardar los resultados, en el wireshark se oprimía Statistics, Protocol Hierarchy (Imagen N° 30) para calcular el número y el porcentaje de paquetes perdidos.

7.- Posteriormente para obtener los indicadores, se tuvo primero que decodificar los paquetes de video en paquetes de Protocolo RTP para poder aplicar el analizador de flujo RTP de Wireshark, de la siguiente manera:

7.1.- Se selecciona un paquete del flujo capturado, en el menú se elije la opción analize, luego decode as, se elige el puerto 1234 y el protocolo a convertir RTP.

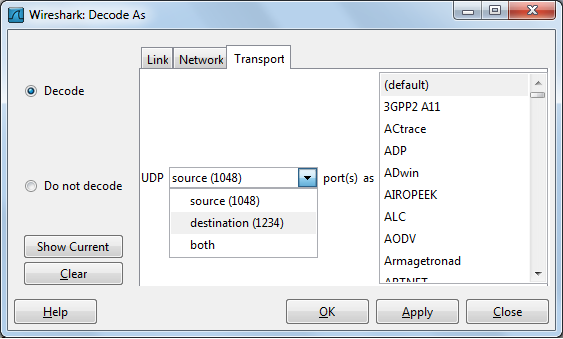


Imagen N° 35: Decodificación para el protocolo RTP

Fuente: Wireshark (2011)

7.2.- Luego se utiliza el analizador RTP oprimiendo en Menu Telephony, RTP, Stream Analysis para que mostraran el Delay y bitrate de cada paquete (Imagen N° 36).

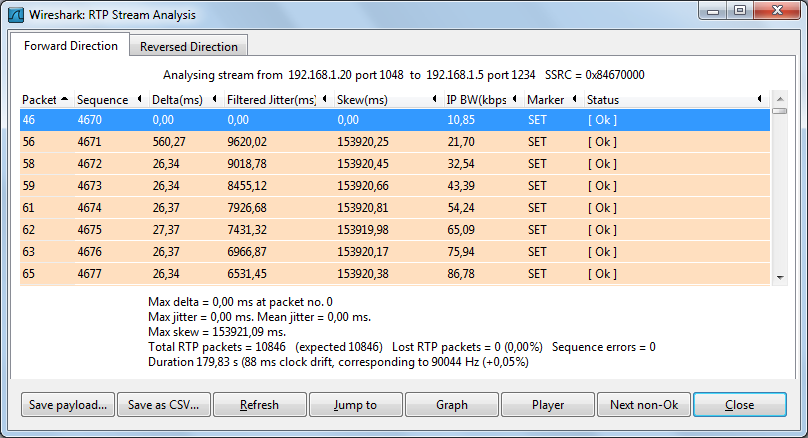


Imagen N° 36: Analizador del RTP

Fuente: Wireshark (2011)

7.3.- Luego, se exporta todo el flujo hacia un archivo CSV donde posteriormente se abre en Excel para calcular el Delay y bitrate (Imagen N° 34), sombreando las columnas y en el menú de Excel seleccionamos fórmulas, autosuma y calculamos el promedio total (Imagen N° 33).

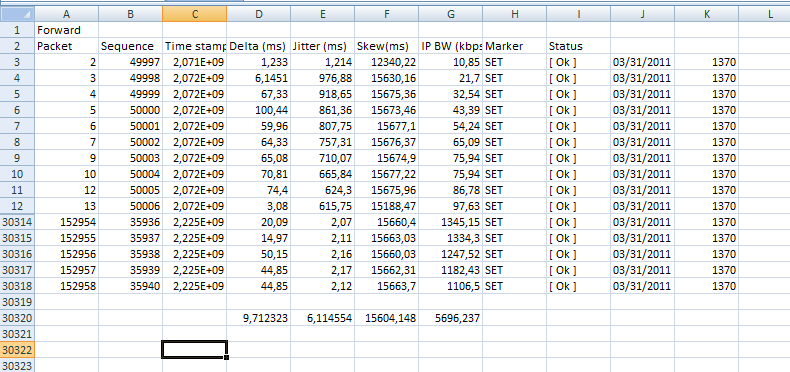


Imagen N° 37: Resultado de la captura de RTP usando Excel

Fuente: Wireshark (2011)

8.- Por último se procede a guardar los valores obtenidos como (% de Paquetes Perdidos, Delay y Bitrate) de cada flujo.

Para Finalizar, en la fase cuatro se utilizó el programa estadístico SPSS (Statistical Package for the Social Sciences) para el análisis de la significancia de las diferencias observadas entre los dos protocolos (Ipv4 e Ipv6).

Como modelo estadístico se aplicó el siguiente:

Antes es importante explicar que se utilizó como variables independientes se encuentra conformada por los protocolos (IPv4 e IPv6) y como variable dependiente las integran el rendimiento de la red (Delay, Bitrate y % paquetes perdidos).

yij = µ + αi + εij

Donde

αi = variable independiente

yij = variable dependiente

**CAPÍTULO IV**

**CAPÍTULO IV**

**ANÁLISIS Y DISCUSIÓN 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 de las pruebas descritas en el capítulo anterior, según el protocolo usado y el tráfico de congestión.

Pruebas IPv4/IPv6 con el tráfico 0% enviando datos:

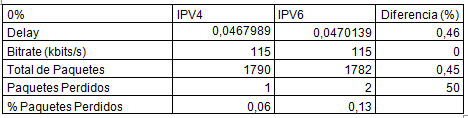
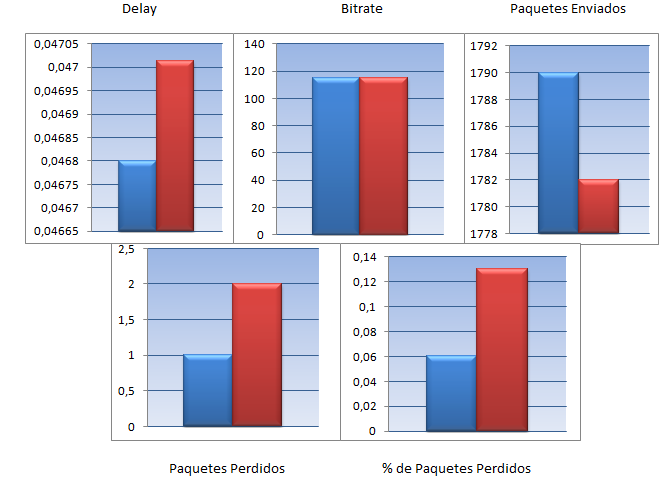


Tabla N° 1: Tráfico 0% enviando Datos

Fuente: Propia (2011)

Gráficos: IPv4 IPv6



Grafica N° 1: Tráfico 0% enviando Datos

Fuente: Propia (2011)

Para la siguiente prueba se generó tráfico del 0% enviando datos, se observó que IPv4 e IPv6 tuvieron comportamientos similares en la red; IPv4 obtuvo una menor latencia (0,46%) pero en el bitrate ambos arrojaron lo mismo valores. En cuanto a la transmisión de paquetes, IPv4 obtuvo un mejor comportamiento por cuanto logro un mayor envío de paquetes con un porcentaje de diferencia de (0,45%) y una menor pérdida de paquetes. Cabe destacar, que la diferencia entre los porcentajes de paquetes trasmitidos y paquetes perdidos fue mínima.

Pruebas IPv4/IPv6 con el tráfico del 50% enviando datos:

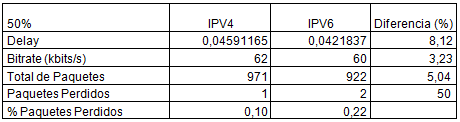
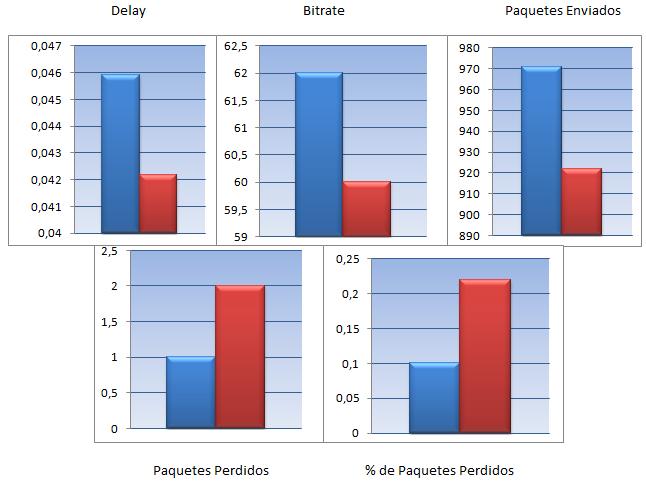


Tabla N° 2: Tráfico 50% enviando Datos

Fuente: Propia (2011)

Gráficos: IPv4 IPv6



Grafica N°2: Tráfico 50% enviando Datos

Fuente: Propia (2011)

En este caso se generó tráfico del 50% enviando datos, y se observó que IPv4 logro un mejor comportamiento en la red, debido que tuvo un mayor bitrate (3,23%). Por otra parte la latencia fue menor en IPv6 con una diferencia de 8,12%. En cuanto a la transmisión de paquetes y porcentaje de paquetes perdidos (50%) IPv4 alcanzó un mejor resultado aunque igual que la prueba del 0% la diferencia fue mínimo.

Pruebas IPv4/IPv6 con el tráfico del 100% enviando datos:

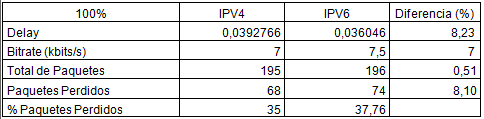
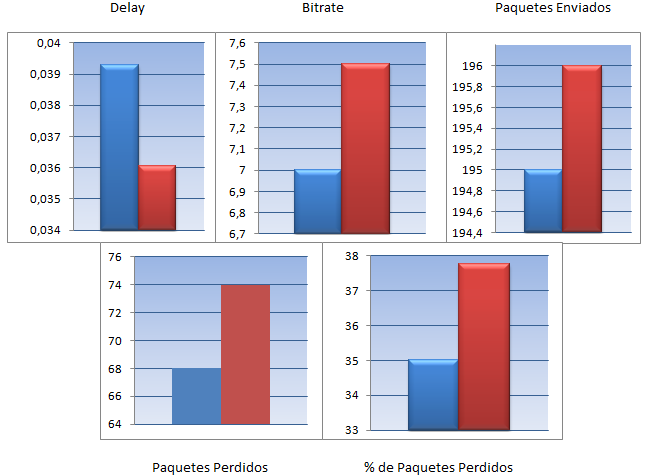


Tabla N° 3: Tráfico 100% enviando Datos

Fuente: Propia (2011)

Gráficos: IPv4 IPv6



Grafica N° 3: Tráfico 100% enviando Datos

Fuente: Propia (2011)

Para la siguiente prueba se generó tráfico al 100% enviando datos, hemos de observar que IPv6 tuvo un mejor comportamiento en la red debido a que su bitrate fue mayor (7%). En cuanto a la transmisión de paquetes IPv6 también tuvo un mejor comportamiento en comparación con IPv4 aunque el porcentaje de paquetes perdidos fue menor en Ipv4 pero no fue una diferencia abrupta.

Pruebas IPv4/IPv6 con el tráfico del 0% enviando video:

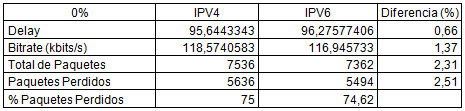
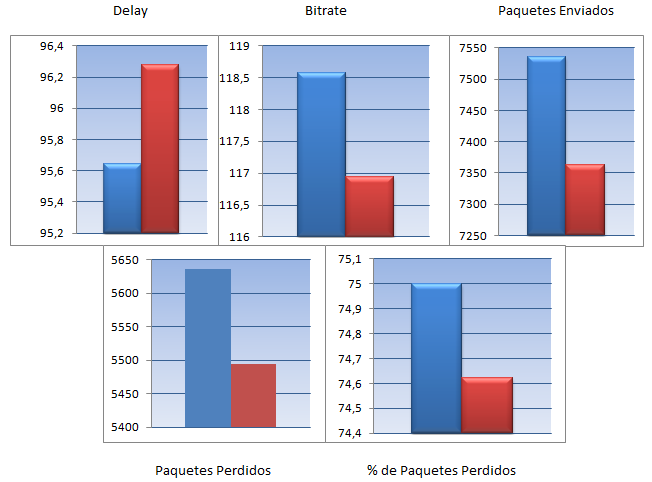


Tabla N° 4: Tráfico 0% enviando Video

Fuente: Propia (2011)

Gráficos: IPv4 IPv6



Grafica N° 4: Tráfico 0% enviando Video

Fuente: Propia (2011)

Para el siguiente caso se generó tráfico del 0% enviando video, pudiendo observar que IPv4 consiguió un mejor comportamiento en la red debió a que alcanzo una latencia menor (0,66) y un bitrate mayor (1,37%) comparado con IPv6. En cuanto a la transmisión de paquetes IPv4 envió más paquetes pero en el porcentaje de paquetes perdidos fue menor con IPv6 (74,62%).

Pruebas IPv4/IPv6 con el tráfico del 50% enviando video:

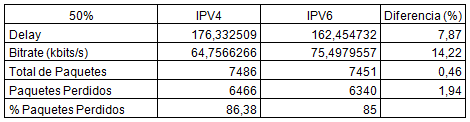
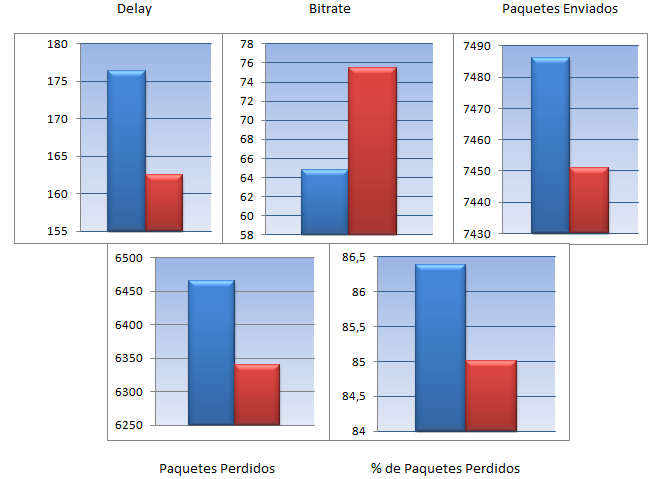


Tabla N° 5: Tráfico 50% enviando Video

Fuente: Propia (2011)

Gráficos: IPv4 IPv6



Grafica N° 5: Tráfico 50% enviando Video

Fuente: Propia (2011)

En el siguiente caso se generó tráfico del 50% enviando video, se observó que IPv6 logro un mejor comportamiento en la red debido que su latencia fue menor (7,87%), en cuanto a IPv4 su bitrate fue menor (14,22%) en comparación con el bitrate de IPv6. En cuanto a la transmisión de paquetes fue mayor en IPv4 pero con una diferencia minuciosa de 0,46% con IPv6, además que IPv6 se sostuvo en esta prueba con menor porcentaje de paquetes perdidos al igual que la pruebas del 0%.

Pruebas IPv4/IPv6 con el tráfico del 100% enviando video:

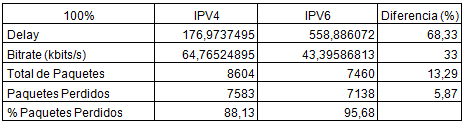
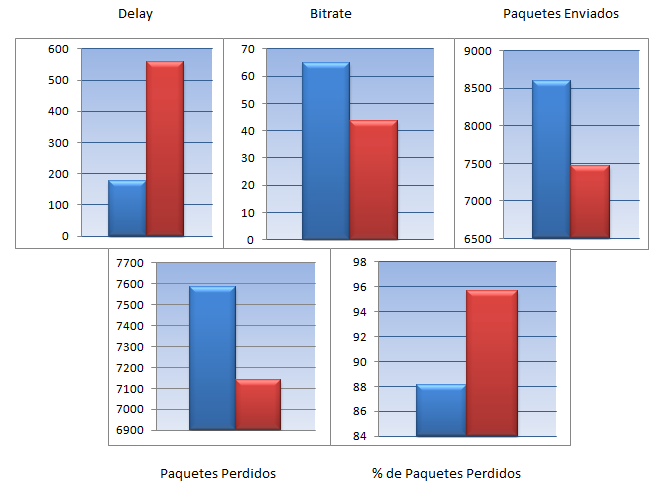


Tabla N° 6: Tráfico 100% enviando Video

Fuente: Propia (2011)

Gráficos: IPv4 IPv6



Grafica N° 6: Tráfico 100% enviando Video

Fuente: Propia (2011)

Para esta prueba se generó tráfico del 100% enviando video, alcanzando IPv4 un mejor comportamiento en la red debido a que su latencia (68,33%) fue menor que la de IPv6 y el bitrate fue mayor (33%), En cuanto a la transmisión de paquetes y en el porcentaje de paquetes perdidos IPv4 también tuvo un mejor comportamiento.

1.2.- Sustentación teórica del análisis de los resultados:

Como conclusión, se observó que IPv4 alcanzó un mejor comportamiento en la red comparado con IPv6, pese a que las diferencias fueron mínimas. Para el análisis de los resultados se consideró un normal comportamiento que el delay y los paquetes perdidos aumentarán y el bitrate disminuyera a medida que iba aumentando la congestión en la red, como lo indica García (2002).

Del mismo modo, en las pruebas de envió de datos se puede notar que el delay fue decreciendo a medida que aumentó la congestión en la red, este suceso se debe a que se activa un mecanismo de anti-cogestión en los enrutadores el cual causa el retardo de los paquetes del flujo generado, aseverando lo descrito por Gauna (2011). Esta acción se pudo apreciar en las pruebas de envío de datos de IPv4 e IPv6 con el tráfico del 0% y 50% que fue cuando se perdió un mínimo porcentaje de paquetes (0,22%) y el delay aumentó en comparación con el tráfico del 100% ya que el número de paquetes perdidos en este tráfico fue mayor y el delay menor. Esta escasa pérdida de paquetes se debió a que MPLS, aportó a la red un rendimiento mejorado y más robusto, donde pudo despachar paquetes mucho más rápido debido a la inteligencia con la que se traslado a los dispositivos frontera y a que puede reducir el número de saltos entre puntos, ayudando a evitar el descarte de paquetes por congestión y los retardos excesivos.

En las pruebas de video se pudo observar que hubo pérdida de paquetes en los tres tipos de tráfico, en parte esto se debe a que en el VideoLAN se utilizó RTP que a su vez funciona sobre el protocolo UDP.

Del mismo modo, en las pruebas de datos podemos notar que en el tráfico del 100% fue donde ocurrió una pérdida de paquetes un poco más notable si se compara con los tráficos 0% y 50%, esto en parte también sucede ya que el TFTP utiliza el protocolo UDP para la transmisión de datos. UDP (Protocolo de Datagramas de Usuario) se define como un protocolo orientado a la no conexión que se utiliza para conexiones que no precisan corrección de errores o continuidad en el flujo, Ortiz y otros (2002).

Cabe destacar que en las pruebas de video de IPv6 con tráfico de 0% y 100% se esperaba que hubiera una mayor pérdida de datos en comparación con IPv4, lo cual no sucedió y pudo haberse originado gracias a la simplificación de la cabecera, ya que de los 12 campos de la cabecera de IPv4 se ha pasado a 8 campos en IPv6. Este cambio permite a los routers procesar los paquetes mucho más rápido, mejorando así el rendimiento. (Millan, 2001).

Por otra parte Interiano y Montes (2005), definen la latencia (Delay) como el tiempo que una trama o paquete tarda en hacer el recorrido desde la estación o nodo origen hasta su destino.

De igual manera (Ferrer; 2007), explica que todo elemento o dispositivo que esté ubicado entre un cliente y un servidor, impondrá necesariamente un retardo a la información que se esté intercambiando entre estos dos dispositivos. Más adelante nos explica que existen diferentes tipos de retardos que pueden afectar su comportamiento, tales como la transmisión que depende de la velocidad de transmisión sobre la que viajan los paquetes de la red, el retardo del procesamiento que es causado por el tiempo que demora un dispositivo de conmutación de paquetes en enviar y recibir, este retardo depende del diseño del hardware del dispositivo y también de la velocidad de su procesador y memoria, por último el retardo de los sistemas de espera que se da cuando varios paquetes compiten por un único recurso o servicio. Debido a lo antes explicado, el comportamiento del Delay en la prueba de datos del 50% comparando IPv4 con IPv6 no se consideró un comportamiento normal y esto se pudo deber a que se vio afectado por estos diferentes tipos de retardo.

2.- Análisis estadístico de los resultados

Para realizar el análisis estadístico se utilizó el procedimiento “Análisis de varianza" ANOVA de un factor que 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. (Precisa Massart y col; 1997).

El procedimiento ANOVA de un factor genera un análisis de varianza de un factor para una variable dependiente cuantitativa respecto a una única variable de factor (la variable independiente). El resultado de este análisis 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 indica que tan parecida son las medias que se están comparando. A menor valor de F, menor diferencia entre las medias. Si la significancia (Sig) asociada al valor estadístico F es mayor al coeficiente de significancia (CoefS) 0.05 los resultados no son significativos. Si el valor de Fcal es menor al valor de F tabulado (Ftab)= 7,7086 se acepta la hipótesis nula, de lo contrario se rechaza y se acepta la hipótesis alternativa, así se confirma (Massart, 1997).

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

Datos (0%, 50% y 100%):

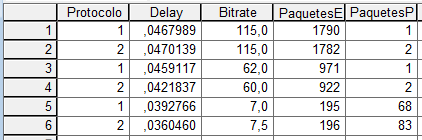
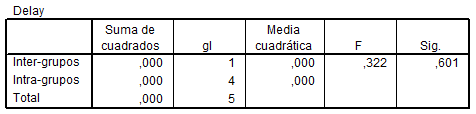


Tabla N° 7: Tabla de valores de los tráficos 0%, 50% y 100% enviando datos.

Protocolo 1: Protocolo IPv4; Protocolo 2: Protocolo IPv6

Fuente: Propia (2011)

**

*Tabla N° 8:* Tabla ANOVA Delay con el tráfico 0%, 50% y 100% enviando datos

Fuente: Propia (2011)

En el siguiente cuadro podemos observar que el valor estadístico de F es menor que el de Ftab (7,71) rechazando la hipótesis alternativa y aceptando la hipótesis nula, del mismo modo el coeficiente de significancia fue mayor que alfa (0,05) afirmando que no hubo diferencia significativa en el delay entre IPv4 e IPv6.

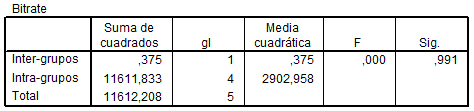


Tabla N° 9: Tabla ANOVA Bitrate con el tráfico 0%, 50% y 100% enviando datos

Fuente: Propia (2011)

Se puede observar en la Tabla N° 9 que el Fcal = 0 es menor que el f tabulado Ftab= 7, y la Sig= 0,991 es mayor al coeficiente de significancia CoefS= 0,05 afirmando que no hubo diferencia significativa entre el Bitrate de IPv4 y el de Ipv6.

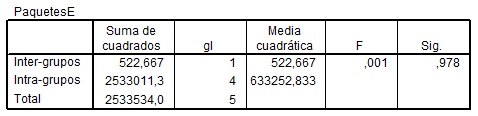


Tabla N° 10: Tabla ANOVA PaquetesE con tráfico 0%, 50% y 100% enviando datos

Fuente: Propia (2011)

En los paquetes enviados no hubo diferencia significativa entre IPv4 e IPv6 ya que la Sig= 0,978 fue mucho mayor que el CoefS= 0,05 y el Fcal= 0,001 también fue mucho menor que (Ftab)= 7,71 afirmando la hipótesis nula (Tabla N° 10).

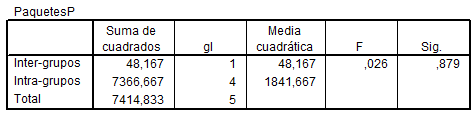


Tabla N° 11: Tabla ANOVA PaquetesP con tráfico 0%, 50% y 100% enviando datos

Fuente: Propia (2011)

De la Tabla N° 11 se observa que el Fcal fue menor que el Ftab (0,26<7,71) y la Sig fue mayor que el CoefS (0,879>0,05) rechazando así la hipótesis alternativa y afirmando que la diferencia entre estos dos protocolos (IPv4 e IPv6) no es significativa.

Video (0%, 50% y 100%):

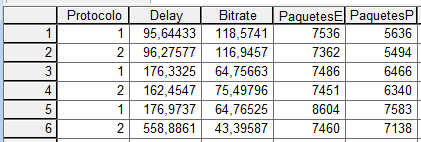
**

Tabla N° 12: Tabla de valores de los tráficos 0%, 50% y 100% enviando video.

Protocolo 1: Protocolo IPv4; Protocolo 2: Protocolo IPv6

Fuente: Propia (2011)

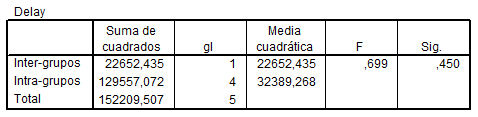


Tabla N° 13: Tabla ANOVA Delay con tráfico 0%, 50% y 100% enviando video

Fuente: Propia (2011)

En la Tabla N° 13 se acepta la hipótesis nula afirmando que la diferencia entre IPv4 e IPv6 no es significativa debido a que el F= 0,699 es menor que el Fcal= 7,71 y que la Sig= 0,450 es mayor que el CoefS= 0,05 rechazando así la hipótesis alternativa.

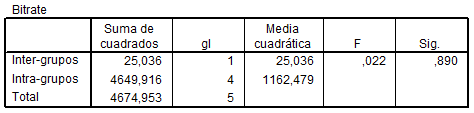


Tabla N° 14: Tabla ANOVA Bitrate con tráfico 0%, 50% y 100% enviando video

Fuente: Propia (2011)

Para el indicador bitrate la Sig= 0,890 fue mayor que el CoefS= 0,05 y F= 0,022 fue menor a Fcal= 7,71 rechazando la hipótesis alternativa y afirmando la hipótesis nula de tal manera que la diferencia entre IPv6 e IPv4 es insignificante (Tabla N° 14).

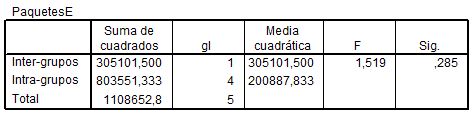
**

Tabla N° 15: Tabla ANOVA PaquetesE con tráfico 0%, 50% y 100% enviando video

Fuente: Propia (2011)

De la Tabla N° 15 se observa que para este caso también se rechaza la hipótesis alternativa debido a que la Sig=0,285 es mayor que el CoefS= 0,05 y que el Fcal= 7,71 es mayor que F= 1,519 afirmando así la hipótesis nula y que la diferencia entre los protocolos no tiene significancia.

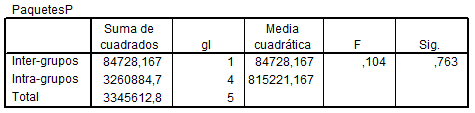


Tabla N° 16: Tabla ANOVA PaquetesP con tráfico 0%, 50% y 100% enviando video

Fuente: Propia (2011)

Con respecto a la Tabla N° 16 se acepta la hipótesis nula, rechazando la hipótesis alternativa debido a que el F y Sig son menor (0,104<7,71) y mayor (0,763>0,05) respectivamente afirmando así que la diferencia entre IPv4 e IPv6 no fueron significativa.

En conclusión, en todos los ambientes de pruebas (Datos y Video) se pudo observar que igual que el indicador anterior lo valores arrojado por F son menores que Ftab (7,71) rechazando la hipótesis alternativa y aceptando la hipótesis nula, en efecto todo los coeficientes de significancia fueron mayores que alfa afirmando que no hubo diferencia significativa entre IPv4 e IPv6.

**CONCLUSIONES**

1.- Se concluye que IPv6 obtuvo un comportamiento muy similar a IPv4, con diferencias nada significativas, y que aunque el desempeño de IPv6 fue un poco menor se debe tener en cuenta que es un protocolo nuevo y se encuentra en etapa de maduración, por lo que es previsible que su desempeño mejore en el tiempo.

2.- Se puede notar que al enviar datos con saturación de tráfico del 0% y 50%, tanto en IPv4 como en IPv6, no hubo pérdidas sustanciales, apenas la mayor pérdida de paquetes fue de 0,22% en IPv6. Debido a esto podemos concluir que MPLS logro influenciar en ambos protocolos ya que opera entre la capa de enlace y capa de red permitiendo una conmutación más rápida.

3.- De forma general, al producir tráfico en la red con porcentajes de saturación de 0%, 50% y 100%, respectivamente y realizando la transmisión de data y video, IPv4 tuvo mayor cantidad de paquetes enviados que IPv6.

4.- En la pruebas de Video bajo la influencia del protocolo IPv6 hubo menor pérdida de datos en comparación con IPv4 durante los tres tráficos (0%, 50% y 100%) donde se concluye que debido a la simplificación de los encabezado de los datagramas en IPv6 los enrutadores pudieron procesar de manera más confiable los datos.

5.- En el cuadro comparativo del tráfico 50% de datos, se puede observar que el delay en IPv6 fue mayor que el de IPv4 cuando debía ser menor. Este resultado se debió al retardo de procesamiento que se da en el diseño del hardware de los dispositivos.

6.- Aunque las diferencias entre el protocolo IPv4 e IPv6 pueden llegar ser notorias visualmente, estadísticamente no lo fue. Al aplicar el análisis estadístico ANOVA se pudo comprobar que las diferencias entre estos dos protocolos no son significativas en ningún caso.

7.- De manera general, se concluye que el protocolo IPv6 no ejerce influencias negativas, cuando se aplica en redes MPLS con las características estudiadas.

**RECOMENDACIONES**

1. Desarrollar futuras investigaciones de redes basadas en MPLS aplicando políticas de calidad, ingeniería de tráfico de tal forma que se puedan evaluar las capacidades del protocolo IPV6.
2. Realizar investigaciones similares pero bajo la plataforma de Linux.
3. Realizar estas pruebas en otras topologías, observando el comportamiento del protocolo y el estándar en conjunto.
4. Incrementar el número de clientes y enrutadores para investigaciones con topologías similares.

**ÍNDICE DE REFERENCIA**

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

Bisquerra, R (2000), Manual de orientación y tutoría. Barcelona: Praxis

Boada y otros (2005). IPv6 y Multiprotocol label switching. Escuela politécnica nacional, Ecuador-Quito.

Canalis (2003), MPLS (Multiprotocol Label Switching), Disponible en: <http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/libmpls.PDF>

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

Cisco (2011), Calidad de servicio. Disponible en: <http://www.cisco.com/web/learning/netacad/index.html>

Deering y Hiden (1998), Protocolo de Internet Version 6 (IPv6). Disponible en: <http://www.ietf.org/rfc/rfc2460.txt>

Doménico y García (2011), Medición y análisis de tráfico en redes MPLS. Disponible en: <http://tesis.pucp.edu.pe/repositorio/handle/123456789/212>

Eliza, Gauna (2011), Evaluación del protocolo IPV6 en una red WAN soportada por el Estándar 802.11n. Proyecto de Trabajo Especial de Grado presentado para optar al título de Licenciada en Computación - La Universidad del Zulia. Edo. Zulia. Venezuela

Eveliux (2011), Definición de Protocolo. Disponible en: <http://www.eveliux.com/mx/curso-de-telecomunicaciones-y-redes.php>

Fernández (2001), VIII Jornada Iberoamericana de Informática. Disponible en: <http://www.ati.es/novatica/2001/151/glovoip.pdf>

Ferrer y Rocas (2001), Telemedicina. España, Madrid Panamericana.

Ferrer (2007), Diseño de redes LAN. Disponible en: <http://www.sisteseg.com/files/Microsoft_Word_-_RED_LAN_Y_SU_TECNOLOGIA.pdf>

Grajales (2000), Tipos de Investigación. Disponible en: <http://tgrajales.net/investipos.pdf>

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

### IETF (2011), [Internet Engineering Task Force](http://www.ietf.org/). Disponible en: <http://www.ietf.org/>

Interiano y montes (2005), Ethernet Conmutada. Disponible en: <http://www.ie.itcr.ac.cr/faustino/Redes/Clase9/>

Jara (2004), Docencia en Qos orientada a rede MPLS. Disponible en: <http://toip.uchile.cl/mediawiki/upload/9/92/Redaccion73.pdf>

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.

Mcquery y otros (2001), Cisco Voz sobre frame realy, ATM and IP. Cisco Press.

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

Millan R. (2001). El protocolo IPv6 (I). Disponible en: http://www.ramonmillan.com/tutoriales/ipv6\_parte1.php

Morales (2006), Investigación de Redes VPN con tecnología MPLS. Disponible en:

[http://catarina.udlap.mx/u\_dl\_a/tales/documentos/lis/morales\_d\_l/CAPÍTULO2.pdf](http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/capitulo2.pdf)

Morcillo (2005), Análisis de la seguridad en IP/MPLS VPN: comparación con ATM. Disponible en: <http://upcommons.upc.edu/pfc/bitstream/2099.1/3716/2/40393-2.pdf>.

Moya y Millan (2002), MPLS (Multiprotocol Label Switching). Disponible en:

<http://www.ramonmillan.com/tutoriales/mpls.php>

NRO (2010), Espacio de direcciones IPv4 disponibles disminuye por debajo del 5%. Disponible en: <http://www.nro.net/media/remaining-ipv4-address-below-5.html>

Rau (2005). Proyecto IPv6, Disponible en: <http://www.rau.edu.uy/ipv6/queesipv6.htm>

Rodríguez y Zambrano (2010), Análisis y diseño de una reingeniería organizativa de la red del campus de la universidad técnica de Manabí mediante la utilización de IPv6 y su implementación en la facultad de ciencias informáticas en el laboratorio de redes. Disponible en: <http://repositorio.utm.edu.ec/bitstream/123456789/27/1/TESIS%20IPV6.pdf>

Rubiano y Urbano (2006), Investigación de la arquitectura MPLS ventajas y servicios. Universidad de los Andes, Colombia-Bogota.

Subía y otros (2006). Comunicaciones IPv6 con MPLS. Escuela Politécnica nacional Ecuador-Quito.

Wallid (2004), Transición a IPv6 en un departamento Universitario. Disponible en: <http://oasis.dit.upm.es/~omar/tesis/tesis1/taro/26-Migracion-IPv6-Omar-Wallid.pdf>

**Anexos**

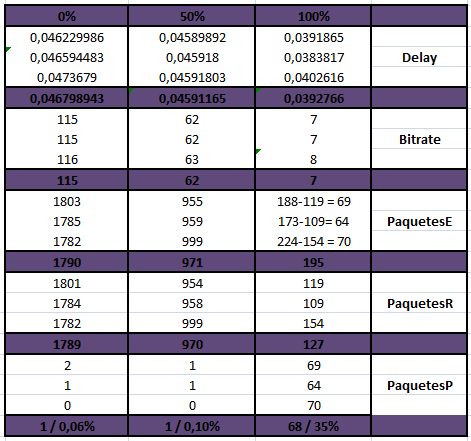


Tabla N° 17: Protocolo IPv4, Tráfico 0%, 50% y 100% enviando datos

Fuente: Propia (2011)

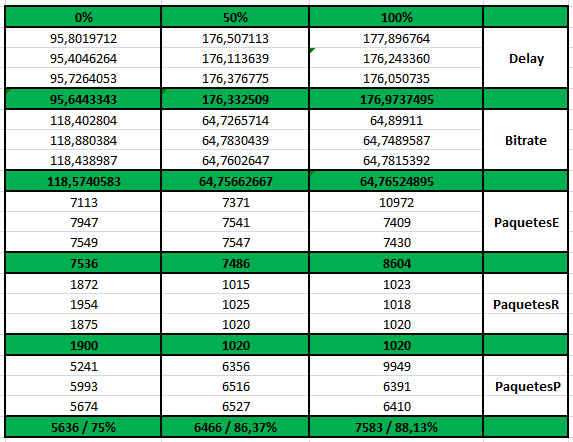


Tabla N° 18: Protocolo IPv4, Tráfico 0%, 50% y 100% enviando video

Fuente: Propia (2011)

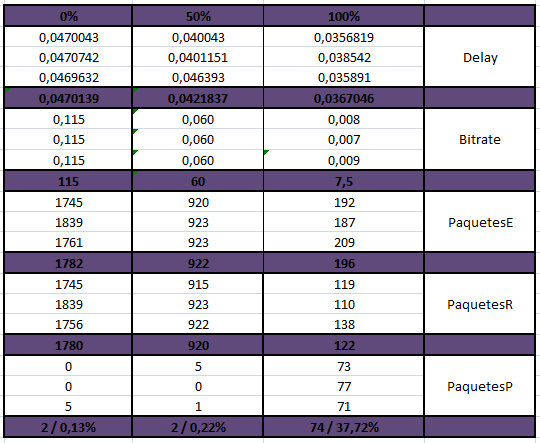


Tabla N° 19: Protocolo IPv6, Tráfico 0%, 50% y 100% enviando datos

Fuente: Propia (2011)

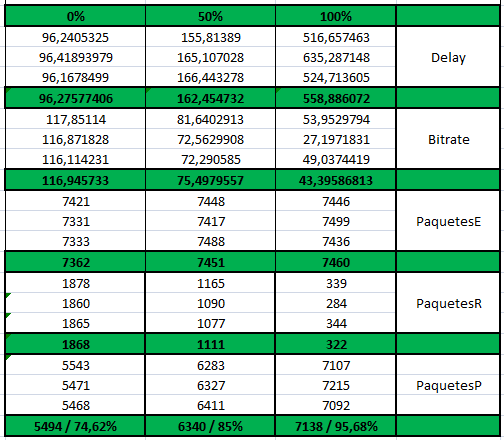


Tabla N° 20: Protocolo IPv6, Tráfico 0%, 50% y 100% enviando video

Fuente: Propia (2011)

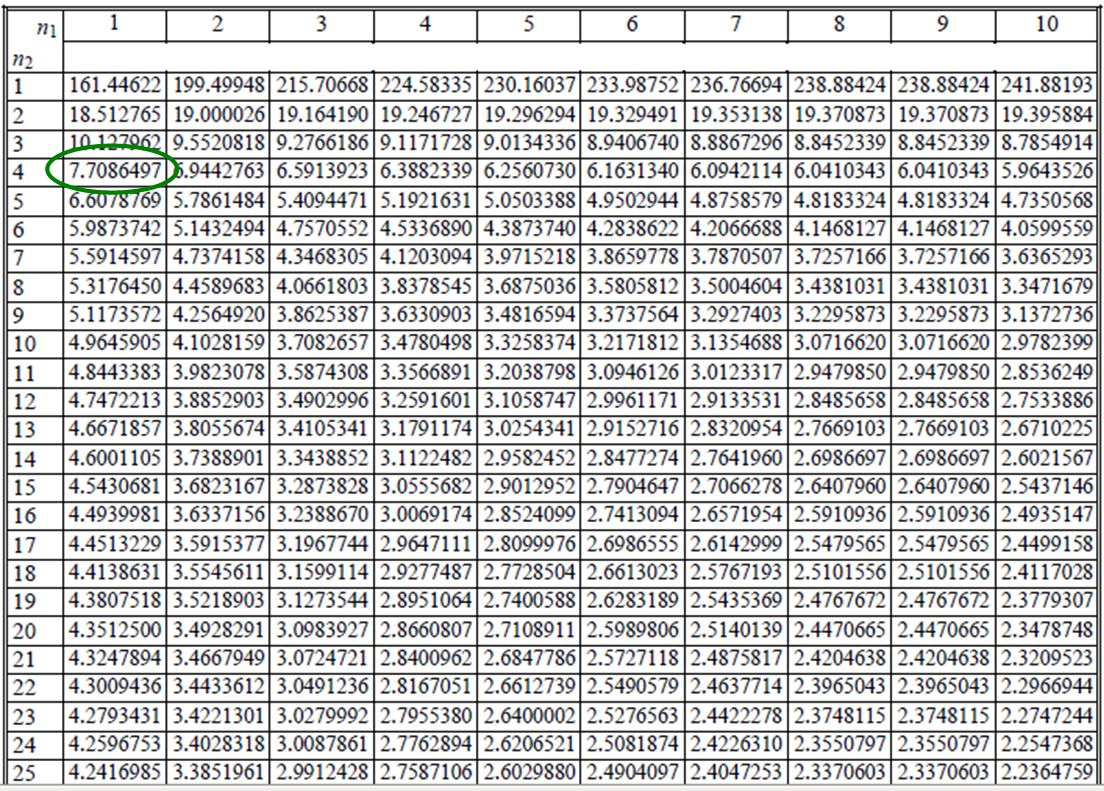


Tabla N° 21: Tabla de Distribución F de Fisher con probabilidad de 0.05

Fuente: Massart (1997).