

TESIS DEFENDIDA POR

Miguel Chávez López

Y APROBADA POR EL SIGUIENTE COMITÉ:

M.C. Raúl Tamayo Fernández

Director del Comité

M.C. Jorge Enrique Preciado Velasco

Miembro del Comité

Dr. José Rosario Gallardo López

Miembro del Comité

M.C. Raúl Rivera Rodríguez

Miembro del Comité

Dr. Pedro Negrete Regagnon

Miembro del Comité

Dr. José Rosario Gallardo López

Jefe del Departamento de Electrónica

Dr. Luis Alberto Delgado Argote

Director de Estudios de Posgrado

Ensenada, B.C. Agosto de 2003

Centro de Investigación Científica y de
Educación Superior de Ensenada



DIVISIÓN DE FÍSICA APLICADA
DEPARTAMENTO DE ELECTRÓNICA Y
TELECOMUNICACIONES

ANÁLISIS Y MODELADO DE MECANISMOS
PARA LA INTEROPERABILIDAD DE MPLS Y
DIFFSERV

TESIS

que para cubrir parcialmente los requisitos necesarios para
obtener el grado de MAESTRO EN CIENCIAS presenta:

MIGUEL CHÁVEZ LÓPEZ

Ensenada, Baja California, México. Agosto de 2003.

RESUMEN de la Tesis de **Miguel Chávez López**, presentada como requisito parcial para la obtención del grado de **MAESTRO EN CIENCIAS** en **ELECTRÓNICA Y TELECOMUNICACIONES**. Ensenada, Baja California, México. Agosto de 2003.

ANÁLISIS Y MODELADO DE MECANISMOS PARA LA INTEROPERABILIDAD DE MPLS Y DIFFSERV

Resumen aprobado por:

M.C. Raúl Tamayo Fernández

Director de Tesis

MPLS fue presentado originalmente como una solución para mejorar la velocidad en los enrutadores, pero ahora está emergiendo como una tecnología de estándares crucial, la cual ofrece nuevas capacidades para redes IP a gran escala. Ejemplos de aplicaciones de MPLS son: Ingeniería de tráfico (la habilidad de los operadores de la red para dictaminar el camino que seguirá el tráfico a través de la red), y soporte de Calidad de Servicio (QoS, Quality of Service). Estos son 2 ejemplos de aplicaciones clave donde MPLS beneficiará a toda tecnología IP disponible en la actualidad.

Actualmente existen otras arquitecturas que permiten al proveedor de servicios ofrecer garantías de Calidad de Servicio al usuario, una de ellas es Servicios Diferenciados (DiffServ), este protocolo trabaja en la capa tres del modelo OSI (capa de red), en tanto MPLS lo hace en la capa dos. De lo anterior se desprende la principal motivación para el desarrollo de este trabajo de investigación, el cual consiste en evaluar la interoperabilidad de MPLS con la arquitectura de Servicios Diferenciados, además de que esta última es la arquitectura adecuada para dorsales.

En este trabajo de investigación se realiza un análisis teórico del protocolo MPLS, así como el modelado y simulación de una arquitectura MPLS - DiffServ. Para el modelado de la red se utilizó la topología de la Red-CUDI con tráfico de video, voz y datos. Para evaluar el desempeño de la arquitectura se compararon los resultados obtenidos en cuanto a retardo extremo a extremo, variación del retardo y probabilidad de pérdida de paquetes con los valores permitidos de estos parámetros para las aplicaciones de video, voz y datos. Así mismo, estos resultados fueron comparados con los obtenidos para una arquitectura DiffServ - ATM de la Red-CUDI.

Palabras clave: MPLS, DiffServ, QoS, ATM, interoperabilidad.

ABSTRACT of the thesis of **Miguel Chávez López**, submitted in partial fulfillment of the requirements to obtain the degree of **MASTER IN SCIENCE in ELECTRONICS AND TELECOMMUNICATIONS**. Ensenada, Baja California, México. August 2003.

ANALYSIS AND MODELING OF MECHANISMS FOR MPLS AND DIFFSERV INTEROPERABILITY

Abstract approved by:

M.S. Raúl Tamayo Fernández

Thesis Director

MPLS was originally presented as a solution to improve routers speed, but now is emerging as an essential technology, which offers new capabilities to large IP Networks. MPLS applications include: Traffic Engineering (the ability of network operators to control the path over which networks traffic will travel) and QoS support. These are two key MPLS applications that will improve every current IP technology.

At this moment, there are other architectures that allow service providers to offer Quality of Service assurances to the user, one of them is Differentiated Services (Diff-Serv), this protocol works in layer three of OSI model (network layer), however MPLS does it in layer two. The previous fact is the main motivation for the development of this work, which consists of evaluating the interoperability of MPLS with the architecture of Differentiated Services, besides this last one is the suitable architecture for network backbones.

In this work it is made a theoretical analysis of MPLS protocol, as well as a modeling and simulation of a MPLS-DiffServ architecture. Red-CUDI network topology was used in MPLS network modeling with video, voice and data traffic. In order to evaluate the performance of the architecture the results obtained as (end to end delay, jitter and loss probability) were compared with the allowed values for video, voice and data applications. Also, these results were compared with those obtained for a DiffServ-ATM architecture in Red-CUDI.

Keywords: MPLS, DiffServ, QoS, ATM, interoperability.

Dedicatoria

A mi familia

por su apoyo incondicional en cada una de
las metas que me he propuesto.

Agradecimientos

A mi director de tesis *M.C. Raúl Tamayo Fernández* por su paciencia y valiosa ayuda, además de las charlas del área de redes de telecomunicaciones que me dejaron bastantes conocimientos.

A mi novia *Karina* por su gran amor y hacer éste último año a su lado el mejor de mi vida. Te Amo.

Al *Dr. Jaime Sánchez García* por su amistad y apoyo tanto escolar como extraescolarmente.

Al *Dr. José Rosario Gallardo López* por su gran ayuda durante el desarrollo de mi trabajo de tesis.

A los miembros del comité de tesis: *M.C. Jorge Preciado Velasco, Dr. José Rosario Gallardo López, M.C. Raúl Rivera Rodríguez y Dr. Pedro Negrete Regagnon* por sus acertados comentarios acerca de mi trabajo.

A mis compañeros telecos: *Adriana, Myriam, Karina, Zeus, Temo, José Luis, Luis Solis, Joaquin, Chava, Rodrigo y Aleks*. Gracias por su amistad y compartir conmigo estos dos años.

A mis compañeros controleros y microonderos: *Elizabeth, José Navarrete, Ruben, Ricardo, Francisco Hirata y Liz*. Gracias por su amistad que hizo más fácil ese primer trimestre de clases.

A *Ramón Muraoka* por su gran amistad y su ayuda a la hora de echarle mecánica al vocho.

Al Centro de Investigación Científica y de Educación Superior de Ensenada.

Al Consejo Nacional de Ciencia y Tecnología por su apoyo económico sin el cual no me hubiera sido posible realizar este trabajo de investigación.

Tabla de Contenido

| CAPÍTULO | PÁGINA |
|--|-----------|
| I Introducción | 1 |
| I.1 Motivación o Justificación | 3 |
| I.2 Objetivos | 3 |
| I.3 Materiales y Métodos | 4 |
| I.4 Organización de la Tesis | 6 |
| II Calidad de Servicio (QoS) | 7 |
| II.1 Introducción | 7 |
| II.2 Parámetros de Calidad de Servicio | 8 |
| II.3 Arquitecturas de QoS | 10 |
| II.3.1 Servicios Integrados (IntServ) | 12 |
| II.3.2 Servicios Diferenciados (DiffServ) | 15 |
| II.3.3 Conmutación de Etiquetas Multiprotocolo (MPLS) | 17 |
| III El Protocolo MPLS | 20 |
| III.1 Introducción | 20 |
| III.2 Conmutación de Etiquetas Multiprotocolo | 22 |
| III.3 Dominio MPLS | 25 |
| III.4 El encabezado MPLS | 27 |
| III.5 Estructuras de datos en MPLS | 28 |
| III.6 Protocolos de distribución de etiquetas | 30 |
| III.7 Interoperabilidad de MPLS con Servicios Diferenciados (DiffServ) | 31 |
| III.7.1 E-LSP | 33 |
| III.7.2 L-LSP | 35 |
| III.8 Propuesta de Enrutadores de Conmutación de Etiquetas (LSR) | 37 |
| III.8.1 Arquitectura de un LSR de Frontera | 38 |
| III.8.2 Arquitectura de un LSR de Núcleo | 40 |
| IV Implementación de los Modelos de Simulación | 42 |
| IV.1 Introducción | 42 |
| IV.2 Diffserv sobre ATM utilizando 6 PVCs | 44 |
| IV.2.1 Modelo de Red | 44 |
| IV.2.2 Modelo de Nodo | 46 |
| IV.2.2.1 Modelo de Nodo de Generadores de Tráfico | 46 |
| IV.2.2.2 Modelo de Nodo de Asociados Académicos | 46 |
| IV.2.2.3 Modelo de Nodo para Gigapops | 47 |

Tabla de Contenido (Continuación)

| CAPÍTULO | PÁGINA |
|---|-----------|
| IV.2.2.4 Modelo de Nodo para Recepción de Tráfico y Captura de Estadísticas | 48 |
| IV.2.3 Modelo de Procesos | 49 |
| IV.2.3.1 Modelo de Procesos para el Segmentador ATM | 49 |
| IV.2.3.2 Modelo de Procesos para el Ensamblador ATM | 50 |
| IV.3 MPLS sobre SONET | 51 |
| IV.3.1 Modelo de Red | 51 |
| IV.3.1.1 Modelo de Red MPLS - Dorsal Tij-Gdl-D.F. | 51 |
| IV.3.1.2 Modelo de Red MPLS - Dorsal Completa | 52 |
| IV.3.2 Modelo de Nodo | 53 |
| IV.3.2.1 Modelo de Nodo para LSR de Frontera | 53 |
| IV.3.2.2 Modelo de Nodo para LSR de Núcleo | 55 |
| IV.3.2.3 Modelo de Nodo para Recepción de Tráfico y Captura de Estadísticas | 55 |
| IV.3.3 Modelo de Procesos | 56 |
| IV.3.3.1 Modelo de Procesos para el Clasificador Multicampo | 56 |
| IV.3.3.2 Modelo de Procesos para el Acondicionador de Tráfico | 58 |
| IV.3.3.3 Modelo de Procesos para Asignación de Etiqueta | 61 |
| IV.3.3.4 Modelo de Procesos para el Clasificador EXP | 63 |
| IV.3.3.5 Modelo de Procesos para el Calendarizador | 64 |
| IV.3.3.6 Modelo de Procesos para el Clasificador de Etiquetas | 68 |
| IV.3.3.7 Modelo de Procesos para Intercambio y Envío de Etiqueta | 70 |
| V Resultados y Análisis Numérico | 72 |
| V.1 Introducción | 72 |
| V.2 Parámetros de Simulación | 72 |
| V.3 Obtención de Parámetros Adecuados de Operación de los Mecanismos de QoS | 75 |
| V.3.1 DiffServ sobre ATM utilizando 6 PVCs | 76 |
| V.3.2 MPLS sobre SONET | 77 |
| V.4 Análisis de Resultados | 79 |
| V.4.1 DiffServ sobre ATM utilizando 6 PVCs | 79 |
| V.4.1.1 Retardo Extremo a Extremo | 79 |
| V.4.1.2 Variación del Retardo | 81 |
| V.4.1.3 Probabilidad de Pérdida de Paquetes | 82 |
| V.4.1.4 Caudal Eficaz | 83 |
| V.4.2 MPLS sobre SONET Dorsal Tij - Gdl - D.F. | 84 |
| V.4.2.1 Retardo Extremo a Extremo | 84 |
| V.4.2.2 Variación del Retardo | 86 |

Tabla de Contenido (Continuación)

| CAPÍTULO | PÁGINA |
|---|------------|
| V.4.2.3 Probabilidad de Pérdida de Paquetes | 88 |
| V.4.2.4 Caudal Eficaz | 89 |
| V.4.3 Comparación entre los modelos DiffServ sobre ATM y MPLS sobre SONET Dorsal Tij-Gdl-D.F. | 90 |
| V.4.3.1 Retardo Extremo a Extremo | 90 |
| V.4.3.2 Variación del Retardo | 91 |
| V.4.3.3 Probabilidad de Pérdida de Paquetes | 93 |
| V.4.3.4 Caudal Eficaz | 94 |
| V.4.4 MPLS sobre SONET Dorsal Completa | 95 |
| V.4.4.1 Retardo Extremo a Extremo | 95 |
| V.4.4.2 Variación del Retardo | 97 |
| V.4.4.3 Probabilidad de Pérdida de Paquetes | 98 |
| V.4.4.4 Caudal Eficaz | 99 |
| VI Conclusiones | 101 |
| VI.1 Conclusiones | 101 |
| VI.2 Aportaciones | 102 |
| VI.3 Recomendaciones | 103 |
| VI.4 Trabajos Futuros | 104 |
| Literatura Citada | 105 |
| Apéndices | 107 |
| A Modelos de Tráfico | 107 |
| A.1 Introducción | 107 |
| A.2 Modelo para Fuente de Tráfico de Voz | 107 |
| A.3 Modelo para Fuente de Tráfico de Video | 108 |
| A.4 Modelo para Fuente de Tráfico FTP | 109 |
| A.5 Modelo para Fuente de Tráfico WWW | 110 |
| A.6 Modelo para Fuente de Tráfico SMTP | 111 |
| Lista de Acrónimos | 113 |

Lista de Figuras

| FIGURA | | PÁGINA |
|--------|--|--------|
| 1 | Dominio MPLS | 26 |
| 2 | Encabezado MPLS | 27 |
| 3 | NHLFE, FTN e ILM | 30 |
| 4 | E-LSP | 34 |
| 5 | L-LSP | 36 |
| 6 | Arquitectura de un LSR de Frontera | 38 |
| 7 | Arquitectura de un LSR de Núcleo | 40 |
| 8 | Mapa de la red Internet 2-México | 43 |
| 9 | Modelo de red ATM - 6 PVCs | 45 |
| 10 | Modelo de nodos generadores de tráfico | 46 |
| 11 | Modelo de nodos de Asociados Académicos | 47 |
| 12 | Modelo de nodos de Gigapops | 48 |
| 13 | Modelo de nodo para recepción de tráfico | 48 |
| 14 | Modelo de procesos para el segmentador ATM | 49 |
| 15 | Modelo de procesos para el ensamblador ATM | 50 |
| 16 | Modelo de red MPLS - Dorsal Tij-GDL-D.F. | 52 |
| 17 | Modelo de red MPLS - Dorsal Completa | 52 |
| 18 | Modelo de nodo para LSR de Frontera | 54 |
| 19 | Modelo de nodo para LSR de Núcleo | 55 |
| 20 | Modelo de nodo para Captura de Estadísticas | 56 |
| 21 | Modelo de procesos para el Clasificador Multicampo | 56 |
| 22 | Diagrama de flujo para el Clasificador Multicampo | 57 |
| 23 | Modelo de procesos para el Acondicionador de Tráfico | 58 |
| 24 | Diagrama de flujo para el Acondicionador | 60 |
| 25 | Modelo de procesos para Asignación de Etiqueta | 61 |
| 26 | Diagrama de flujo para Asignación de Etiqueta | 62 |
| 27 | Modelo de procesos para el Clasificador EXP | 63 |
| 28 | Diagrama de flujo para el Clasificador EXP | 64 |
| 29 | Modelo de procesos para el Calendarizador | 65 |
| 30 | Diagrama de flujo para el Calendarizador | 67 |
| 31 | Modelo de procesos para el Clasificador de Etiquetas | 68 |
| 32 | Diagrama de flujo para el Clasificador de Etiquetas | 69 |
| 33 | Modelo de procesos para Intercambio y Envío de Etiqueta | 70 |
| 34 | Diagrama de flujo para Intercambio y Envío de Etiqueta | 71 |
| 35 | Modelo de red para validación de mecanismos de QoS | 75 |
| 36 | Retardo extremo a extremo para el modelo DiffServ sobre ATM - 6 PVCs | 80 |

Lista de Figuras (Continuación)

| FIGURA | | PÁGINA |
|--------|---|--------|
| 37 | Variación del Retardo para el modelo DiffServ sobre ATM - 6 PVCs . . | 81 |
| 38 | Probabilidad de Pérdida de Paquetes para el modelo DiffServ sobre ATM | 83 |
| 39 | Caudal eficaz para el modelo DiffServ sobre ATM - 6 PVCs | 84 |
| 40 | Retardo extremo a extremo para el modelo MPLS Dorsal Tij-Gdl-D.F. | 85 |
| 41 | Variación del Retardo para el modelo MPLS Dorsal Tij-Gdl-D.F. . . . | 87 |
| 42 | Probabilidad de Pérdida de Paquetes para el modelo MPLS Dorsal Tij-Gdl-D.F. | 88 |
| 43 | Caudal eficaz para el modelo MPLS Dorsal Tij-Gdl-D.F. | 89 |
| 44 | Comparación entre los modelos DiffServ sobre ATM y MPLS sobre SONET de acuerdo al retardo extremo a extremo de cada tipo de servicio. . . . | 91 |
| 45 | Comparación entre los modelos DiffServ sobre ATM y MPLS sobre SONET de acuerdo a la variación del retardo de cada tipo de servicio. | 92 |
| 46 | Comparación entre los modelos DiffServ sobre ATM y MPLS sobre SONET de acuerdo a la probabilidad de pérdida de paquetes de cada tipo de servicio. | 93 |
| 47 | Comparación entre los modelos DiffServ sobre ATM y MPLS sobre SONET de acuerdo al Caudal Eficaz de cada tipo de servicio. | 95 |
| 48 | Retardo extremo a extremo para el modelo MPLS Dorsal Completa . . | 96 |
| 49 | Variación del Retardo para el modelo MPLS Dorsal Completa | 97 |
| 50 | Probabilidad de Pérdida de Paquetes para el modelo MPLS Dorsal Completa | 98 |
| 51 | Caudal eficaz para el modelo MPLS Dorsal Completa | 99 |
| 52 | Modelo ON-OFF utilizado para la fuente de tráfico FTP | 110 |
| 53 | Modelo ON-OFF utilizado para la fuente de tráfico WWW | 111 |
| 54 | Comportamiento bimodal de la fuente de tráfico SMTP | 112 |

Lista de Tablas

| TABLA | | PÁGINA |
|-------|--|--------|
| I | Clases de Servicio propuestas | 37 |
| II | Tasa de generación de tráfico para cada servicio | 73 |
| III | Condiciones de tráfico para cada escenario de simulación | 74 |
| IV | Valores límites para los parámetros de QoS | 74 |
| V | Ancho de Banda asignado a cada PVC | 76 |
| VI | Parámetros de configuración para el Token Bucket | 78 |
| VII | Tasa de servicio asignada a cada clase de tráfico MPLS | 79 |

Capítulo I

Introducción

El enorme crecimiento de Internet, y la aparición de nuevas aplicaciones con transmisión de video, voz y datos, traen consigo la necesidad de mecanismos que hagan posible el funcionamiento eficaz de tales aplicaciones y motivan el desarrollo de otras más innovadoras. Esto ha sido una de las principales motivaciones para el desarrollo de la tecnología MPLS (Multi-Protocol Label Switching, Conmutación de Etiquetas Multiprotocolo) como una solución versátil para hacer frente a las necesidades de las redes de la actualidad, como son: velocidad, escalabilidad, manejo de Calidad de Servicio (QoS) e ingeniería de tráfico. MPLS representa el siguiente nivel de evolución en estándares, donde se combinan las tecnologías de conmutación de capa dos (enlace de datos) y tecnologías de enrutamiento (capa 3). MPLS aparece como una solución para alcanzar los requerimientos de ancho de banda y servicios para la nueva generación de redes basadas en el protocolo IP.

MPLS se ha convertido en una tecnología clave para el futuro de las redes IP de gran escala. MPLS ofrece facilidades para la implementación de redes IP a través de WANs basadas en ATM, proporcionando capacidades de ingeniería de tráfico en redes de paquetes, aportando capacidades de Calidad de Servicio en IP y auxiliando en el desarrollo de VPNs basadas en IP.

MPLS difiere significativamente de los métodos de procesamiento de “salto por salto” de las redes tradicionales. Una etiqueta corta, de longitud fija, de fácil procesamiento, proporciona una representación pequeña de un encabezado de paquete IP. Algunos fabricantes iniciaron desarrollando soluciones propietarias basadas en el concepto de conmutación de etiquetas, lo que provocó que la IETF iniciará el desarrollo de un estándar de interoperabilidad llamado MPLS.

En base a lo mencionado anteriormente se puede definir a MPLS como una solución para enfrentar los problemas presentes en las redes actuales, tales como velocidad, escalabilidad, gestión de la Calidad de Servicio e ingeniería de tráfico. MPLS ha emergido como una solución para la gestión del ancho de banda y los requerimientos de servicio para las redes dorsales de la próxima generación basadas en el protocolo IP. MPLS administra los asuntos relacionados con la escalabilidad y enrutamiento (basado en QoS y métricas de calidad de servicio) y puede implementarse sobre las redes ATM y Frame Relay existentes. El término de multiprotocolo se le asigna a MPLS porque sus técnicas de enrutamiento son aplicables a cualquier protocolo de capa de red.

A la par del desarrollo de MPLS, se han estado impulsando diversas arquitecturas que permitan ofrecer garantías de calidad a servicios sensibles a parámetros como caudal eficaz, retardo y pérdidas de paquetes. Entre las arquitecturas más desarrollados actualmente se encuentran: Servicios Integrados, basados en la reservación de recursos, y Servicios Diferenciados, basados en una clasificación, marcación, calendarización y acondicionamiento de los paquetes.

I.1 Motivación o Justificación

MPLS fue presentado como una solución para mejorar la velocidad en los enrutadores, pero ahora está emergiendo como una tecnología de estándares crucial, la cual ofrece nuevas capacidades para redes IP a gran escala. Ejemplos de aplicaciones de MPLS son: Ingeniería de tráfico (la habilidad de los operadores de la red para dictaminar el camino que seguirá el tráfico a través de la red), y soporte de Calidad de Servicio (QoS, Quality of Service). Estos son 2 ejemplos de aplicaciones clave donde MPLS beneficiará a toda tecnología IP disponible en la actualidad.

Actualmente existen otras arquitecturas que permiten al proveedor de servicios ofrecer garantías de Calidad de Servicio al usuario, una de ellas es Servicios Diferenciados (DiffServ), este protocolo trabaja en la capa tres del modelo OSI (capa de red), en tanto que MPLS lo hace en la capa dos. De lo anterior se desprende la principal motivación para el desarrollo de este trabajo de investigación, el cual consiste en evaluar la interoperabilidad de MPLS con la arquitectura de Servicios Diferenciados, además de que esta última es la arquitectura más adecuada para dorsales por cuestiones de escalabilidad.

I.2 Objetivos

Realizar investigación sobre los parámetros y requerimientos para la interoperabilidad de MPLS en redes que utilicen mecanismos de Calidad de Servicio. Se analizará específicamente el uso de MPLS para su incorporación a redes con tecnologías de Ser-

vicios Diferenciados.

Modelar la tecnología MPLS a través del simulador de redes OPNET Modeler, con aplicaciones específicas de video, voz, y datos, para obtener parámetros de operación adecuados de esta tecnología.

I.3 Materiales y Métodos

Materiales.

- Acceso a bibliotecas de CICESE y UCSD.
- Acceso a Internet mediante un enlace de 2 Mbps y a Internet2 mediante un enlace de 34 Mbps.
- Acceso a Supercomputadora Sun con 8 procesadores ultraSPARC III 900 Mhz con 8 MB de cache, dispositivos de almacenamiento Sun StorEdge D240 Media con: DVD-ROM, DAT y 2 Discos de 18 GB c/u y discos externos de alta velocidad Sun StorEdge T3 Array de 324 GB (total).
- Computadora personal con Procesador AMD Athlon a 1.43 GHz, 512 MB de memoria RAM, Disco Duro de 80 GB-7200 RPM y tarjeta de red D-Link 10/100 Fast Ethernet.
- Simulador OPNET Modeler versión 9.0.A.

- Software Diverso (Microcal Origin Pro 7.0, MikTEX 2.2, WinEdt 5.3, Office XP, Microsoft Visio Pro 2002, etc.)

Metodología.

1. Investigación bibliográfica de la arquitectura MPLS.
2. Investigación bibliográfica de la arquitectura DiffServ.
3. Estudio del software de simulación OPNET Modeler.
4. Investigación bibliográfica de los mecanismos necesarios para la implementación de MPLS sobre redes ATM.
5. Investigación bibliográfica de los mecanismos necesarios para la interoperabilidad de MPLS y DiffServ.
6. Definición de los modelos para los mecanismos a simular.
7. Simulación de los modelos.
8. Análisis de resultados.
9. Validación de resultados.
10. Análisis comparativo entre los modelos DiffServ sobre ATM y MPLS sobre SONET.
11. Obtención de conclusiones.
12. Escritura de tesis.

I.4 Organización de la Tesis

El presente trabajo de tesis se encuentra organizado de la siguiente manera:

El Capítulo II define el concepto de Calidad de Servicio, se analizan sus parámetros de medición y las principales arquitecturas de Calidad de Servicio definidas por la IETF (Internet Engineering Task Force) hasta el momento de la escritura de este trabajo.

El Capítulo III presenta un análisis teórico de la arquitectura MPLS y su interoperabilidad con la arquitectura de Servicios Diferenciados. Además se presentan los mecanismos que componen la estructura interna de los enrutadores que forman una Red MPLS.

El Capítulo IV presenta los modelos de las arquitecturas DiffServ sobre ATM y MPLS sobre SONET implementados mediante el simulador OPNET, así como una descripción de su programación mediante diagramas de flujo.

El Capítulo V presenta el análisis numérico de los resultados obtenidos mediante la ejecución de secuencias de simulación en OPNET. También se presenta una comparación entre los modelos DiffServ sobre ATM y MPLS sobre SONET.

Finalmente, el Capítulo VI presenta las conclusiones, recomendaciones y aportaciones surgidas de este trabajo de tesis, así como trabajos futuros que pueden derivarse del mismo.

Capítulo II

Calidad de Servicio (QoS)

II.1 Introducción

La capacidad de una red para asegurar recursos a una aplicación, así como otorgar diferentes niveles de servicio se conoce como *Calidad de Servicio (QoS)*. Su objetivo principal es dar prioridad a determinada aplicación, lo cual incluye una asignación de ancho de banda, un control sobre el retardo extremo a extremo y la variación del retardo (necesario para aplicaciones en tiempo real), así como bajas pérdidas. Cabe mencionar que otorgar esta prioridad no debe influir en el desempeño de otras aplicaciones.

La calidad de servicio encierra propiedades de una red, sin embargo, el término de calidad describe el proceso de la entrega de datos de una manera confiable e incluso mejor que lo normal. Este método incluye aspectos de pérdidas de paquetes y retardos, los cuales deben ser mínimos o casi nulos.

Por lo tanto, tenemos que la unión de los términos calidad y servicio encierra información sobre el comportamiento de la red, así como la definición de las características y propiedades de un servicio en específico. De este modo se tiene que la calidad de servicio involucra la capacidad de diferenciar entre el tráfico o servicios de un usuario con respecto de otro [Ferguson y Huston, 1992].

II.2 Parámetros de Calidad de Servicio

El que una red pueda ofrecer Calidad de Servicio a sus usuarios, se encuentra determinado por varios parámetros que miden la calidad de servicio; entre los considerados más importantes, debido a que la mayoría de las aplicaciones requieren de una combinación de los mismos [Weiss, 1998], se encuentran los cinco siguientes:

1. **Disponibilidad de Servicio.-** Se refiere a la oportunidad que tiene un usuario de tener acceso a los dispositivos de una red. Depende del número de puertos de acceso a la red y se ve afectado cuando se presentan niveles de congestión, ya que en ese instante el servicio ofrecido al usuario puede experimentar retardo o puede simplemente no ser otorgado, por ello, este punto encierra características de administración de los recursos de la red basándose en la carga ideal de tráfico que transite sobre ella, esto con la finalidad de detectar los niveles de congestión de la red.
2. **Pérdida de Paquetes.-** Son consecuencia de los niveles de congestión que pueden presentarse en un enlace de una red. Una forma de evitar esta pérdida de paquetes es mediante la reducción del tráfico que compite por el uso del enlace, lo cual puede liberar a dicho enlace de la presencia del nivel de congestión y se puede lograr mediante el envío de avisos hacia el nodo fuente para que disminuya el tráfico que inyecta al enlace y por consiguiente el nivel de congestión [Weiss, 1998]. El porcentaje de paquetes perdidos en los distintos dispositivos de la red

se puede obtener mediante el cálculo de una probabilidad de pérdida de paquetes (PLR, Probability Loss Ratio), dada por la siguiente expresión matemática:

$$PLR = \frac{\text{No. total de paquetes perdidos}}{\text{No. total de paquetes transmitidos}} \quad (1)$$

3. **Retardo.-** También se conoce como retardo extremo a extremo, y se refiere al tiempo total que transcurre desde que un paquete es transmitido por su nodo fuente hasta que llega a su nodo destino. Aplicaciones en tiempo real (videoconferencia o voz) requieren de ciertos niveles mínimos de retardo para su buen desempeño. Niveles grandes de retardo pueden ocasionar que el nodo destino descarte los paquetes, haciendo un mal uso del ancho de banda y afectando el desempeño de la aplicación [Weiss, 1998].
4. **Variación del Retardo o Jitter.-** Se define como la diferencia del retardo perteneciente a paquetes similares, los cuales siguen una misma trayectoria dentro de la red. Se ve afectado por la variación en la cantidad de tráfico no similar, que compite por el mismo enlace [Weiss, 1998].
5. **Caudal Eficaz.-** Se refiere al monto total de tráfico recibido con éxito por el nodo destino y está dado por la siguiente expresión matemática:

$$Th = \rho[1 - PLR] \quad (2)$$

donde: Th representa el caudal eficaz, ρ la utilización del enlace y PLR la probabilidad de pérdida de paquetes.

Cualquier diseño de red debe tratar de maximizar los puntos 1 y 5, reducir el punto 3 y eliminar los puntos 2 y 4, para poder ofrecer Calidad de Servicio a sus usuarios.

II.3 Arquitecturas de QoS

La creciente demanda en el uso de aplicaciones multimedia, así como de aplicaciones en tiempo real, por parte de los usuarios de la Internet, ha provocado que el modelo de datagramas o de mejor esfuerzo (Best Effort) en el cual basa su funcionamiento actualmente la Internet, sea insuficiente para cumplir con los requerimientos mínimos de recursos de estas aplicaciones. Esto, aunado a la variedad de servicios que se ofrecen (videoconferencia, correo electrónico, hospedaje de sitios web, transferencia de archivos, etc.), ha creado la necesidad de implementar nuevas arquitecturas que sean capaces de hacer una *asignación de recursos* y una *diferenciación de servicios*, es decir, ofrecer Calidad de Servicio a estas aplicaciones para garantizar su buen desempeño.

En la década de los noventa la IETF (Internet Engineering Task Force) presentó las primeras arquitecturas para ofrecer QoS, estas fueron *Servicios Integrados (IntServ)* y *Servicios Diferenciados (DiffServ)*. Ambas arquitecturas ofrecen asignación de recursos, además de abarcar puntos importantes para la implementación de QoS.

Servicios Integrados provee un aseguramiento de recursos mediante una reservación

de los mismos para aplicaciones de flujos individuales, mientras que Servicios Diferenciados utiliza una combinación de políticas de frontera, abastecimiento y preferencia de tráfico [Wang, 2001].

La implementación de QoS en la Internet va más allá de tan solo hacer una reserva de recursos y utilizar mecanismos de clasificación y calendarización. También son necesarios mecanismos que ayuden a optimizar el uso de los recursos asignados. Esta necesidad surge debido a que los protocolos de enrutamiento que se utilizan actualmente, seleccionan el camino más corto hacia el nodo destino, basándose en métricas sencillas, tales como número de saltos y retardo. Claramente esto no es suficiente para hacer un uso óptimo de los recursos de la red. Si recordamos, para hacer una reserva de recursos se necesita encontrar una trayectoria que cuente con los recursos solicitados, tales como ancho de banda, pero el protocolo IP (Internet Protocol) no cuenta con la información necesaria para tomar estas decisiones.

Llevar al cabo una optimización de recursos requiere contar con un control explícito de las rutas por las cuales puede circular el tráfico del usuario, de esta manera, el tráfico puede ser ordenado para maximizar el uso de los recursos y la utilización de la red.

La arquitectura propuesta por la IETF para optimizar el desempeño de la red fue *MPLS (Multiprotocol Label Switching)*, la cual mediante mecanismos de enrutamiento explícito e ingeniería de tráfico, proporciona a los proveedores de servicios las herramientas necesarias para administrar el desempeño de sus redes.

A continuación se presenta una breve descripción de los mecanismos de calidad de

servicio mencionados anteriormente.

II.3.1 Servicios Integrados (IntServ)

A inicios de la década de los noventa la IETF creó el grupo de trabajo de Servicios Integrados con el objetivo de estandarizar una nueva arquitectura de reservación de recursos.

La arquitectura de Servicios Integrados se basa en una reservación de recursos *por flujo*. Para que a una aplicación se le aseguren recursos, esta tiene que solicitar una reservación de los mismos antes de que pueda inyectar tráfico a la red.

La reservación de recursos implica varias etapas a realizar por parte de la aplicación que los solicita. Primero, esta debe de caracterizar su fuente de tráfico y los requerimientos de recursos. Enseguida, la red utiliza un protocolo de enrutamiento para encontrar una trayectoria que cumpla con los recursos solicitados.

La reservación de recursos se hace en cada elemento de la red a lo largo de la trayectoria, mediante un protocolo de reservación, específicamente se utiliza el protocolo RSVP (Resource Reservation Protocol); un mecanismo de control de admisión se encarga de verificar si cada elemento cuenta con los recursos suficientes para aceptar esta reservación.

Una vez que la reservación es establecida, la fuente puede comenzar a enviar datos de dicha aplicación, a través de la trayectoria, haciendo un uso exclusivo de los recursos

que le fueron reservados. Además, la reservación de recursos es apoyada por mecanismos de clasificación de paquetes y calendarización empleados por los enrutadores.

Servicios Integrados propone dos modelos de servicio: El modelo de *Servicio Garantizado* y el modelo de *Servicio de Carga Controlada*.

- **Servicio garantizado.-** Garantiza el ancho de banda, un mínimo retardo extremo a extremo y no presenta pérdidas de paquetes, para tráfico conforme al perfil establecido. Esto lo lleva a cabo mediante un estricto control de admisión y una calendarización justa de las colas (Fair Queuing). Está dirigido para aplicaciones con estrictos requerimientos de ancho de banda y retardo, tales como videoconferencia, voz y aplicaciones en tiempo real.
- **Servicio de carga controlada.-** No proporciona ninguna garantía en cuanto a retardo y ancho de banda. Intenta proveer un servicio que se encuentre entre el modelo de mejor esfuerzo y el modelo de servicio garantizado mediante mecanismos de control de admisión y clasificación de tráfico. Las aplicaciones que utilizan el servicio de carga controlada experimentan un comportamiento parecido al que les ofrecería el modelo de mejor esfuerzo, cuando la red tiene poca carga. La diferencia radica en que el servicio de carga controlada no se deteriora si la carga en la red aumenta. Este modelo de servicio es apropiado para aplicaciones que pueden tolerar una cierta cantidad de pérdidas y retardo dentro de un nivel razonable, tales como transferencia de archivos (FTP, File Transfer Protocol) y

correo electrónico (SMTP, Simple Mail Transfer Protocol).

La implementación de servicios integrados en las dorsales de los proveedores de servicio de Internet (ISPs, Internet Service Provider) para ofrecer calidad de servicio a sus usuarios no representa una buena solución. Esto debido a que, servicios integrados está orientado a aplicaciones de larga duración y sensibles al retardo. Actualmente el tráfico WWW es el predominante en cualquier red, las características que lo definen implican cambios significativos sobre los datos transmitidos, el encabezado requerido para la reservación es demasiado grande y mucho de este tráfico presenta características de corta duración. Además, la reservación de recursos requiere de acuerdos entre distintos proveedores de servicios, ya que aquellos que solicitan una reservación de recursos tienen que pagar por ellos, cualquier reservación debe de ser autorizada, autenticada y contabilizada, tal arquitectura simplemente no existe en la Internet actual.

Estos puntos llevan a la conclusión de que servicios integrados puede ser un mecanismo para la implementación de calidad de servicio sobre redes corporativas (Intranets), ya que éstas son limitadas en tamaño y operan bajo un mismo dominio administrativo.

En [Cruz Patiño, 2001] se presenta un análisis teórico, el cual incluye modelado y simulación de la arquitectura de Servicios Integrados.

II.3.2 Servicios Diferenciados (DiffServ)

Cuando los proveedores de servicios se dieron cuenta que Servicios Integrados no era una buena solución para sus dorsales de Internet, la IETF creó el grupo de trabajo de Servicios Diferenciados, buscando una arquitectura alternativa para la asignación de recursos. Contrario a la reservación por flujos que hace IntServ, Servicios Diferenciados realiza la reservación de recursos mediante una combinación de políticas de frontera, abastecimiento y asignación de prioridades para lograr una diferenciación de servicios.

DiffServ clasifica el tráfico dentro de grupos pequeños llamados clases de transmisión. Las clases se ubican dentro de un comportamiento por salto llamado PHB (Per Hop Behavior), el cual se implementa sobre cada enrutador del dominio DiffServ y se encarga de determinar el nivel de calidad de servicio que se otorgará a un flujo de tráfico.

La arquitectura de Servicios Diferenciados se define en el RFC 2475; es un modelo donde el tráfico que entra a la red es clasificado y posiblemente condicionado en las fronteras de la red, así como asignado a diferentes comportamientos de flujo agregado. Cada comportamiento de flujo agregado corresponde a un código DS (DiffServ), que se encuentra asignado sobre el campo ToS (Type of Service), perteneciente al encabezado IPv4 ó bien al campo Tipo de Clase, perteneciente al encabezado IPv6, ambos de 8 bits. Dentro de la red, los paquetes son transmitidos de acuerdo al comportamiento asociado con el código DS.

Los enrutadores que se encuentran en la frontera de una red de Servicios Diferenciados son los responsables de asignar los paquetes a sus respectivos comportamientos de flujo agregado. Esta clasificación de paquetes se realiza en base a un acuerdo de nivel de servicio (SLA, Service Level Agreement), realizado entre el usuario y el proveedor de servicios. Las fronteras de la red también son las responsables de realizar un control de admisión, donde el tráfico fuera del perfil acordado es descartado, retardado, quizás marcado con una prioridad menor o bien colocado dentro de algún tipo de flujo agregado.

Servicios Diferenciados se compone de elementos funcionales implementados en los enrutadores de la red, los cuales conforman el comportamiento por salto PHB en la transmisión de paquetes. Estos elementos funcionales se basan en la clasificación, medición, marcación, control de admisión, calendarización y acondicionamiento del tráfico. Los parámetros de operación de cada elemento dependen del SLA. El control de admisión se basa en políticas de encolamiento para el descarte de paquetes en caso de congestión.

DiffServ no requiere de la reservación de recursos previa a la transmisión del tráfico, ya que la asignación de éstos se basa específicamente en el tipo de comportamiento al que fue asignada una determinada aplicación. Los recursos demandados por dicha aplicación se especifican previamente en el SLA. Además, DiffServ elimina los problemas de escalabilidad que posee IntServ gracias a que los nodos interiores del dominio DiffServ sólo realizan operaciones más sencillas que las realizadas sobre la frontera de la red. Por

lo tanto, se puede concluir diciendo que el modelo DiffServ es un mecanismo confiable para la asignación y aseguramiento de los recursos de una red a gran escala, teniendo en cuenta que la calidad de aseguramiento depende del monto total de recursos y gestión que sean demandados por los usuarios de la red.

En [Caballero Cárdenas, 2002] se presenta un análisis teórico, el cual incluye modelado y simulación de la arquitectura de Servicios Diferenciados.

II.3.3 Conmutación de Etiquetas Multiprotocolo (MPLS)

Originalmente MPLS fue pensado como una solución alterna para integrar IP y ATM (Asynchronous Transfer Mode). Aunque ya habían sido estandarizadas varias arquitecturas para integrar IP y ATM, la mayoría eran complejas y tenían problemas de escalabilidad. La necesidad de una mejor integración de IP y ATM llevó al desarrollo de MPLS.

MPLS hace uso de la conmutación de etiquetas. Una etiqueta corta, de longitud fija es agregada al encabezado del paquete y empleada para el envío del paquete a su siguiente salto. En el momento en que un Enrutador de Conmutación de Etiquetas (LSR, Label Switching Router) recibe un paquete etiquetado, este utiliza la etiqueta del encabezado del paquete para decidir su siguiente salto, así como su etiqueta de salida correspondiente. En MPLS, la trayectoria que sigue un paquete cuando circula por la red MPLS, la cual se conoce con el nombre de trayectoria conmutada de etiqueta (LSP, Label Switched Path), debe de ser establecida antes de que pueda ser utilizada.

MPLS hace más simple el envío de los paquetes (Packet Forwarding). Revisar una etiqueta corta es un trabajo mucho más sencillo para los enrutadores que buscar un prefijo en una tabla de enrutamiento. Con MPLS, el envío de los paquetes puede realizarse independientemente del protocolo de red que se utilice.

A pesar de las ventajas presentadas anteriormente, una de las razones principales detrás de la implementación de MPLS ha sido la necesidad de la Ingeniería de Tráfico en las dorsales de Internet. El mecanismo de enrutamiento explícito de MPLS proporciona a las redes IP una herramienta de selección de rutas de la cual carecen actualmente.

MPLS incorpora conceptos y características de las arquitecturas de Servicios Integrados y Servicios Diferenciados. Por ejemplo, MPLS permite hacer una reservación de ancho de banda sobre un LSP, además, los paquetes pueden ser marcados para indicar su prioridad de descarte.

El objetivo de MPLS no es reemplazar el enrutamiento IP, sino más bien mejorar los servicios proporcionados por las redes IP mediante el uso de ingeniería de tráfico, garantizar una QoS y redes privadas virtuales (VPNs, Virtual Private Networks).

MPLS permite la comunión del modelo de datagrama y del modelo de circuito virtual en las redes IP. El modelo de datagramas, en el cual se basa la Internet actual, envía los paquetes salto por salto de acuerdo a la dirección destino del paquete. El modelo de circuito virtual, utilizado por ATM y Frame Relay, requiere que primero se establezcan las conexiones antes de que el tráfico pueda ser enviado. MPLS permite integrar ambos modelos, ofreciendo una solución que combina escalabilidad y una mejor

gestión de la red.

El objetivo principal de este trabajo es realizar investigación sobre los parámetros y requerimientos para la interoperabilidad de MPLS en redes que utilicen mecanismos de calidad de servicio, para posteriormente implementarlo mediante un modelo de simulación. Por ello, en el siguiente capítulo se presenta un estudio detallado de este protocolo.

Capítulo III

El Protocolo MPLS

III.1 Introducción

El envío de los paquetes IP en la Internet se basa en el modelo de datagramas: protocolos de enrutamiento se encargan de calcular las trayectorias mediante el intercambio de información de enrutamiento y cada paquete es enviado de forma independiente en base a su dirección IP destino. En cambio, ATM y Frame Relay son tecnologías orientadas a conexión, un circuito virtual debe ser establecido previo al envío de los paquetes o celdas (en el caso de ATM).

Los proveedores de servicios se han dado cuenta de la necesidad de ofrecer servicios IP (IP Multicast por nombrar uno), en sus redes ATM. Para lograr lo anterior se buscó la manera de integrar IP y ATM, una de las soluciones propuestas fue el modelo de superposición de IP sobre ATM. Este modelo involucra el establecimiento de una malla de circuitos virtuales privados (PVCs, Private Virtual Circuits) entre los enrutadores IP alrededor de la nube ATM, lo anterior tiene como consecuencia problemas de escalabilidad, además de que los enlaces ATM son invisibles al enrutamiento IP [Wang, 2001]. La necesidad de una mejor integración de IP y ATM llevó al desarrollo de la conmutación de etiquetas. Algunas de las razones que hacen interesante el uso de la

conmutación de etiquetas son:

- **Velocidad y retardo.-** El envío tradicional IP es muy lento para manejar las cargas de tráfico de Internet. La conmutación de etiquetas es mucho más rápida debido a que la etiqueta es usada como un apuntador de la tabla de envío, esto solo es realizado una vez en comparación con una tabla de enrutamiento cuyo acceso es hecho miles de veces.
- **Variación del retardo.-** Cada nodo en la red debe examinar la IP destino y compararla con una larga lista de potenciales IP destino. En la conmutación de etiquetas la trayectoria de los paquetes es establecida previo a su envío. Debido a esto se agiliza el envío de los paquetes, provocando una reducción en el jitter.
- **Escalabilidad.-** La conmutación de etiquetas permite asociar varias direcciones IP con una o pocas etiquetas.
- **Simplicidad.-** Existen varios métodos para asignar una etiqueta al tráfico del usuario, y una vez realizado esto, el envío del tráfico es simple.
- **Utilización de los recursos.-** Los mecanismos de control para asignar la etiqueta no deben de ser una carga para la red.
- **Control de las rutas.-** Se tiene un control de la trayectoria de envío del tráfico, lo cual ayuda a optimizar el uso de los recursos de la red mediante una mejor distribución del tráfico que circula en esta, lo cual se conoce comúnmente como ingeniería de tráfico [Black, 2002].

Varias compañías han tratado de combinar la operación de alta velocidad de la conmutación ATM con los procesos de enrutamiento de la capa IP. Cuatro ejemplos a destacar son: El enrutador de conmutación de celdas (CSR, Cell Switching Router) desarrollado por Toshiba, Conmutación IP (IP Switching) desarrollado por Ipsilon, Conmutación de etiquetas (Tag Switching) desarrollado por Cisco Systems y conmutación IP basada en enrutamiento agregado (Aggregate Route-based IP Switching) desarrollado por IBM.

En 1997 la IETF creó el grupo de trabajo MPLS para lograr la interoperabilidad entre las distintas tecnologías de conmutación de etiquetas.

III.2 Conmutación de Etiquetas Multiprotocolo

El encabezado de los paquetes contiene mucha más información de la necesaria para simplemente seleccionar el siguiente salto del paquete. Seleccionar el siguiente salto puede ser una tarea de tan solo dos funciones. La primera separa el conjunto completo de paquetes en un conjunto de clases equivalentes de envío (FECs, Forwarding Equivalence Classes). La segunda asigna cada FEC a un posible siguiente salto. Todos los paquetes que pertenecen a una FEC en particular siguen la misma trayectoria a través de la red.

Una FEC es un grupo de paquetes IP que son enviados de la misma manera por la red, por ejemplo, por la misma trayectoria o recibiendo el mismo tratamiento de envío.

En MPLS la asignación de un paquete a una FEC en particular puede basarse no

solo en su dirección IP destino como ocurre normalmente en las redes IP, sino también en la dirección IP fuente, en el puerto fuente o destino, o en el código DiffServ (DSCP, DiffServ Code Point) del encabezado IP.

En el envío IP convencional, mientras el paquete circula por la red, cada nodo en turno examina el paquete y lo asigna a una FEC. En MPLS, la asignación de un paquete a una FEC en particular se realiza solo una vez, al momento que este entra en la red. La FEC a la cual es asignado el paquete es codificada mediante un valor pequeño de longitud fija llamado *etiqueta*. La etiqueta es enviada con el paquete hacia el siguiente salto, es decir, los paquetes son etiquetados antes de ser enviados [Rosen *et al.*, 2001].

En MPLS, una vez que el paquete es asignado a una FEC, los enrutadores subsecuentes no analizan el encabezado del paquete, el envío de los paquetes es controlado completamente por las etiquetas [Rosen *et al.*, 2001]. Esto cuenta con algunas ventajas comparado con el envío tradicional de la capa de red, algunas de estas son:

- El envío de paquetes MPLS pueden hacerlo conmutadores que tengan la capacidad de analizar y reemplazar la etiqueta, y que no tengan la capacidad de analizar el encabezado de la capa de red.
- Las consideraciones que determinan la manera en que los paquetes son asignados a una FEC en particular pueden volverse más complicadas, sin que esto afecte a los enrutadores, ya que estos basan el envío de los paquetes en la etiqueta.
- Algunas veces es necesario que determinados paquetes viajen por una trayectoria

en particular, la cual es seleccionada en el momento que el paquete entra a la red. En MPLS, la etiqueta puede ser usada para representar esta trayectoria, evitando que esta tenga que ser llevada en el encabezado de la capa de red.

Algunas veces, los enrutadores analizan el encabezado IP del paquete no solo para decidir el siguiente salto, sino también para determinar sus requerimientos de calidad de servicio. MPLS permite que la prioridad o la clase de servicio del paquete puedan ser determinadas del valor de la etiqueta.

El concepto principal detrás de MPLS es la etiqueta. Una etiqueta es asignada a los paquetes cuando entran en la red MPLS y la red utiliza esta etiqueta, en lugar de la información del encabezado de la capa de red, para el envío de los paquetes hacia el nodo destino [Thomas, 2001]. Una etiqueta es un identificador corto, de longitud fija, con significado local, la cual es utilizada para identificar a una FEC. La etiqueta que es colocada a un paquete en particular, representa la FEC a la cual ha sido asignado este paquete.

El significado local de la etiqueta indica que el valor de la etiqueta solo tiene importancia en un enlace particular entre dos LSRs, los demás LSRs en la trayectoria pueden usar el mismo valor de etiqueta sin ningún conflicto. Debido a su significado local, el valor de la etiqueta puede cambiar en tanto el paquete recorre la red MPLS.

La trayectoria del paquete a través de la red está completamente determinada por la etiqueta inicial que le asigna el LSR de Ingreso a la red. Cada LSR en la trayectoria

cuenta con una tabla de asignación de etiquetas, esta tabla toma la interfaz de entrada y el valor de la etiqueta de entrada y les asigna una interfaz de salida y el valor de la etiqueta de salida a los paquetes.

III.3 Dominio MPLS

Un dominio MPLS es un conjunto de enrutadores que realizan operaciones de enrutamiento y envío de paquetes etiquetados y que se encuentren dentro del mismo dominio administrativo [Rosen *et al.*, 2001]. Se encuentra formado por los siguientes elementos:

- **LSR de Frontera.-** Conecta al dominio MPLS con un nodo que se encuentre fuera de este. Un LSR de frontera es llamado LSR de Ingreso cuando este recibe los paquetes del usuario, los clasifica en una FEC, genera el encabezado MPLS y le asigna una etiqueta. Si el encabezado de la capa de red del paquete contiene requerimientos de Calidad de Servicio, el LSR de Ingreso condicionará el tráfico de acuerdo a estos requerimientos. Un LSR de frontera es llamado LSR de Egreso cuando este recibe un paquete MPLS, remueve el encabezado MPLS y envía el paquete hacia su destino fuera del dominio MPLS.
- **LSR de Núcleo.-** También recibe el nombre de LSR de Tránsito o solo LSR, recibe paquetes MPLS y los envía hacia el siguiente LSR de acuerdo al valor de su etiqueta, se encarga de cambiar el valor de la etiqueta y solamente procesa el

encabezado MPLS.

- **Trayectoria Conmutada de Etiqueta (LSP).**- Se define como la trayectoria utilizada para el envío de paquetes dentro del dominio MPLS, debe establecerse antes de que puedan enviarse los paquetes.

En la figura 1 se presenta el esquema de un dominio MPLS; donde pueden observarse los elementos que forman un dominio MPLS, así como la asignación de la etiqueta a los datagramas IP.

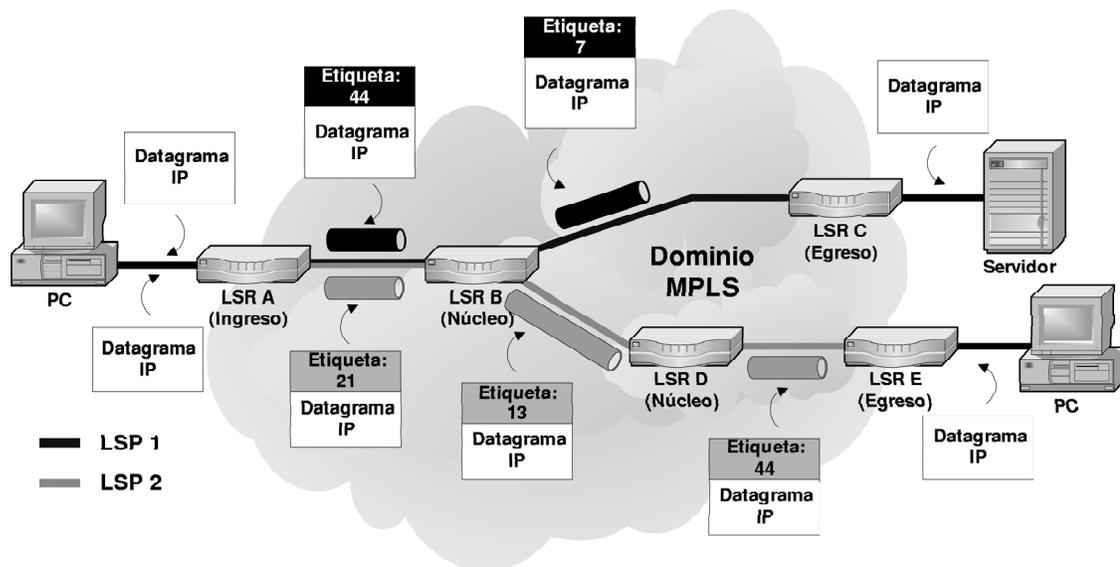


Figura 1. Dominio MPLS

III.4 El encabezado MPLS

El encabezado MPLS está formado de 4 octetos (32 bits). Se encuentra entre los encabezados de la capa de enlace de datos y de la capa de red. Es creado por el LSR de ingreso y utilizado por este mismo para determinar la FEC, la cual a su vez es usada para crear la etiqueta [Tappan *et al.*, 2001]. En la figura 2 se observan los distintos campos que forman el encabezado MPLS.

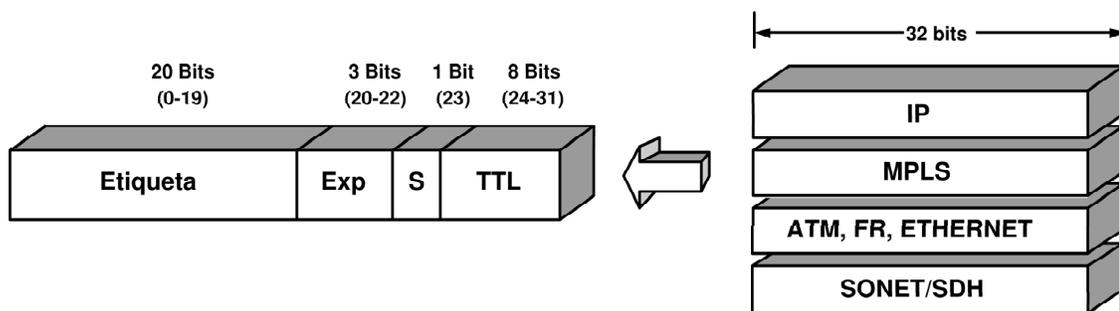


Figura 2. Encabezado MPLS

- **Etiqueta.-** Está formado de 20 bits (0-19) y lleva el valor de la etiqueta. Cuando un paquete etiquetado es recibido por un LSR, este utiliza la etiqueta de la parte superior de la pila de etiquetas para encontrar la información asociada con la etiqueta, la cual incluye el siguiente salto del paquete, etiqueta de salida, interfaz de salida o remover la etiqueta.
- **Experimental (Exp).-** Está formado de 3 bits (20-22); como su nombre lo indica, está reservado para uso experimental, aunque comúnmente es utilizado para ofrecer Calidad de Servicio. Debido a lo anterior este campo también recibe el nombre de CoS (Class of Service).

- **Pila de Etiquetas (S).**- Está formado de 1 bit (23), se encarga de informar a los enrutadores el estado de la pila de etiquetas. Cuando tiene un valor de 1, indica que el paquete solo lleva una etiqueta, si tiene un valor de 0, indica que el paquete lleva dos o más etiquetas.
- **Tiempo de vida (TTL).**- Esta formado de 8 bits. Define un límite en el número de saltos que puede hacer un paquete MPLS dentro de la red. Reemplaza el campo de límite de saltos del encabezado IP.

Este formato de encabezado solo se utiliza en redes de paquetes, tales como Ethernet, enlaces punto a punto (PPP, Point To Point Protocol) o redes que utilicen la tecnología de Paquetes sobre SONET (PoS, Packet over SONET). En el caso de redes ATM, se utilizan los campos VPI (Virtual Path Identifier) y VCI (Virtual Channel Identifier) para llevar el valor de la etiqueta. Los campos S, EXP y TTL no se utilizan ya que el formato del encabezado de las celdas ATM ya se encuentra definido.

III.5 Estructuras de datos en MPLS

Cada LSR dentro del dominio MPLS mantiene cuatro estructuras de datos para determinar como procesar los paquetes que recibe, por ejemplo, determinar el siguiente salto del paquete. Estas estructuras son: La Base de Datos de Etiquetas para envío al siguiente salto (NHLFE, Next Hop Label Forwarding Entry), Asignación FEC a NHLFE (FTN, FEC to NHLFE Map), Asignación de la Etiqueta de Arribo (ILM,

Incoming Label Map) y la última es la Tabla de Enrutamiento IP.

- **NHLFE.-** Contiene la información necesaria para el envío de los paquetes, tal como el siguiente salto del paquete, la etiqueta de entrada, la etiqueta de salida, la interfaz de salida, el encapsulado de la capa de enlace de datos a utilizar y la operación a realizar en la pila de etiquetas. Obtiene su información de la tabla de enrutamiento y de las bases de datos FTN e ILM.
- **FTN.-** Asocia cada FEC con un conjunto de NHLFEs. Se utiliza cuando los paquetes arriban sin etiquetar y tienen que ser etiquetados antes de ser enviados. Es empleada principalmente por los LSR de Frontera que son los que normalmente reciben paquetes sin etiquetar.
- **ILM.-** Asigna cada etiqueta de arribo a un conjunto de NHLFEs. Se emplea cuando los paquetes arriban etiquetados. Es empleada principalmente por los LSR de Núcleo que son los que normalmente reciben paquetes etiquetados. En caso de que el paquete tenga más de una etiqueta, la etiqueta superior es usada como índice dentro de la ILM [Rosen *et al.*, 2001].
- **Tabla de Enrutamiento IP.-** Contiene información acerca de la dirección IP del siguiente salto, las métricas asociadas con este destino y la interfaz por la que debe ser enviado el paquete para alcanzar el siguiente salto. Estos datos son utilizados para crear la NHLFE.

En la figura 3 se presentan las estructuras de datos mencionadas anteriormente. En ella se observa cómo al llegar paquetes sin etiquetar, la base de datos FTN se encarga de asignarlos a determinado elemento de la base de datos NHLFE, esta en base a la información que tiene, envía el paquete hacia su siguiente salto. Cuando llegan paquetes etiquetados, la base de datos ILM es la encargada de asignarles un elemento de la base de datos NHLFE.

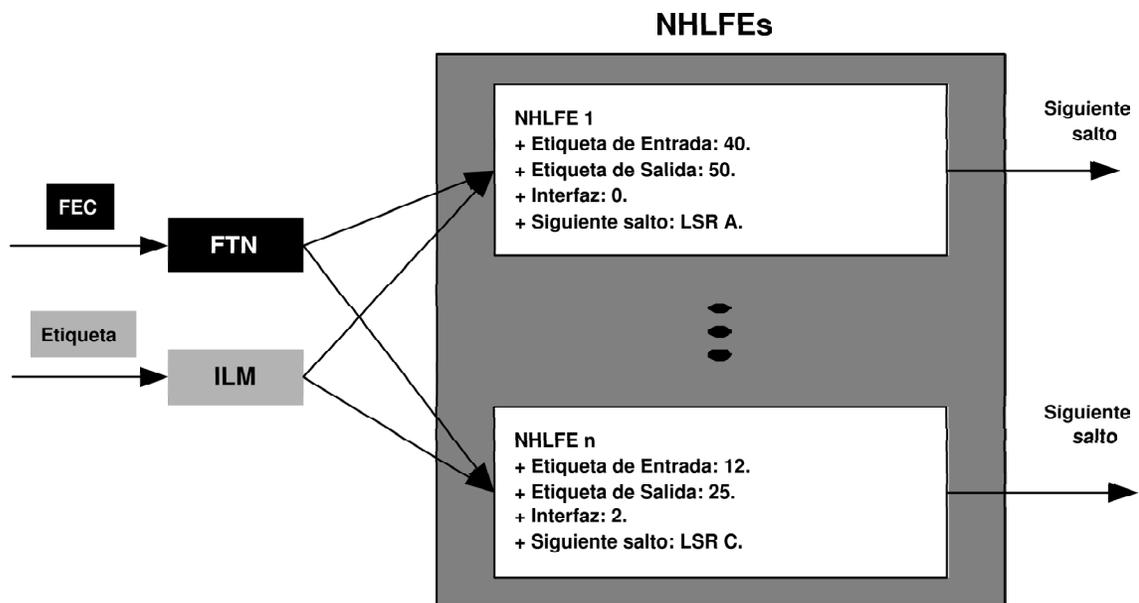


Figura 3. NHLFE, FTN e ILM

III.6 Protocolos de distribución de etiquetas

Un protocolo de distribución de etiquetas es un conjunto de procedimientos mediante el cual un LSR le informa a otro de las asociaciones etiqueta/FEC que ha hecho

para enviar tráfico entre ellos. Protocolos como BGP (Border Gateway Protocol) y RSVP (Resource Reservation Protocol) han sido modificados de manera que puedan llevar información de distribución de etiquetas, también han sido desarrollados nuevos protocolos, tales como el Protocolo de Distribución de Etiquetas (LDP, Label Distribution Protocol) y el Protocolo de Distribución de Etiquetas Basado en Restricciones (CR-LDP, Constraint-Based LDP)

III.7 Interoperabilidad de MPLS con Servicios Diferenciados (DiffServ)

Para que un proveedor de servicios tenga la capacidad de ofrecer Servicios Diferenciados a través de su red MPLS, es necesario contar con uno o varios mecanismos que aseguren que cada clase de servicio reciba su correspondiente PHB en cada LSR por el cual circule dentro del dominio MPLS.

Debido a que el DSCP (DiffServ Code Point) se encuentra en el encabezado IP y como los LSRs no examinan el encabezado IP para enviar los paquetes, se necesita de un mecanismo que pueda determinar el PHB apropiado a partir del encabezado MPLS. Con este fin la IETF en su RFC 3270 define dos mecanismos:

- LSP con Clase de Calendarización PHB deducida del campo EXP (E-LSP, EXP Inferred PHB Scheduling Class LSP).

- LSP con Clase de Calendarización PHB deducida solo de la etiqueta (L-LSP, Label Only Inferred PHB Scheduling Class LSP).

Antes de analizar estos dos mecanismos, es necesario definir los siguientes conceptos:

- **Comportamiento por Salto (PHB).**- Se define como el tratamiento DiffServ (calendarización/descarte) aplicado por un enrutador a todos los paquetes que tienen que recibir el mismo servicio DiffServ, es decir, tienen el mismo DSCP.
- **Agregado de Comportamiento (BA).**- Es un conjunto de paquetes con el mismo DSCP y por lo tanto reciben el mismo PHB en los enrutadores.
- **Agregado de Orden (OA, Ordered Aggregate).**- Es un conjunto de BAs que comparten una restricción de orden. Se refiere a que los paquetes pertenecientes a un mismo flujo no pueden ser desordenados si difieren solo en la prioridad de descarte, es decir, deben mantener el mismo orden desde el LSR de Ingreso hasta el LSR de Egreso, por ejemplo, los paquetes que pertenecen a las clases DiffServ AF21, AF22 y AF23 deben ser asignados a la misma cola [Black, 2002].
- **Clase de Calendarización PHB (PSC, PHB Scheduling Class).**- Conjunto de uno o más PHBs que utilizan los BAs que pertenecen a determinado OA. Se refiere a que los paquetes con el mismo PHB deben ser enviados por la misma LSP. Por ejemplo, AF1x es una clase de calendarización PHB que contiene los PHBs AF11, AF12 y AF13 [Le Faucher *et al.*, 2002].

III.7.1 E-LSP

Se conoce como E-LSP debido a que el PHB del paquete es determinado del valor del campo EXP del encabezado MPLS. Cada LSR en la trayectoria utiliza el valor de la etiqueta para determinar el siguiente salto del paquete y el valor del campo EXP para determinar el PHB (calendarización y prioridad de descarte) que debe aplicar al paquete durante el proceso de envío. Los E-LSPs permiten utilizar hasta un máximo de 8 PHBs por FEC [Semeria, 2002], lo cual pone al descubierto una de las limitaciones de los E-LSP, ya que DiffServ permite hasta 64 PHBs gracias a que el campo ToS cuenta con 6 bits, en tanto el campo EXP solo tiene un tamaño de 3 bits.

La asignación de los PHBs hacia el campo EXP del encabezado MPLS puede realizarse en el instante en que se establece la LSP de los paquetes, o puede ser configurada manualmente por el administrador del sistema.

En la figura 4 se presenta un ejemplo de un E-LSP. En este caso se observa que se utilizan tres PHBs, EF (Expedited Forwarding), AF (Assured Forwarding) y BE, en tanto se transporta un flujo agregado de tráfico desde el LSR de Ingreso hasta el LSR de Egreso.

El LSR de Ingreso es responsable de analizar los paquetes IP del usuario, asignarles el valor de etiqueta, configurar apropiadamente los bits del campo EXP y colocarlos en la cola que les corresponde. Además debe contar con una tabla que le permita asignar cada PHB en un valor del campo EXP. Los LSR de Núcleo deciden el siguiente salto

del paquete en base al valor de su etiqueta y lo colocan en la cola adecuada de acuerdo al valor del campo EXP. Finalmente, el LSR de Egreso, remueve el encabezado MPLS y coloca en la cola y envía el paquete en base al contenido del encabezado IP.

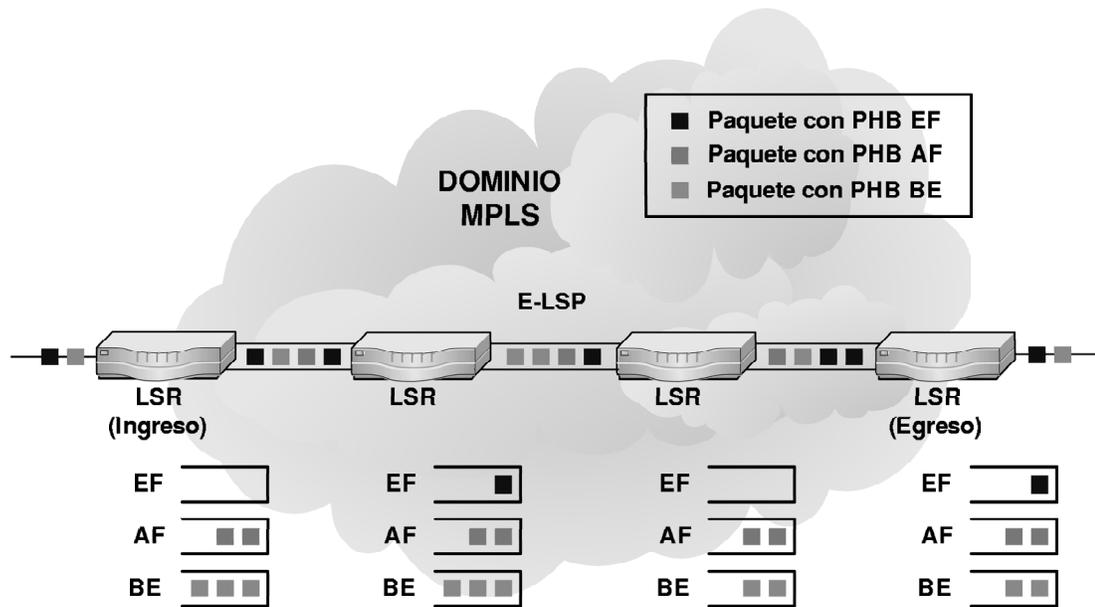


Figura 4. E-LSP

Es importante mencionar que todos los LSRs que formen el E-LSP deben de contar con la misma tabla de asignación PHB-EXP. De no ser así, el campo EXP puede ser reescrito indebidamente por algún LSR, provocando que los paquetes pertenecientes a cierto PHB reciban un tratamiento que no les corresponde.

Este tipo de trayectorias E-LSP sólo puede utilizarse en redes de paquetes, tales como Ethernet y Paquetes sobre SONET, no así en redes ATM ya que las celdas ATM no cuentan con el campo EXP.

III.7.2 L-LSP

Utilizan el valor de la etiqueta para decidir el siguiente salto del paquete y el PHB a aplicar a este mismo. Cuando se utiliza el encabezado MPLS, la prioridad de descarte del paquete es llevada en el campo EXP. Para el caso de redes MPLS sobre ATM, la prioridad de descarte es llevada dentro del campo CLP (Cell Loss Priority) del encabezado ATM.

En lugar de establecer una sola LSP entre el LSR de Ingreso y el LSR de Egreso, un LSR de Ingreso puede establecer múltiples LSPs entre él y un LSR de Egreso, donde cada LSP transporta el tráfico perteneciente a un par FEC-OA, es decir, cada LSP es configurado con los requerimientos de Calidad de Servicio de una clase de calendarización PSC en particular.

En la figura 5 se presenta un ejemplo de un L-LSP. En él, se establecen tres L-LSP, uno para cada una de tres diferentes clases de tráfico, en este caso EF, AF1x y BE. Por supuesto, cada L-LSP está configurado con los requerimientos de retardo y bajas pérdidas de cada clase de tráfico.

El LSR de Ingreso, en base a la dirección IP destino y el DSCP del encabezado IP del paquete, le asigna un valor de etiqueta que coloque al paquete dentro del L-LSP apropiado. De acuerdo a lo anterior se puede decir que un LSR de Ingreso establece una relación entre una etiqueta, una FEC y un PHB. Los LSR de Núcleo analizan el valor de la etiqueta y de acuerdo a este determinan el siguiente salto y la clase de calendarización

del paquete. Finalmente, el LSR de Egreso remueve el encabezado MPLS y coloca en la cola y envía el paquete de acuerdo al contenido del encabezado IP.

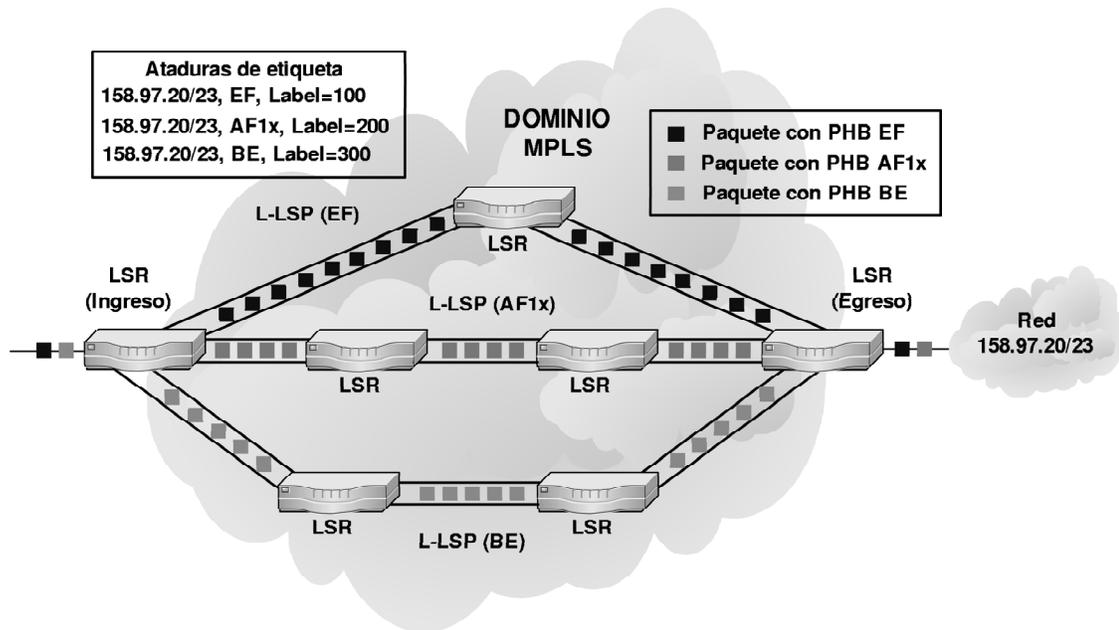


Figura 5. L-LSP

En comparación con las trayectorias E-LSP, las trayectorias L-LSP no se encuentran limitadas a 8 PHBs por FEC, si no que pueden establecer un conjunto de L-LSPs que permitan utilizar los 64 PHBs que establece DiffServ. Además, las trayectorias L-LSP sí pueden ser utilizadas en redes MPLS sobre ATM. Sus desventajas son expuestas al momento de su configuración, la cual es compleja, además de que tener varios L-LSPs complica la administración de la red.

Una vez analizadas las dos arquitecturas disponibles para la interoperabilidad de MPLS y DiffServ se decidió modelar una arquitectura E-LSP ya que esta es la que se

ajusta mejor a la topología de la Red-CUDI y su administración es de menor complejidad que una arquitectura L-LSP.

III.8 Propuesta de Enrutadores de Conmutación de Etiquetas (LSR)

En esta sección se presenta la arquitectura propuesta para un LSR de Frontera y un LSR de Núcleo, para implementar el modelo de E-LSP para ofrecer Servicios Diferenciados en una red MPLS [Rouhana, 2000].

Primero es necesario definir de que manera se relacionarán las clases de servicio de DiffServ con las clases de servicio que se utilizan en MPLS. La Tabla I muestra las relaciones definidas en este trabajo de investigación.

Tabla I. Clases de Servicio propuestas

| <i>Servicios Diferenciados</i> | | | | | <i>MPLS</i> | | |
|--------------------------------|------------|--------|-----|--------|-------------|-----|----------|
| Servicio | Aplicación | | | ToS | Servicio | EXP | Descarte |
| Premium | Video | | | 111111 | Oro | 111 | N/A |
| | Voz | | | 111110 | | 110 | N/A |
| Asegurado | Olímpico | Oro | FTP | 100110 | Plata | 101 | Baja |
| | | | | | | 100 | Alta |
| | | Plata | WWW | 100010 | Bronce | 011 | Baja |
| Bronce | SMTP | 100000 | 010 | Alta | | | |
| Best Effort | Tráfico BE | | | 000000 | Best Effort | 000 | N/A |

Los mecanismos de Calidad de Servicio empleados en las distintas etapas de los LSR son los siguientes: clasificadores multicampo (MF, Multifield), acondicionadores del tipo

“Leaky Bucket” y “Token Bucket”, WRED (Weighted Random Early Detection) para el control de admisión y calendarizadores WFQ (Weighted Fair Queuing). En [Caballero Cárdenas, 2002] se puede encontrar un análisis detallado de los mecanismos anteriores. Se decidió utilizar los mecanismos mencionados ya que estos se encuentran disponibles en los enrutadores Cisco de la serie 7204 [Cisco Press, 2001], que forman la dorsal de la red Internet2 de México, la cual se utilizará en la simulación del protocolo MPLS.

III.8.1 Arquitectura de un LSR de Frontera

En la figura 6 se presentan las distintas etapas que componen la arquitectura de un LSR de Frontera.

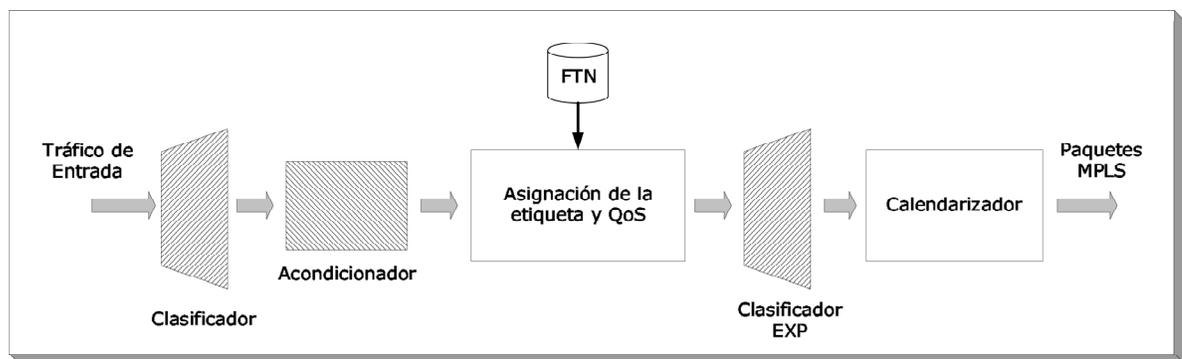


Figura 6. Arquitectura de un LSR de Frontera

La primera etapa es un clasificador multicampo, el cual únicamente se requiere en las fronteras de la red MPLS. Se encarga de recibir el flujo de tráfico del usuario y asignarlo a una clase equivalente de envío en base al contenido del encabezado IP de los paquetes. En este caso el tráfico se clasificó de acuerdo al tipo de aplicación (video,

voz, ftp, etc.) y a su dirección IP destino.

La segunda etapa es un acondicionador de tráfico. Se encarga de mantener el flujo de tráfico de cada clase dentro de los parámetros acordados, tales como tasa de transmisión y tamaño de la ráfaga. El acondicionador consiste de leaky buckets asociados al tráfico del Servicio Premium (video y voz) y Best Effort; los paquetes pertenecientes a estos servicios que no cumplan con el perfil de tráfico acordado son descartados. El Servicio Asegurado (FTP, WWW y SMTP) tiene asociados token buckets, los paquetes que se encuentren fuera del perfil de tráfico son marcados con una prioridad de descarte mayor.

La etapa de asignación de la etiqueta y QoS se auxilia de la base de datos FTN para colocar el encabezado MPLS al paquete, con los valores de etiqueta y del campo EXP que corresponden a la clase de tráfico que pertenece.

La siguiente etapa es la del clasificador del campo EXP, clasifica los paquetes en las clases de servicio de MPLS (Oro, Plata, Bronce y Best Effort) de acuerdo al valor del campo EXP del encabezado MPLS.

Por último se tiene la etapa de calendarización. Cuenta con un mecanismo de control de admisión para cada clase de tráfico. La clase Oro y la clase Best Effort tienen asociadas el mecanismo “Drop Tail” para el almacenamiento de los paquetes en la cola, este mecanismo descarta todos los paquetes que arriban cuando la cola está llena . Las clases Plata y Bronce tienen asociado el mecanismo WRED, ya que se necesita de un mecanismo que tome en cuenta la prioridad de descarte (alta o baja) de los paquetes

al momento de asignarles un espacio en la cola. Finalmente, el mecanismo WFQ se encarga de dar servicio a la cola de cada clase de tráfico, tomando en cuenta el peso asignado a cada una de estas.

III.8.2 Arquitectura de un LSR de Núcleo

En la figura 7 se presentan las distintas etapas que componen la arquitectura de un LSR de Núcleo.

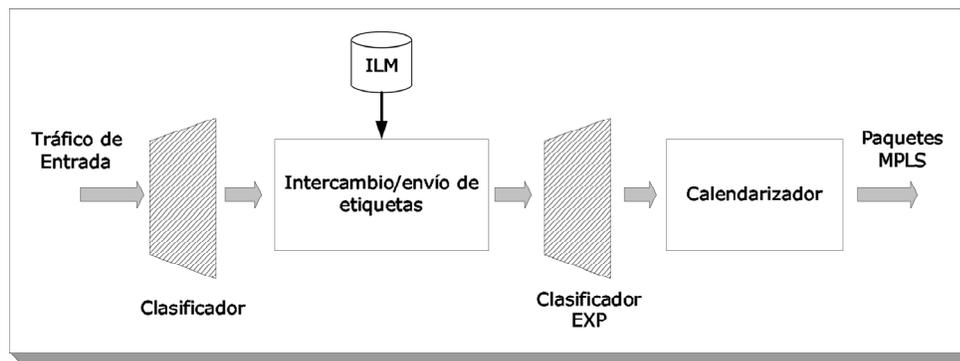


Figura 7. Arquitectura de un LSR de Núcleo

La primera etapa es un clasificador de etiquetas. Se encarga de recibir el flujo de tráfico de los LSRs de Frontera y/o otro LSR de Núcleo, identificar la clase de tráfico a la que pertenecen los paquetes y su nodo destino de acuerdo al valor de la etiqueta del encabezado MPLS.

La segunda etapa es la de intercambio y envío de etiquetas. Recibe los paquetes clasificados en la etapa anterior, remueve su etiqueta de entrada y le coloca su etiqueta de salida en base a la información de la base de datos ILM.

La etapa del clasificador del campo EXP y la etapa del calendarizador realizan las mismas funciones de clasificación, control de admisión y calendarización, tanto en los LSR de Núcleo como en los LSR de Frontera.

En el siguiente capítulo se presentan los modelos de simulación implementados en el simulador de redes OPNET Modeler para LSRs de Frontera y LSRs de Núcleo, así como el modelo de red donde se implementó el protocolo MPLS.

Capítulo IV

Implementación de los Modelos de Simulación

IV.1 Introducción

Una vez hecho el análisis teórico, se procede al modelado y simulación del protocolo MPLS. Con este fin se utilizó el simulador de redes OPNET Modeler, en su versión 9.0. En base a la experiencia adquirida de trabajos de tesis previos se tomó la decisión de que este era el simulador adecuado para llevar al cabo la implementación de los modelos.

Dichos modelos se implementaron de acuerdo a la topología de la dorsal de la red de Internet 2 de México, conocida también con el nombre de Red-CUDI (Corporación Universitaria para el Desarrollo de Internet). Mayor información acerca de la Red-CUDI puede obtenerse en el Portal de Internet de CUDI (www.cudi.edu.mx).

En la figura 8 se observa cómo la dorsal se encuentra formada por los nodos Gigapops (nodos de acceso a la red de Internet 2 y acrónimo de Gigabit Point of Presence) de Tijuana, Guadalajara, Monterrey, Ciudad Juárez y el Distrito Federal. A los Gigapops se conectan los nodos de Asociados Académicos, tales como CICESE, UACJ (Univer-

sidad Autónoma de Ciudad Juárez), U de G (Universidad de Guadalajara), ITESM (Instituto Tecnológico y de Estudios Superiores de Monterrey) y UNAM (Universidad Nacional Autónoma de México), por mencionar algunos, formando entre todos estos nodos la Red-CUDI.

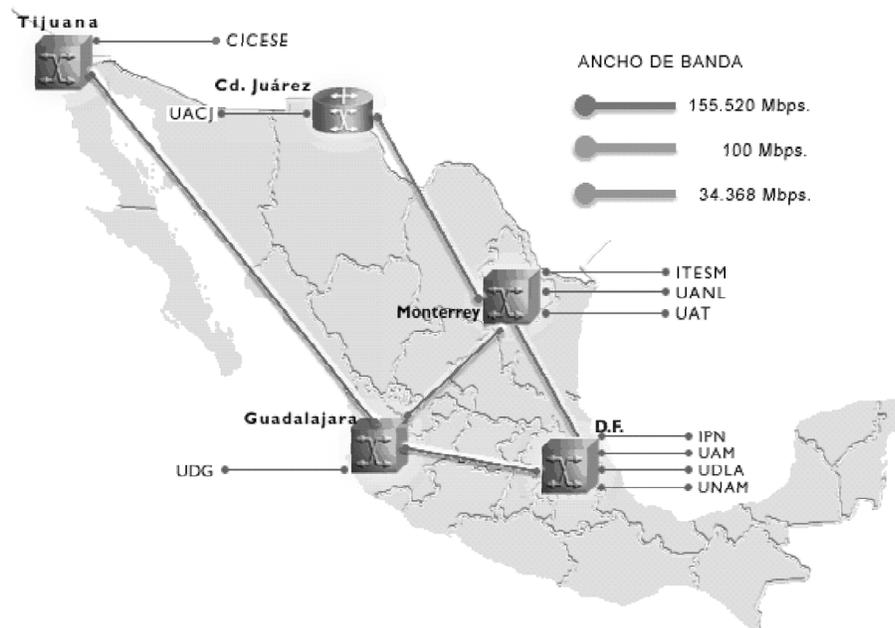


Figura 8. Mapa de la red Internet 2-México

Con el propósito de tener una justificación y una opción más de comparación, para llevar al cabo la implementación del protocolo MPLS en la Red-CUDI, se realizaron modelos para dos casos de configuraciones posibles de la dorsal, los cuales son:

1. DiffServ sobre ATM utilizando 6 PVCs.
2. MPLS sobre SONET.

El uso del simulador OPNET implica la definición de un modelo de red, varios modelos de nodos y de procesos. Debido a esto, en las siguientes secciones se estarán presentando estos tres tipos de modelos.

IV.2 Diffserv sobre ATM utilizando 6 PVCs

Para este caso los mecanismos de Calidad de Servicio fueron modelados a nivel de capa de red, ya que, en la práctica esta es la única manera en la que pueden ser configurados en la interfaz ATM de los Gigapops, además, esta interfaz solo permite configurar clases de servicio UBR (Unspecified Bit Rate) [Cisco Press, 2003]. Se definió un PVC (Private Virtual Circuit) de tipo UBR para cada clase de tráfico DiffServ, por lo que, el tráfico cuyo caudal sobrepase la Tasa Pico de Celdas (PCR, Peak Cell Rate) del PVC, será descartado.

IV.2.1 Modelo de Red

Este modelo de red no incluye los Gigapops de Monterrey y Ciudad Juárez y por lo tanto tampoco a los nodos de Asociados Académicos conectados a ellos. Esto se hizo con la finalidad de optimizar los tiempos de simulación y dedicar un mayor tiempo al análisis de los modelos MPLS sobre SONET.

En la figura 9 podemos observar cuatro tipos de nodos: nodos generadores de tráfico, nodos de Asociados Académicos, nodos Gigapops y nodos de recepción de tráfico y

captura de estadísticas. Los nodos generadores de tráfico son de 5 tipos: video, voz, FTP (File Transfer Protocol), WWW (World Wide Web) y SMTP (Simple Mail Transfer Protocol), además se incluye un nodo generador de tráfico al cual se le proporciona un tratamiento BE (Best Effort). Los nodos generadores de tráfico utilizan enlaces Fast Ethernet para conectarse a los nodos de Asociados Académicos de CICESE y la U de G. Los nodos de Asociados Académicos pertenecen a CICESE, U de G, UNAM, IPN (Instituto Politécnico Nacional), UAM (Universidad Autónoma de México) y UDLA (Universidad de Las Américas). Se conectan a su correspondiente Gigapop mediante enlaces E3 (34 Mbps). Los Gigapops de Tijuana, Guadalajara y el Distrito Federal se conectan mediante enlaces SMT-1 (155 Mbps). Los nodos de Asociados Académicos IPN, UNAM, UDLA y UAM actúan como los nodos de recepción de tráfico y captura de estadísticas.

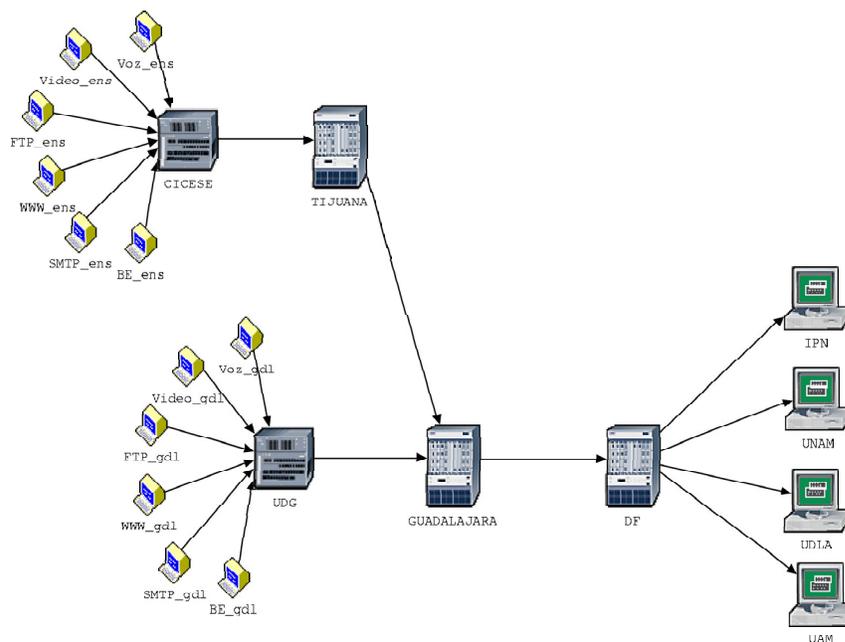


Figura 9. Modelo de red ATM - 6 PVCs

IV.2.2 Modelo de Nodo

Los modelos de nodos definen la arquitectura interna de cada uno de los nodos que forman la Red-CUDI. Estos modelos se presentan a continuación.

IV.2.2.1 Modelo de Nodo de Generadores de Tráfico

En la figura 10 se presenta el modelo de un nodo generador de tráfico, el cual se compone de una fuente generadora de paquetes IP y su transmisor. Este modelo es el mismo para los 6 tipos de nodos generadores de tráfico, la diferencia entre ellos se encuentra en el modelo de procesos de su fuente generadora, donde cada uno de ellos está hecho en base a las características del tipo de tráfico que modelan. En [Caballero Cárdenas, 2002] y el Apéndice A se presenta un análisis más detallado de estos modelos.



Figura 10. Modelo de nodos generadores de tráfico

IV.2.2.2 Modelo de Nodo de Asociados Académicos

En la figura 11 se presenta el modelo de nodo implementado en los Asociados Académicos CICESE y U de G, los cuales son los nodos que inyectan el tráfico de los nodos generadores hacia la dorsal de la red. Estos modelos se encuentran basados en los utilizados en [Caballero Cárdenas, 2002], de hecho únicamente se les agregó el

bloque de segmentación de los paquetes IP. Este último bloque se encarga de dividir los paquetes IP en celdas ATM y enviarlas a través de los PVCs.

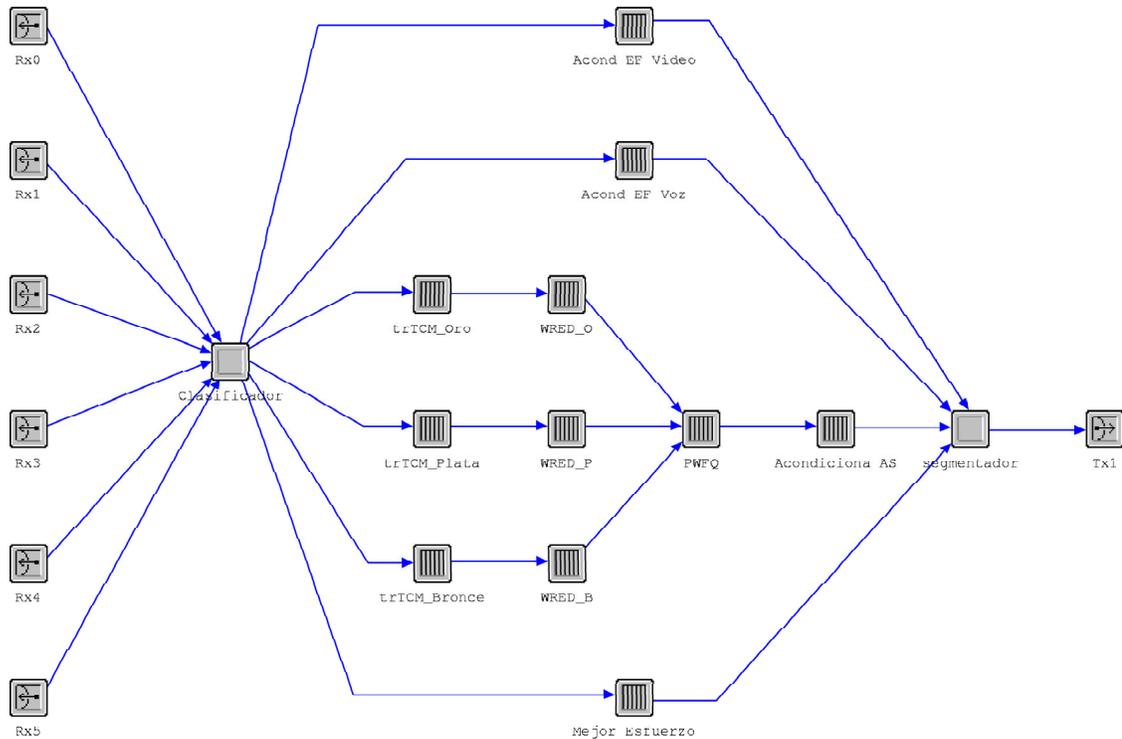


Figura 11. Modelo de nodos de Asociados Académicos

IV.2.2.3 Modelo de Nodo para Gigapops

En la figura 12 se presenta el modelo de nodo implementado en los Gigapops de Tijuana, Guadalajara y el Distrito Federal. El bloque de reensamble se encarga de identificar las celdas que pertenecen a cada paquete para volver a formarlos y enviarlos hacia los bloques de clasificación, calendarización y acondicionamiento, todos estos tomados de [Caballero Cárdenas, 2002]. Por último la etapa de segmentación divide

una vez más los paquetes en celdas ATM y las envía por su correspondiente PVC.

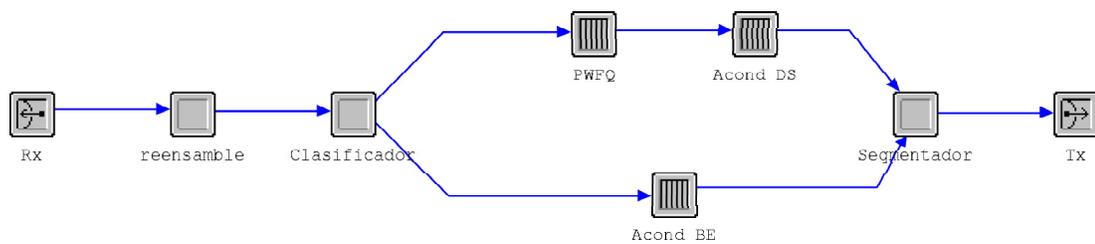


Figura 12. Modelo de nodos de Gigapops

IV.2.2.4 Modelo de Nodo para Recepción de Tráfico y Captura de Estadísticas

En la figura 13 se presenta el modelo de nodo implementado en los nodos de captura de estadísticas IPN, UNAM, UDLA y UAM. Se encuentra formado de bloques de recepción, reensamble y captura de estadísticas. El bloque de reensamble vuelve a formar los paquetes para que sean procesados por el bloque de captura de estadísticas. Éste último mide los parámetros de Calidad de Servicio como son: retardo extremo a extremo, variación del retardo y pérdida de paquetes.

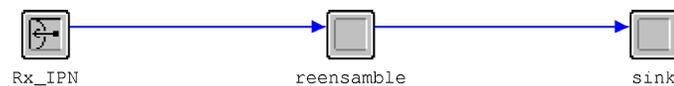


Figura 13. Modelo de nodo para recepción de tráfico

IV.2.3 Modelo de Procesos

Como ya se ha mencionado, varios de los modelos de procesos de los distintos bloques de los modelos de nodos fueron tomados de [Caballero Cárdenas, 2002], por lo tanto, en esta sección solo se estarán presentando los modelos de procesos de los bloques que fueron agregados.

IV.2.3.1 Modelo de Procesos para el Segmentador ATM

La figura 14 muestra el modelo de procesos para el segmentador ATM.

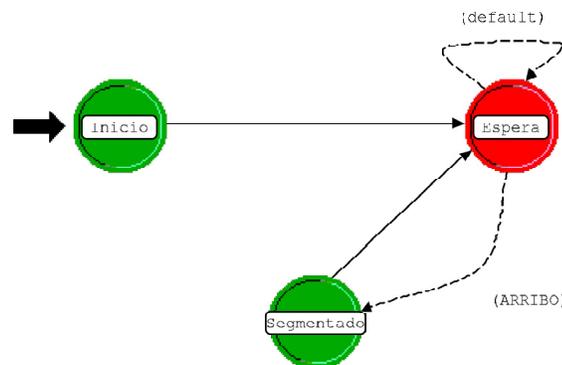


Figura 14. Modelo de procesos para el segmentador ATM

El modelo se compone de tres estados: Inicio, Espera y Segmentación. En el estado de Inicio se realiza la inicialización de variables y se pasa al estado de Espera, en el cual se mantiene la ejecución del modelo hasta que ocurre una interrupción de arribo de paquete. Esta interrupción pasa la ejecución del programa hacia el estado de Segmentación, el cual obtiene el paquete IP, calcula la longitud de éste y el valor obtenido lo divide por 384, que es la longitud de la carga útil (en bits) de una celda ATM. El

resultado de esta operación indica el número de celdas en que debe dividirse el paquete. Cada celda lleva los valores de VPI/VCI acordes al PVC a través del cual deben ser transmitidas, además, llevan un identificador de celda y la longitud del paquete IP para poder reconstruirlo en el proceso inverso.

IV.2.3.2 Modelo de Procesos para el Ensamblador ATM

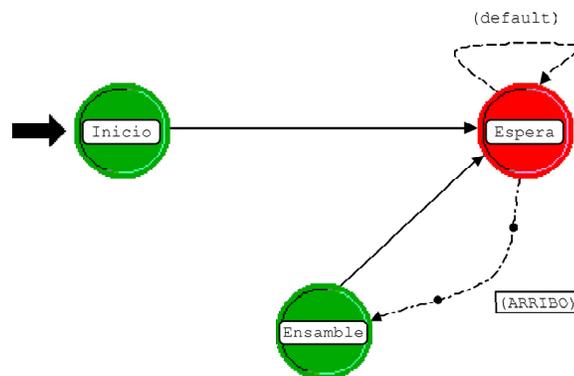


Figura 15. Modelo de procesos para el ensamblador ATM

La figura 15 nos muestra el modelo de proceso para el ensamblador ATM, el cual se compone de tres estados: Inicio, Espera y Ensamble. En el estado de Inicio se inicializan variables, el estado de Espera representa el tiempo en el cual no ha llegado ningún paquete. En el momento en que ocurre una interrupción de arribo de un paquete, la ejecución del programa pasa al Estado Ensamble, el cual mediante el contenido de los campos de identificación de celda y longitud del paquete IP, reconstruye los paquetes.

IV.3 MPLS sobre SONET

Se definieron los modelos tomando en cuenta una evolución de la Red-CUDI a una red de Paquetes sobre SONET (PoS, Packets over SONET) o bien SDH (Synchronous Digital Hierarchy). Para llevar a la práctica este modelo, es necesario integrar una interfaz PoS a los Gigapops y a los nodos de Asociados Académicos de la red.

IV.3.1 Modelo de Red

Esta vez fue necesario definir dos modelos de red para obtener los resultados requeridos para hacer una buena evaluación del desempeño del protocolo MPLS, como protocolo de transporte de distintos tipos de tráfico y ser capaz de proporcionar Calidad de Servicio a los usuarios de la Red-CUDI. Estos modelos se presentan en las siguientes secciones.

IV.3.1.1 Modelo de Red MPLS - Dorsal Tij-Gdl-D.F.

Este modelo de red no incluye el Gigapop de Monterrey y se compone de los mismos nodos Gigapops, de Asociados Académicos, generadores de tráfico y de recepción de tráfico y captura de estadísticas del modelo de red DiffServ sobre ATM. Se realizó con el objetivo de hacer una comparación más precisa con los resultados obtenidos en [Caballero Cárdenas, 2002], en cuanto a retardo extremo a extremo, variación del retardo y pérdida de paquetes. La figura 16 muestra el modelo de Red MPLS.

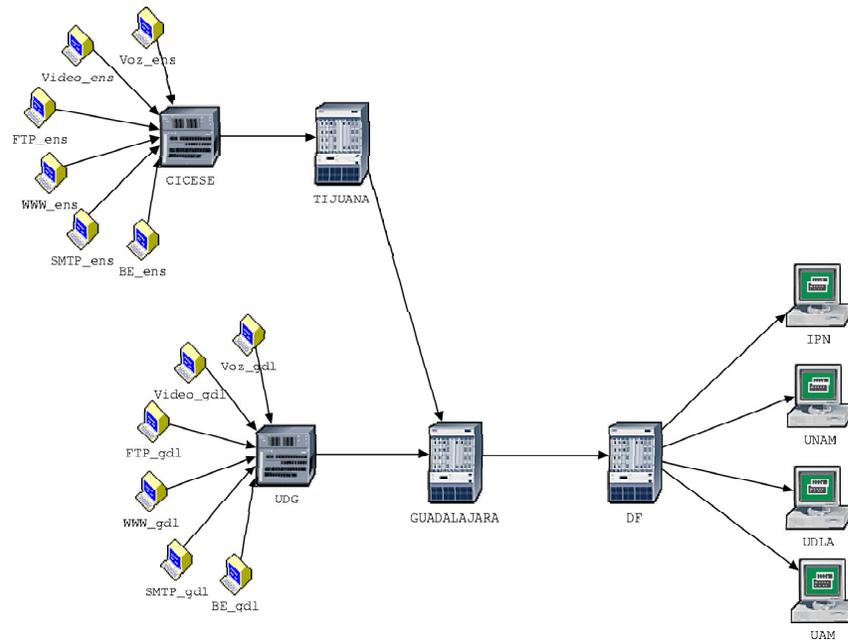


Figura 16. Modelo de red MPLS - Dorsal Tij-GDL-D.F.

IV.3.1.2 Modelo de Red MPLS - Dorsal Completa

La figura 17 muestra el modelo de red MPLS - Dorsal Completa.

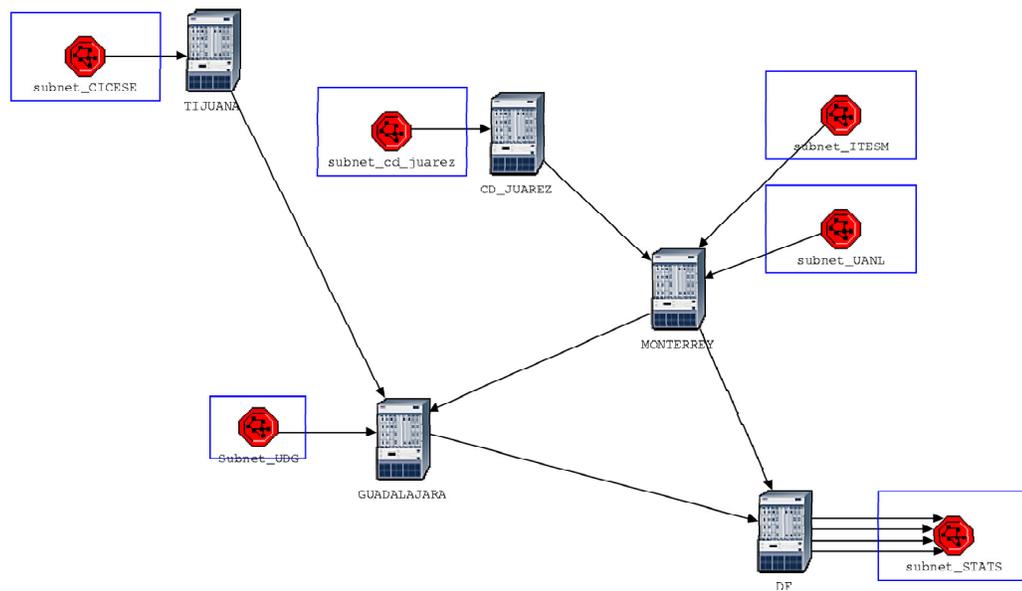


Figura 17. Modelo de red MPLS - Dorsal Completa

Este modelo de red se encuentra formado por los Gigapops de Tijuana, Guadalajara, Monterrey, Ciudad Juárez y el Distrito Federal, donde cada uno corresponde a un LSR de Núcleo. Los nodos de subred CICESE, U de G, UACJ, ITESM y UANL, contienen al LSR de Frontera de cada Asociado Académico y sus nodos generadores de tráfico, respectivamente. El nodo de subred "stats" contiene a los nodos de recepción de tráfico y captura de estadísticas IPN, UNAM, UDLA y UAM. El modelo tiene como objetivo analizar el comportamiento del protocolo MPLS bajo un esquema completo de la dorsal de la Red-CUDI.

IV.3.2 Modelo de Nodo

En esta sección se presentan los modelos de nodo que definen la arquitectura interna de un LSR de Frontera y un LSR de Núcleo, definidas en el capítulo anterior. Además del modelo de nodo para los nodos de recepción de tráfico y captura de estadísticas. Los modelos de nodo de los generadores de tráfico son los mismos que los utilizados en el modelo de DiffServ sobre ATM. Todos los modelos corresponden a los dos casos de modelos de red presentados en la sección anterior.

IV.3.2.1 Modelo de Nodo para LSR de Frontera

En la figura 18 se observa el modelo de nodo para un LSR de Frontera. Está constituido por seis receptores de tráfico, uno por cada nodo generador de tráfico, cinco bloques de procesos, de los cuales el primero representa el proceso para el clasificador

multicampo, el segundo representa los mecanismos de acondicionamiento de tráfico, el tercer bloque de proceso contiene a la base de datos FTN y al mecanismo de asignación de etiquetas, el siguiente bloque representa el proceso para el clasificador del campo EXP y el último bloque de procesos representa a la etapa de calendarización que incluye a los mecanismos WRED y WFQ. Por último, el modelo incluye un transmisor encargado de enviar el tráfico hacia la dorsal.

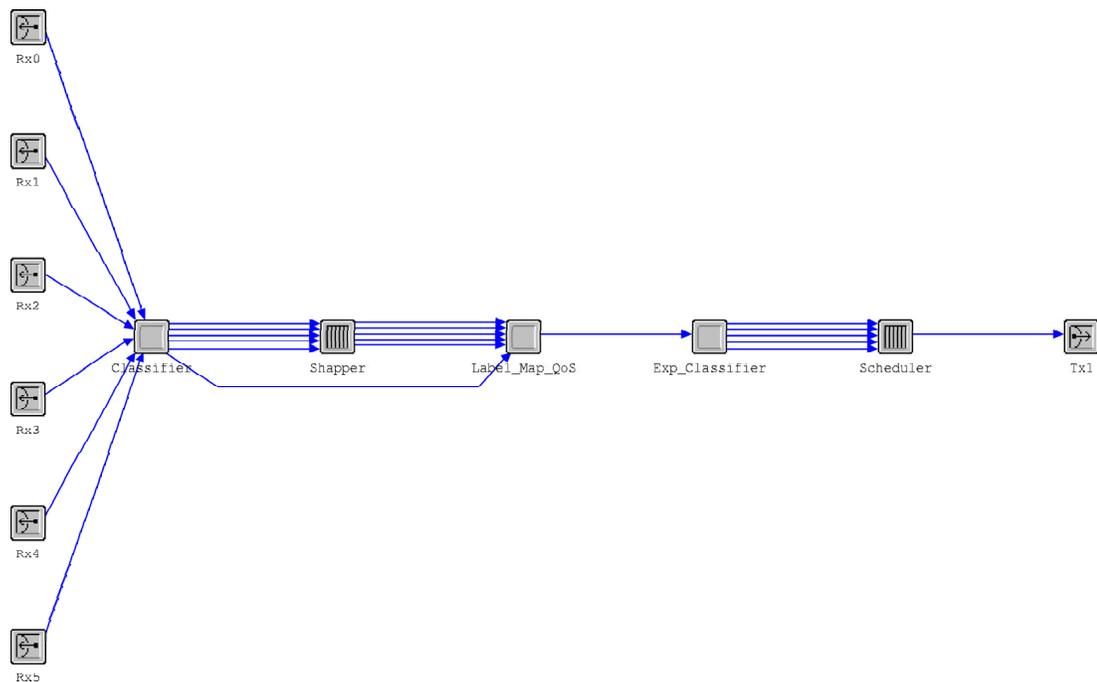


Figura 18. Modelo de nodo para LSR de Frontera

Este modelo de nodo se implementó en los nodos de Asociado Académico CICESE, U de G, UACJ, ITESM y UANL, ya que todos ellos representan los nodos de ingreso de tráfico hacia el dominio MPLS.

IV.3.2.2 Modelo de Nodo para LSR de Núcleo

En la figura 19 se observa el modelo de nodo para un LSR de Núcleo. Está constituido por un bloque de recepción del tráfico proveniente del LSR de Frontera u otro LSR de Núcleo. Cuatro bloques de procesos, de los cuales uno representa el proceso para el clasificador de etiquetas, un segundo bloque de procesos que incluye a la base de datos ILM y al mecanismo de intercambio de etiquetas, un tercer bloque de procesos que representa al clasificador del campo EXP y un cuarto bloque que representa la etapa de calendarización que incluye a los mecanismos WRED y WFQ.



Figura 19. Modelo de nodo para LSR de Núcleo

Este modelo de nodo se implementó en los nodos Gigapops de Tijuana, Guadalajara, Monterrey, Ciudad Juárez y el Distrito Federal, ya que éstos representan los nodos internos del dominio MPLS.

IV.3.2.3 Modelo de Nodo para Recepción de Tráfico y Captura de Estadísticas

En la figura 20 se presenta el modelo de nodo implementado en los nodos de captura de estadísticas IPN, UNAM, UDLA y UAM. Se encuentra formado por un receptor y un bloque de procesos para captura de estadísticas. Éste último se encarga de medir

los parámetros de Calidad de Servicio como son: retardo extremo a extremo, variación del retardo y pérdida de paquetes.



Figura 20. Modelo de nodo para Captura de Estadísticas

IV.3.3 Modelo de Procesos

En esta sección se presentarán los modelos de procesos de los distintos bloques que forman a los modelos de nodo.

IV.3.3.1 Modelo de Procesos para el Clasificador Multicampo

En la figura 21 se presenta el modelo de procesos que se implementó para el clasificador multicampo. El Estado “Init” indica el inicio del proceso, el estado “Idle” mantiene la ejecución del proceso en espera del arribo de un paquete. Una vez que arriba un paquete la ejecución del proceso pasa al estado “FEC”, el cual lleva al cabo la clasificación de los paquetes y los asigna a una FEC de acuerdo al contenido del encabezado IP del paquete y su dirección IP destino.

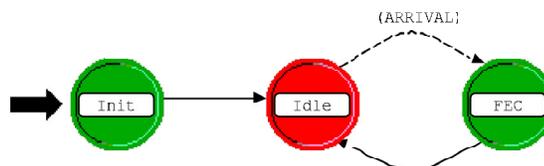


Figura 21. Modelo de procesos para el Clasificador Multicampo

El diagrama de flujo empleado en la programación del clasificador multicampo se presenta en la figura 22.

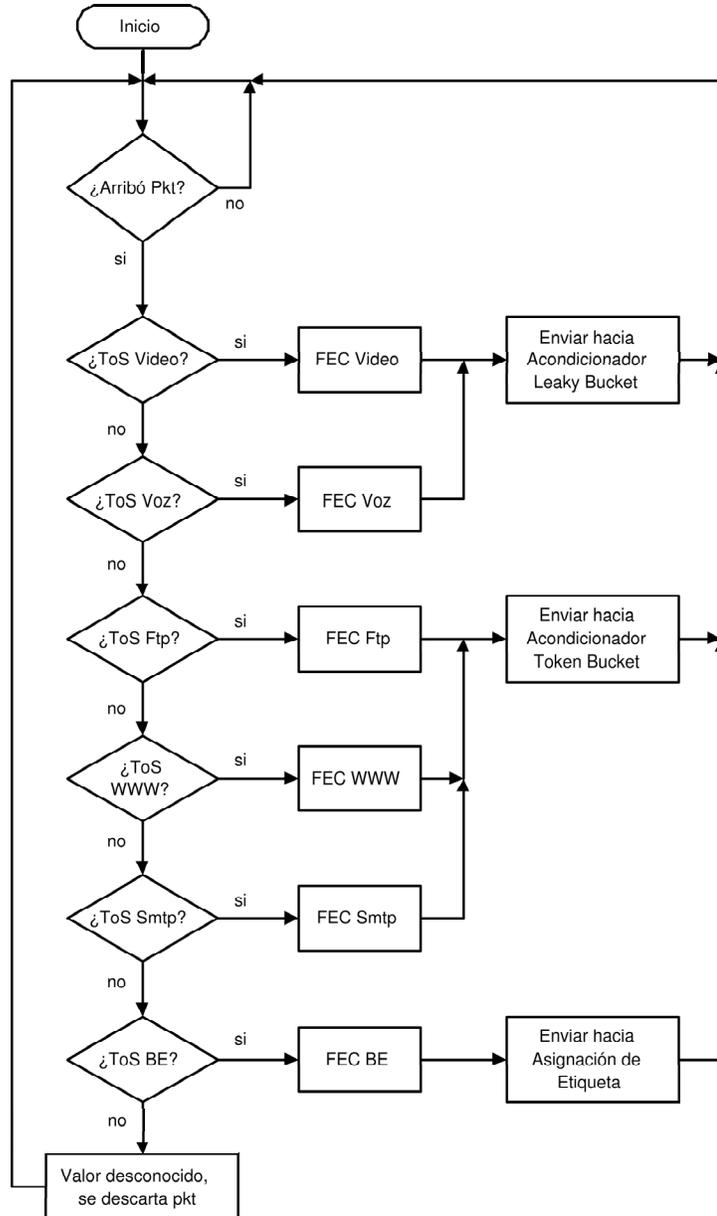


Figura 22. Diagrama de flujo para el Clasificador Multicampo

Como primer paso se verifica el arribo de un paquete, si es así, se obtienen los valores del campo ToS para identificar la clase de tráfico a la que pertenecen los paquetes, para

asignarles una FEC. Si el paquete es asignado a la FEC Video o Voz, éste será enviado al proceso de leaky bucket del acondicionador de tráfico, o bien, si el paquete es asignado a la FEC Ftp, WWW o Smtip, el paquete será enviado al proceso de token bucket del acondicionador. Finalmente, si el paquete es asignado a la FEC BE, el paquete es enviado al proceso de asignación de etiqueta.

IV.3.3.2 Modelo de Procesos para el Acondicionador de Tráfico

En la figura 23 se presenta el modelo de procesos que se implementó para el acondicionador de tráfico. Está basado en el modelo FIFO que incluye OPNET.

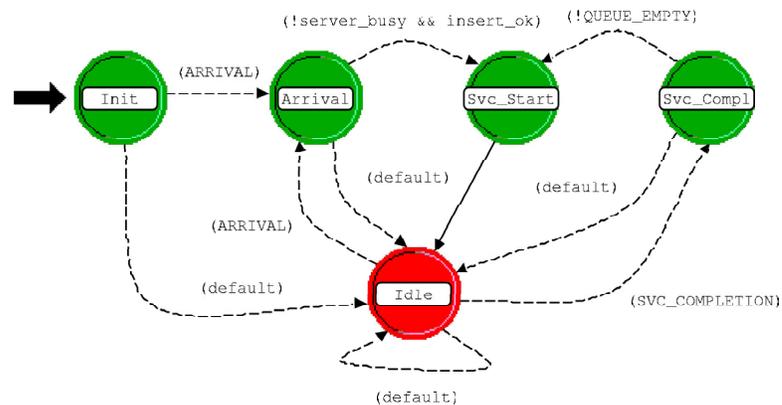


Figura 23. Modelo de procesos para el Acondicionador de Tráfico

El Estado “Init” indica el inicio del proceso, solo que ahora la ejecución del proceso puede pasar al estado “Arrival” si arriba un paquete inmediatamente, de no ser así, se pasa al estado “Idle”. Una vez en el estado “Idle”, la ejecución del proceso puede pasar al estado “Svc_Compl” si ha terminado el tiempo de servicio de un paquete ó pasar al estado “Arrival” si arriba un paquete. En el estado “Arrival” se obtiene el

tamaño en bits del paquete y se identifica la FEC a la que pertenece. Las FEC de Video y Voz tienen asociadas el mecanismo Leaky Bucket, por lo que los paquetes que arriban con una tasa mayor a la permitida son descartados. Las FEC de FTP, WWW y SMTP tienen asociadas el mecanismo Token Bucket, para estos paquetes se comparan su tamaño (en bits) y su tasa de llegada (en bits por segundo) con los parámetros de configuración PBS (Peak Burst Size) y PIR (Peak Information Rate) del token bucket. Los paquetes que no cumplen con estos parámetros son marcados con una prioridad de descarte alta. Una vez colocado en la cola el paquete se revisa el estado del servidor, si está ocupado se pasa la ejecución del proceso al estado “Idle”, si está libre se pasa al estado “Svc_Start”, en el cual se calendariza el tiempo de servicio de los paquetes de acuerdo a su tiempo de llegada al proceso de acondicionamiento. En el estado “Svc_Compl” los paquetes son removidos de la cola y enviados hacia el siguiente proceso.

El diagrama de flujo empleado en la programación del acondicionador se presenta en la figura 24. Como primer paso se obtienen la tasa de servicio del enlace y los parámetros PBS y PIR del token bucket para las FEC FTP, WWW y SMTP. Enseguida se verifica el arribo de un paquete, si es así, se marca el paquete con su tiempo de llegada al proceso y se obtiene su tamaño en bits. Después se identifica la FEC del paquete, si pertenece a las FEC Video o Voz se verifica el estado de la cola, si está llena se descarta el paquete, de lo contrario es encolado; si el paquete pertenece a las FEC FTP, WWW o SMTP se obtiene su tasa de llegada y el tamaño del paquete se compara con el PBS,

si es menor o igual, se compara su tasa de llegada con el PIR, si es menor o igual, el paquete es marcado con una prioridad de descarte baja y es colocado en la cola. Si el tamaño del paquete excede el PBS o su tasa excede el PIR, el paquete es marcado con una prioridad de descarte alta y es colocado en la cola.

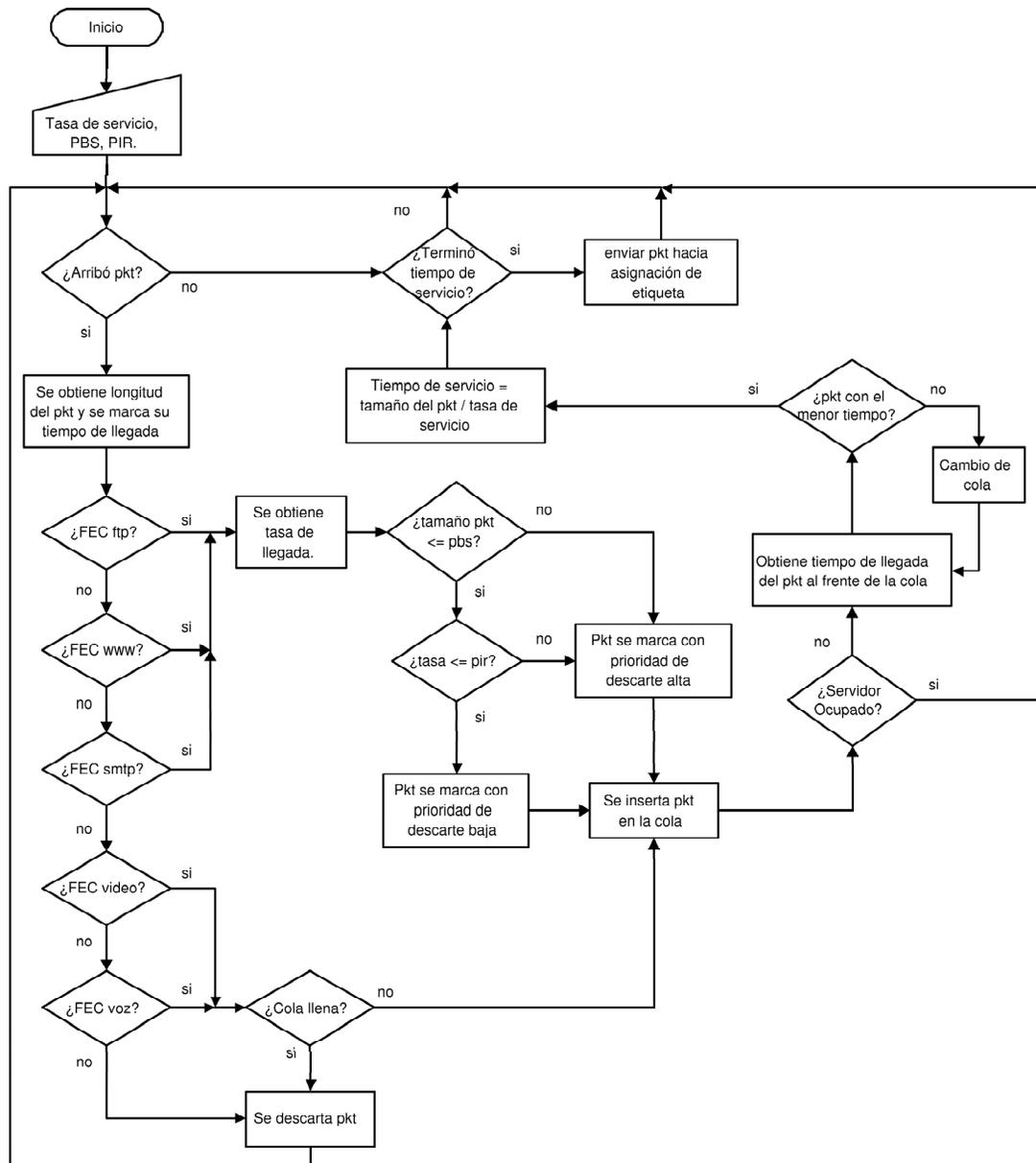


Figura 24. Diagrama de flujo para el Acondicionador

Una vez que los paquetes son colocados en su cola se verifica el estado del servidor, si está disponible se obtiene el tiempo de llegada de los paquetes al frente de cada cola y se comparan para encontrar el que cuente con el menor tiempo de llegada, al cual se calendariza su tiempo de servicio. Finalmente, cuando termina el tiempo de servicio de un paquete, éste es enviado hacia el proceso de asignación de etiqueta.

IV.3.3.3 Modelo de Procesos para Asignación de Etiqueta

En la figura 25 se presenta el modelo de procesos que se implementó para Asignación de Etiqueta. El Estado “Init” indica el inicio del proceso, el estado “Idle” mantiene la ejecución del proceso en espera del arribo de un paquete. Una vez que arriba un paquete la ejecución del proceso pasa al estado “Arrival”, el cual lleva a cabo la asignación de la etiqueta y el campo EXP a los paquetes de acuerdo a su FEC.

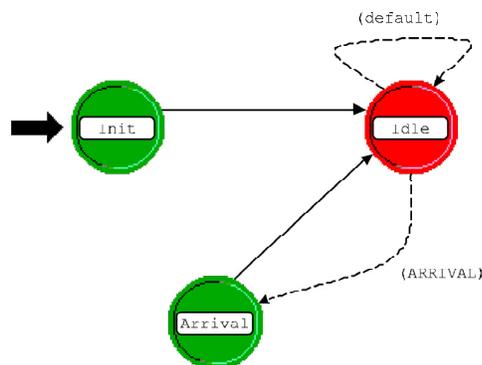


Figura 25. Modelo de procesos para Asignación de Etiqueta

El diagrama de flujo empleado en la programación del proceso de Asignación de Etiqueta se presenta en la figura 26.

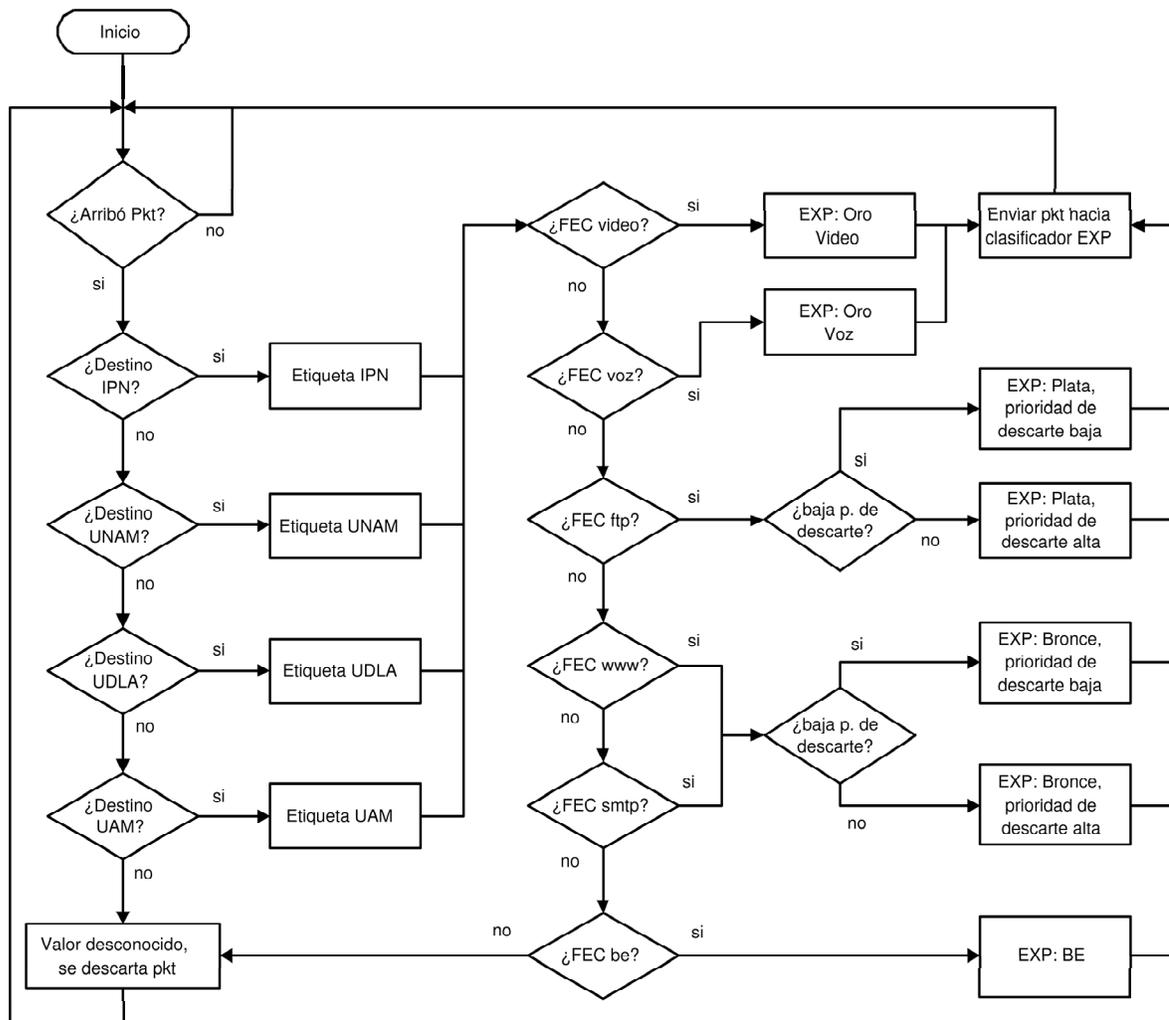


Figura 26. Diagrama de flujo para Asignación de Etiqueta

Como primer paso se verifica el arribo de un paquete, si es así, se identifica la dirección IP destino del paquete, y se le asigna la etiqueta correspondiente. Enseguida se identifica la FEC del paquete, si es Video o Voz, se asigna el valor del campo EXP de la clase Oro video y voz respectivamente. Si es una FEC Ftp, se obtiene su prioridad de descarte y de acuerdo a ésta se asigna el valor del campo EXP de la clase Plata con baja o alta prioridad de descarte respectivamente. Si es una FEC WWW o Smtip, se

obtiene su prioridad de descarte y de acuerdo a ésta se asigna el valor del campo EXP de la clase Bronce con baja o alta prioridad de descarte respectivamente. Si es una FEC BE se le asigna el campo EXP de la clase BE. Finalmente, el paquete es enviado al proceso de clasificación del campo EXP.

IV.3.3.4 Modelo de Procesos para el Clasificador EXP

En la figura 27 se presenta el modelo de procesos que se implementó para el clasificador EXP. El Estado “Init” indica el inicio del proceso, el estado “Idle” mantiene la ejecución del proceso en espera del arribo de un paquete. Una vez que arriba un paquete la ejecución del proceso pasa al estado “Arrival”, el cual lleva a cabo la clasificación de los paquetes de acuerdo al contenido del campo EXP del encabezado MPLS del paquete.

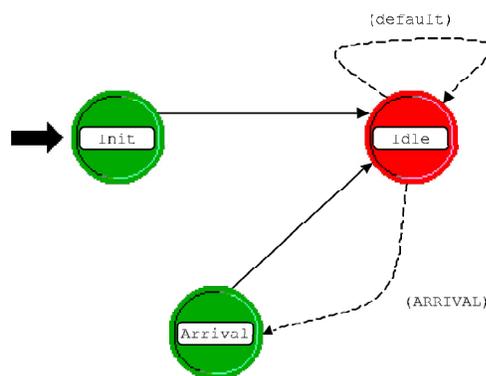


Figura 27. Modelo de procesos para el Clasificador EXP

El diagrama de flujo empleado en la programación del clasificador EXP se presenta en la figura 28. Como primer paso se verifica el arribo de un paquete, si es así, se identifica el valor del campo EXP del paquete. Si el paquete pertenece a las clases Oro

ó BE, es enviado al mecanismo de control de admisión Drop-Tail, pero si pertenece a las clases Plata o Bronce, el paquete es enviado al mecanismo de control de admisión WRED.

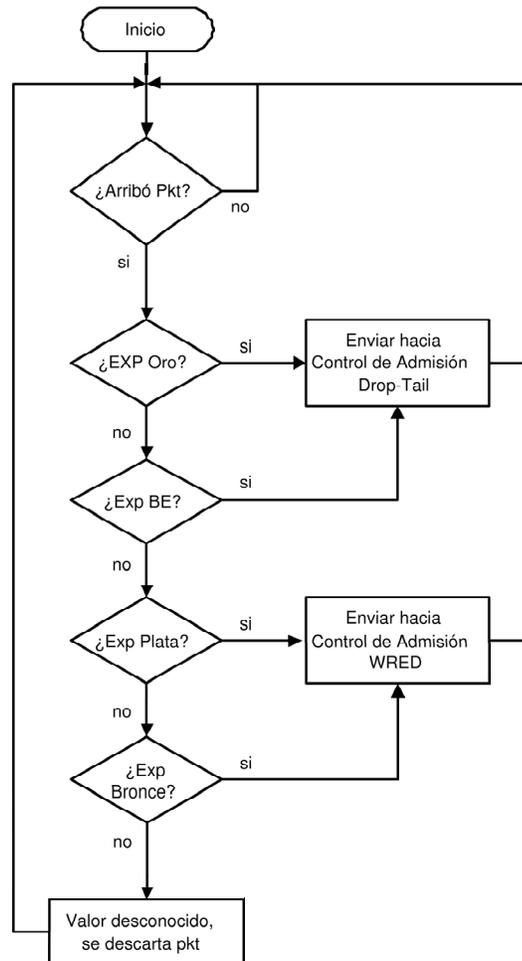


Figura 28. Diagrama de flujo para el Clasificador EXP

IV.3.3.5 Modelo de Procesos para el Calendarizador

En la figura 29 se presenta el modelo de procesos que se implementó para el calendarizador. El Estado “Init” indica el inicio del proceso. En el estado “Idle”, la ejecución

del proceso puede pasar al estado “Svc_Cmpl” si ha terminado el tiempo de servicio de un paquete ó pasar al estado “Arrival” si arriba un paquete. En el estado “Arrival” se calcula el tiempo virtual de arribo de los paquetes y son colocados en la cola de acuerdo a su clase; los paquetes que pertenecen a las clases Oro y BE son colocados en su cola por el mecanismo Drop-Tail, en tanto que los paquetes de las clases Plata y Bronce son colocados en su cola por el mecanismo WRED. Una vez que los paquetes son colocados en su cola correspondiente se revisa el estado del servidor, si está ocupado se pasa la ejecución del proceso al estado “Idle”, si está libre se pasa al estado “Svc_Start”, en el cual se calendariza el tiempo de servicio de los paquetes de acuerdo a su tiempo virtual de salida. En el estado “Svc_Cmpl” los paquetes son removidos de la cola y enviados hacia el transmisor.

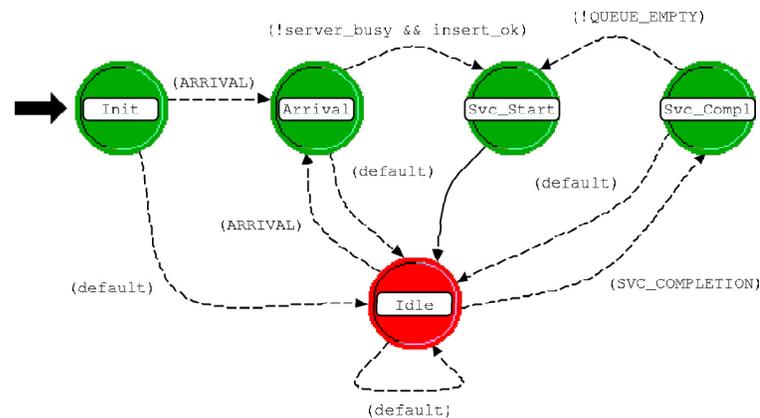


Figura 29. Modelo de procesos para el Calendarizador

El diagrama de flujo empleado en la programación del calendarizador se presenta en la figura 30. Como primer paso se obtienen la tasa de servicio del enlace, la tasa de

servicio asignada a cada clase y los parámetros mínimo y máximo valor de umbral del mecanismo WRED.

El siguiente paso es normalizar las tasas de servicio y verificar la llegada de algún paquete, si es así, se calcula el tiempo virtual actual de arribo de los paquetes $V(t_2)$, si no hay ninguna clase activa la suma de sus fracciones de ancho de banda $\Sigma\Phi_i$ es igual a 0, es decir, todas las colas están vacías, entonces $V(t_2) = 0$, en cambio si hay alguna clase activa, $V(t_2)$ es igual a la suma del tiempo virtual anterior de arribo $V(t_1)$ y la relación de la diferencia de tiempos reales $t_2 - t_1$ y $\Sigma\Phi_i$. Enseguida se identifica la clase de tráfico, si el paquete pertenece a las clases Oro Video, Oro Voz o BE se revisa el estado de su cola, si está llena se descarta el paquete, si no es así, se coloca en la cola el paquete. Para las clases Plata y Bronce, primero se obtiene la prioridad de descarte del paquete, si es baja, se le asigna una $Pmax = 0.1$, si es alta, se le asigna una $Pmax = 0.5$. Después se obtiene el tamaño del paquete y se calcula el tamaño promedio de la cola AQS , si este valor es menor o igual al mínimo valor de umbral Min_Thr , el paquete es colocado en su cola, por el contrario, si AQS excede Min_Thr , pero es menor o igual al máximo valor de umbral Max_Thr , se calcula una probabilidad de descarte Pd , la cual está dada por la probabilidad máxima de descarte y la diferencia entre AQS y Min_Thr dividida por la diferencia de umbrales, si Pd es menor a un número aleatorio el paquete es descartado, de lo contrario el paquete es colocado en la cola. Si AQS excede Max_Thr el paquete es descartado. Una vez colocado en su cola el paquete se actualiza $\Sigma\Phi_i$ y se revisa el estado del servidor, si está disponible se calcula

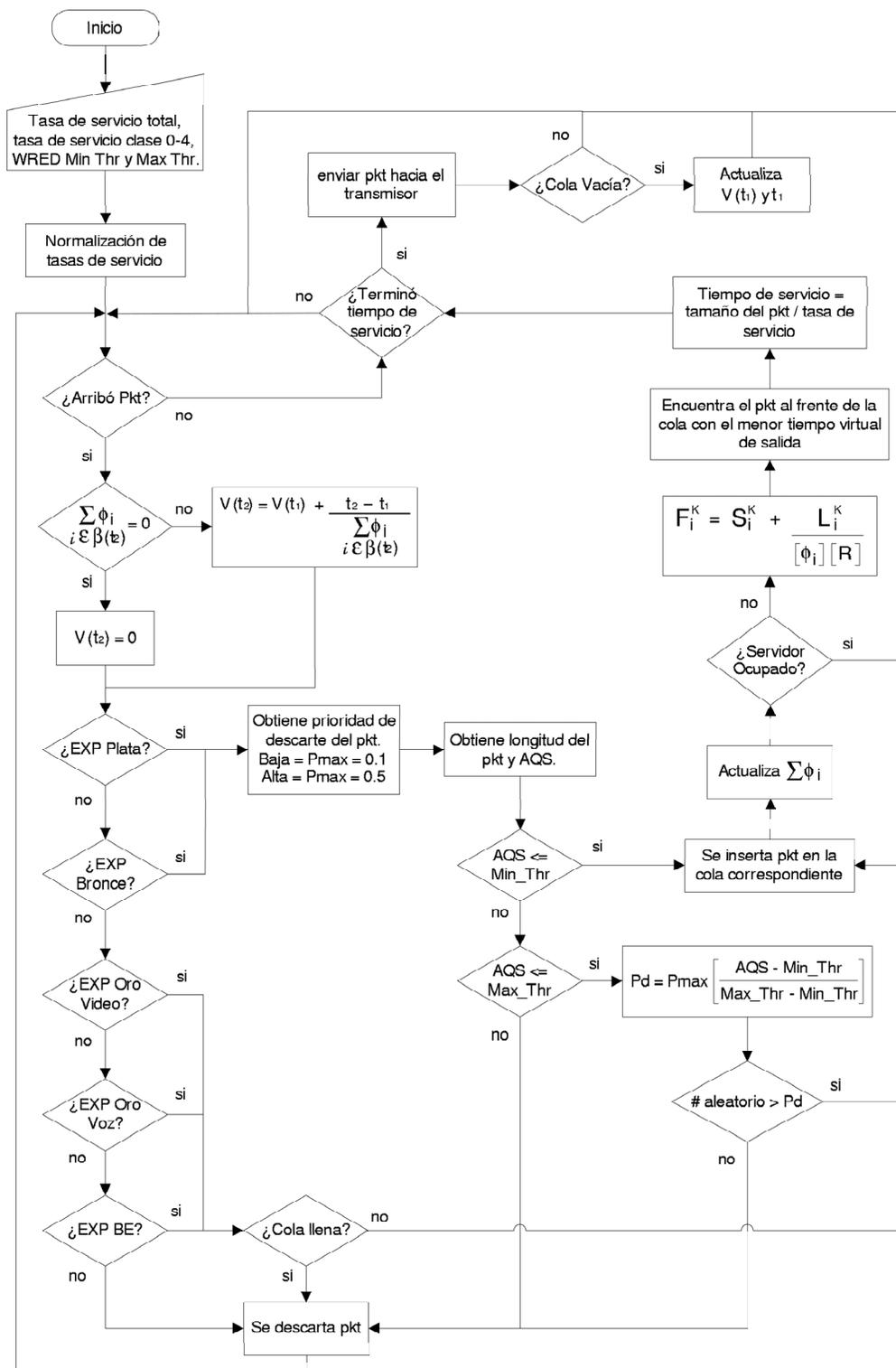


Figura 30. Diagrama de flujo para el Calendarizador

el tiempo virtual de salida F_i^k de los paquetes al frente de cada cola. F_i^k está dado por la suma del tiempo real en el que debía iniciarse la transmisión del paquete S_i^k y la relación del tamaño del paquete L_i^k y su tasa efectiva de servicio $[\Phi_i][R]$. Enseguida se encuentra el paquete con el menor tiempo virtual de salida y se calendariza su tiempo de servicio. Cuando termina el tiempo de servicio de un paquete se remueve de la cola y es enviado al transmisor. Si al remover el paquete la cola queda vacía, se actualizan los valores de $V(t_1)$ y t_1 .

IV.3.3.6 Modelo de Procesos para el Clasificador de Etiquetas

En la figura 31 se presenta el modelo de procesos que se implementó para el clasificador de Etiquetas. El Estado “Init” indica el inicio del proceso, el estado “Idle” mantiene la ejecución del proceso en espera del arribo de un paquete. Una vez que arriba un paquete la ejecución del proceso pasa al estado “Arrival”, el cual lleva a cabo la clasificación de los paquetes de acuerdo al valor de la etiqueta del encabezado MPLS del paquete.

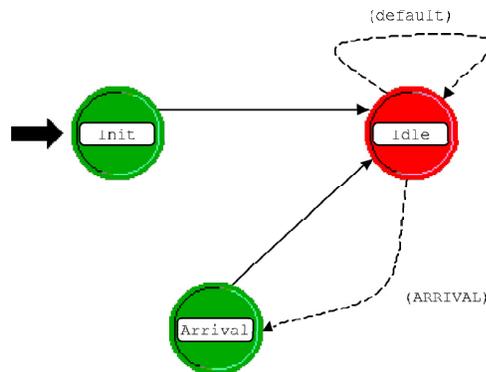


Figura 31. Modelo de procesos para el Clasificador de Etiquetas

El diagrama de flujo empleado en la programación del clasificador de Etiquetas se presenta en la figura 32.

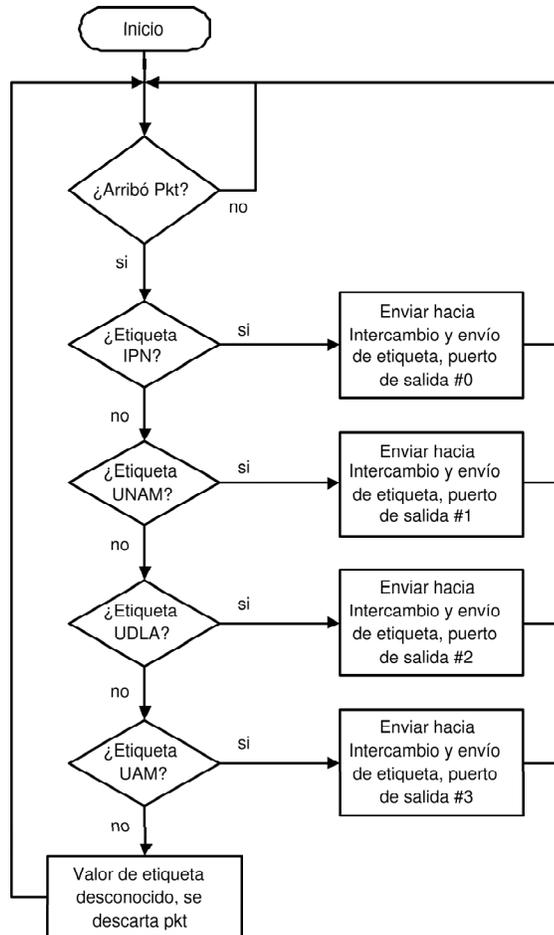


Figura 32. Diagrama de flujo para el Clasificador de Etiquetas

Como primer paso se verifica el arribo de un paquete, si es así, se obtiene el valor de la etiqueta del paquete, si la etiqueta corresponde al destino IPN, el paquete es enviado hacia el proceso de intercambio y envío de etiqueta por el puerto de salida #0, si corresponde al destino UNAM el paquete es enviado por el puerto #1, si corresponde al destino UDLA el paquete es enviado por el puerto #2 ó si la etiqueta corresponde

al destino UAM el paquete es enviado por el puerto #3. Finalmente, los paquetes que arriben con un valor de etiqueta no establecido entre los LSRs, son descartados.

IV.3.3.7 Modelo de Procesos para Intercambio y Envío de Etiqueta

En la figura 33 se presenta el modelo de procesos que se implementó para la etapa de Intercambio y Envío de Etiqueta. El Estado “Init” indica el inicio del proceso, el estado “Idle” mantiene la ejecución del proceso en espera del arribo de un paquete. Una vez que arriba un paquete la ejecución del proceso pasa al estado “Arrival”, dentro del cual se remueve la etiqueta de entrada del paquete y se le asigna una etiqueta de salida de acuerdo a la clasificación hecha por el proceso anterior.

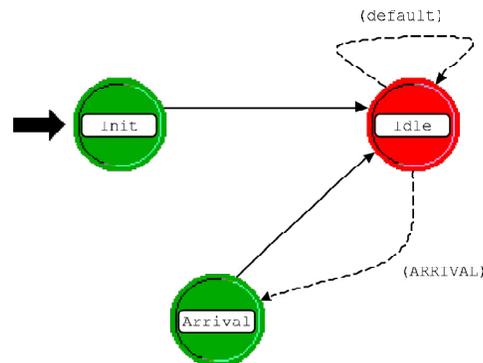


Figura 33. Modelo de procesos para Intercambio y Envío de Etiqueta

El diagrama de flujo empleado en la programación del proceso de Intercambio y Envío de Etiqueta se presenta en la figura 34. Como primer paso se verifica el arribo de un paquete, si es así, se identifica el puerto de entrada del paquete. Si el paquete arribó por el puerto de entrada #0 se remueve su etiqueta IPN de entrada y se le asigna una etiqueta IPN de salida, si el paquete arribó por el puerto #1, #2 ó #3 se remueve su

etiqueta UNAM, UDLA o UAM de entrada y se le asigna una etiqueta UNAM, UDLA o UAM de salida respectivamente. Una vez que se asigna la etiqueta de salida al paquete, éste es enviado hacia el clasificador EXP.

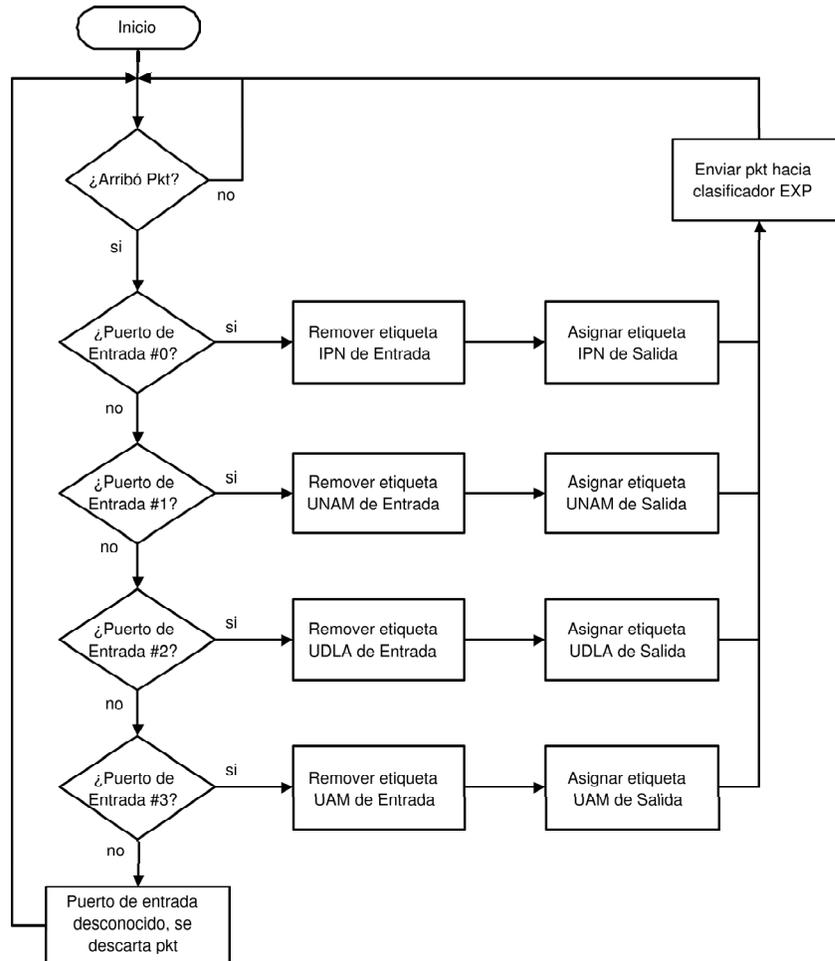


Figura 34. Diagrama de flujo para Intercambio y Envío de Etiqueta

En el siguiente capítulo se presentan los resultados obtenidos en cuanto a retardo, variación del retardo y pérdida de paquetes para el modelo DiffServ sobre ATM utilizando 6 PVCs y para el modelo MPLS sobre SONET, así como una comparación de los resultados obtenidos en ambos modelos.

Capítulo V

Resultados y Análisis Numérico

V.1 Introducción

En este capítulo se presentan los resultados obtenidos durante la simulación de los modelos DiffServ sobre ATM utilizando 6 PVCs y MPLS sobre SONET, implementados en la dorsal de la red Internet2-México. Los parámetros de calidad de servicio que se midieron en cada escenario de simulación fueron: retardo extremo a extremo, la variación del retardo y la probabilidad de pérdida de paquetes.

Además se presenta un análisis comparativo entre los resultados obtenidos para los modelos DiffServ sobre ATM - 6 PVCs y MPLS sobre SONET Dorsal Tij-Gdl-DF. Esta comparación se llevó al cabo de acuerdo a los parámetros de Calidad de Servicio mencionados anteriormente.

V.2 Parámetros de Simulación

Los resultados presentados mediante los distintos gráficos que se encuentran en las secciones posteriores, son el resultado del cálculo de un promedio de los datos obtenidos de tres secuencias de simulación, cada una de ellas hecha con una semilla distinta. Estas

secuencias de simulación constaban de diez escenarios, cada uno con una variación en el tráfico inyectado a la red. Cada escenario contaba con una duración de 50 segundos, durante los primeros 5 segundos el tráfico generado por las fuentes no era inyectado a la red, para dar tiempo a que éstas estabilizaran su tasa de generación. De esta misma manera, a los 45 segundos se detenía la generación de tráfico para permitir que todos los paquetes terminaran su procesamiento. Cabe mencionar que las variaciones de tráfico para cada escenario se basaron en la tasa de generación de tráfico de una fuente individual para cada servicio, las cuales se presentan en la tabla II.

Tabla II. Tasa de generación de tráfico para cada servicio

| Servicio | Tasa de generación de tráfico de una fuente |
|-----------------|--|
| Video | 1.5 Mbps |
| Voz | 60 Kbps |
| FTP | 75 Kbps |
| WWW | 22 Kbps |
| SMTP | 55 Kbps |
| BE | 2 Mbps |

En la tabla III se presenta el tráfico inyectado a la red por cada nodo generador de tráfico en cada escenario de simulación. Estas cantidades de tráfico corresponden a un solo nodo Asociado Académico, por lo que el tráfico total inyectado a la dorsal, depende del número de Asociados Académicos con los que cuente el modelo de red, por ejemplo, el modelo de red MPLS Dorsal Tij-Gdl-D.F. cuenta con dos nodos de Asociado Académico (CICESE y U de G) por lo tanto, el tráfico total inyectado a la red es el doble del que se presenta en la tabla III.

Para generar el tráfico de cada nodo presentado en la tabla III se agregan fuentes de

Tabla III. Condiciones de tráfico para cada escenario de simulación

| Escenario | Video (Mbps) | Voz (Mbps) | FTP (Mbps) | WWW (Mbps) | SMTP (Mbps) | Tráfico Total (Mbps) |
|-----------|--------------|------------|------------|------------|-------------|----------------------|
| 1 | 1.5 | 1.5 | 0.5 | 0.5 | 0.5 | 4.5 |
| 2 | 3 | 3 | 1 | 1 | 1 | 9 |
| 3 | 4.5 | 4.5 | 1.5 | 1.5 | 1.5 | 13.5 |
| 4 | 6 | 6 | 2 | 2 | 2 | 18 |
| 5 | 7.5 | 7.5 | 2.5 | 2.5 | 2.5 | 22.5 |
| 6 | 9 | 9 | 3 | 3 | 3 | 27 |
| 7 | 10.5 | 10.5 | 3.5 | 3.5 | 3.5 | 31.5 |
| 8 | 10 | 12 | 4 | 4 | 4 | 34 |
| 9 | 10 | 12 | 4.3 | 4.3 | 4.3 | 35 |
| 10 | 10 | 12 | 4.6 | 4.6 | 4.6 | 36 |

tráfico, donde el número de fuentes a agregar depende de la tasa de generación de una fuente para cada tipo de servicio. De esta manera, para generar un tráfico de 1 Mbps se necesita una mayor cantidad de fuentes de tipo WWW (45 fuentes) que de tipo FTP (13 fuentes), ya que como puede observarse en la tabla II, la tasa de generación de una fuente WWW (22 Kbps) es menor que la de una fuente FTP (75 Kbps).

Para realizar el análisis del desempeño de los modelos DiffServ sobre ATM y MPLS sobre SONET para proveer Calidad de Servicio, se tomaron en cuenta los valores de los parámetros de calidad de servicio que se presentan en la tabla IV.

Tabla IV. Valores límites para los parámetros de QoS

| Servicio | Probabilidad de Pérdida de Paquetes (PLR) | Retardo | Variación del Retardo |
|----------|---|-----------|-----------------------|
| Video | 10^{-6} | 400 mseg | 30 mseg |
| Voz | 10^{-3} | 400 mseg | 20 mseg |
| Datos | 10^{-6} | 1400 mseg | — |

Los valores anteriores nos indican los límites donde se garantiza un desempeño

aceptable de cada servicio. Los valores de los parámetros para los servicios de voz y datos se tomaron de [RACE D-732, 1994] y [RACE D-511, 1994], en tanto que para el servicio de video se encuentran en [Bong, 1998].

V.3 Obtención de Parámetros Adecuados de Operación de los Mecanismos de QoS

Previo a la ejecución de las secuencias de simulación de los modelos DiffServ sobre ATM y MPLS sobre SONET fue necesario llevar al cabo algunas pruebas para obtener los parámetros de configuración óptimos de los mecanismos de Calidad de Servicio involucrados en la arquitectura de los enrutadores de ambos modelos. Dichas pruebas se realizaron sobre la red que se presenta en la figura 35, la cual incluye a los nodos generadores de tráfico, un nodo de frontera y un nodo de captura de estadísticas.

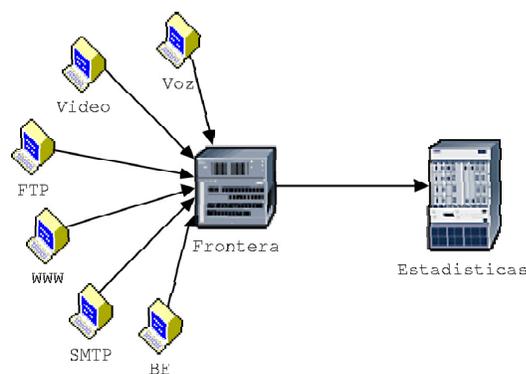


Figura 35. Modelo de red para validación de mecanismos de QoS

Los enlaces de las fuentes hacia el nodo de frontera son de 100 Mbps y el enlace

entre el nodo de frontera y el nodo de captura de estadísticas es de 34 Mbps, las cuales son las velocidades de los modelos completos.

V.3.1 DiffServ sobre ATM utilizando 6 PVCs

Como se mencionó en el capítulo IV, los mecanismos de QoS, con excepción de los mecanismos de segmentación y reensamble de celdas, utilizados en los enrutadores de Asociado Académico y Gigapop se encuentran basados en los modelos utilizados en [Caballero Cárdenas, 2002], por lo que los valores para los parámetros de configuración de estos mecanismos son los mismos que los utilizados en el trabajo de investigación citado.

Para el caso de los mecanismos de segmentación y reensamble fue necesario definir el ancho de banda para cada PVC que cumpliera con los requerimientos de cada clase de servicio, por lo que después de varias pruebas y de definir el tráfico a inyectar a la red por cada servicio durante los distintos escenarios de simulación, el ancho de banda asignado a cada PVC se estableció como se muestra en la tabla V.

Tabla V. Ancho de Banda asignado a cada PVC

| Servicio | Ancho de Banda del PVC (Mbps) |
|-----------------|--------------------------------------|
| Video | 12 Mbps |
| Voz | 9 Mbps |
| FTP | 4 Mbps |
| WWW | 4 Mbps |
| SMTTP | 4 Mbps |
| BE | 1 Mbps |

Cabe recordar que cada PVC es del tipo UBR, por lo que fue necesario configurar a cada uno su tasa pico de celda, la cual se estableció igual al ancho de banda del PVC de cada tipo de servicio.

Para los enlaces STM-1 (155 Mbps) entre los Gigapops el ancho de banda del PVC se asignó proporcionalmente a la distribución de ancho de banda que se presenta en la tabla V, es decir, si al PVC de video le corresponde un ancho de banda de 12 Mbps del total de 34 Mbps del enlace E3, para el enlace STM-1 le corresponde un ancho de banda de 54 Mbps; lo mismo sucede para los otros PVCs.

V.3.2 MPLS sobre SONET

En el capítulo III se mencionan los mecanismos de QoS que utilizan los enrutadores de conmutación de etiquetas, entre estos se tienen el Token Bucket como mecanismo de acondicionamiento de tráfico, WRED para control de admisión a las colas y WFQ como mecanismo de calendarización de tráfico, los cuales requieren de la configuración de ciertos parámetros de acuerdo a las características del tráfico que circula a través de ellos.

El mecanismo Token Bucket requiere la configuración de los parámetros de tamaño pico de la ráfaga (PBS) y tasa pico de información (PIR), cuyos valores toman en cuenta las características del tráfico FTP, WWW y SMTP. Debido a que estas fuentes manejan un tamaño de paquete variable, fue necesario hacer varias pruebas para obtener el tamaño máximo de paquete para cada fuente, obteniendo que el tamaño máximo en bits

para paquetes FTP es de 500 Kb, para paquetes WWW es de 200 Kb y para paquetes SMTP es de 5 Kb. Además, tomando en cuenta que la máxima tasa de transmisión en un escenario de simulación de estas fuentes es de 4.3 Mbps, los valores para los parámetros PBS y PIR quedaron como se muestra en la tabla VI.

Tabla VI. Parámetros de configuración para el Token Bucket

| FEC | PBS (Kb) | PIR (Kbps) |
|------------|---------------------|-----------------------|
| FTP | 500 | 6000 |
| WWW | 200 | 6000 |
| SMTP | 5 | 6000 |

El mecanismo WRED requiere la configuración de los parámetros de mínimo y máximo valor de umbral de la cola y probabilidad máxima de descarte. El valor de umbral mínimo debe ser lo suficientemente grande de tal manera que la utilidad del enlace sea máxima. Para el mecanismo Token Bucket se consideró que los paquetes que arriban con una tasa menor a un PIR de 6 Mbps eran atendidos, por lo que se decidió utilizar un mínimo valor de umbral de 6 Mbps, en base a esto se consideró un máximo valor de umbral de 12 Mbps. La probabilidad máxima de descarte depende de la prioridad de descarte del paquete, donde a los paquetes con una baja prioridad de descarte les corresponde una $P_{max} = 0.1$ y a los paquetes con alta prioridad de descarte les corresponde una $P_{max} = 0.5$.

Por último, el mecanismo WFQ requiere la configuración de la tasa de servicio del enlace y la tasa de servicio que corresponde a cada clase de tráfico MPLS. Después de varias pruebas donde se variaba la tasa de servicio asignada a cada clase de tráfico de

acuerdo a las condiciones de tráfico máximas en los escenarios de simulación, las tasas de servicio para cada clase de tráfico quedaron como se muestra en la tabla VII.

Tabla VII. Tasa de servicio asignada a cada clase de tráfico MPLS

| | <i>Enlace E3</i> | <i>Enlace STM-1</i> |
|-------------------------|--------------------------------|--------------------------------|
| Clase de Tráfico | Tasa de Servicio (Mbps) | Tasa de Servicio (Mbps) |
| Oro Video | 11 Mbps | 50 Mbps |
| Oro Voz | 10 Mbps | 45 Mbps |
| Plata | 5 Mbps | 23 Mbps |
| Bronce | 7 Mbps | 32 Mbps |
| BE | 1 Mbps | 5 Mbps |

V.4 Análisis de Resultados

En esta sección se presenta el análisis de resultados en cuanto a retardo extremo a extremo, variación del retardo, probabilidad de pérdida de paquetes y caudal eficaz, para los modelos DiffServ sobre ATM y MPLS sobre SONET.

V.4.1 DiffServ sobre ATM utilizando 6 PVCs

V.4.1.1 Retardo Extremo a Extremo

En la figura 36 se presenta la gráfica obtenida para el retardo extremo a extremo de los servicios de video, voz, FTP, WWW, SMTP y BE. En la gráfica se observa que para las primeras simulaciones donde el tráfico generado es poco, el tráfico de Voz y Best Effort experimentan el menor retardo de todos los tipos de tráfico, ya que el tamaño

de sus paquetes es pequeño pero conforme se va incrementando el tráfico de los otros nodos, el retardo del tráfico Best Effort se va incrementando hasta llegar a tener el mayor retardo de todos.

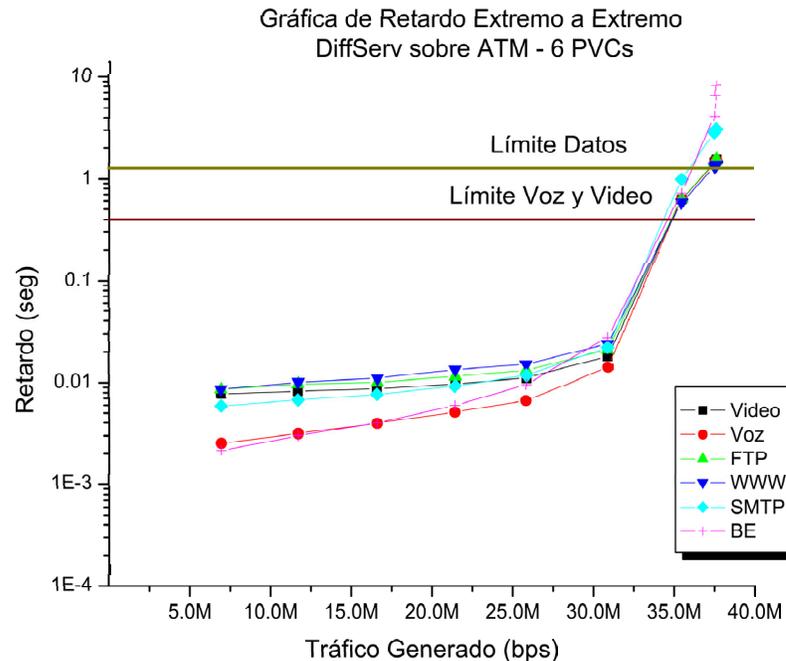


Figura 36. Retardo extremo a extremo para el modelo DiffServ sobre ATM - 6 PVCs

Los valores de retardo para el tráfico de video, voz, FTP, WWW y SMTP se mantienen por debajo de los límites establecidos para su buen desempeño, con un tráfico total generado de hasta 33 Mbps. Esto se debe a que al segmentar el paquete en varias celdas ATM, cada una con su correspondiente encabezado, provoca que aumente el caudal de tráfico generado, reduciendo el porcentaje de utilización del enlace. Para un tráfico total mayor a 33 Mbps el tráfico de video, voz y datos exceden sus límites permitidos de retardo, lo que tiene como consecuencia el descarte de paquetes por los nodos de estadísticas.

V.4.1.2 Variación del Retardo

En la figura 37 se presenta la gráfica obtenida para la variación del retardo de los servicios de video, voz, FTP, WWW, SMTP y BE.

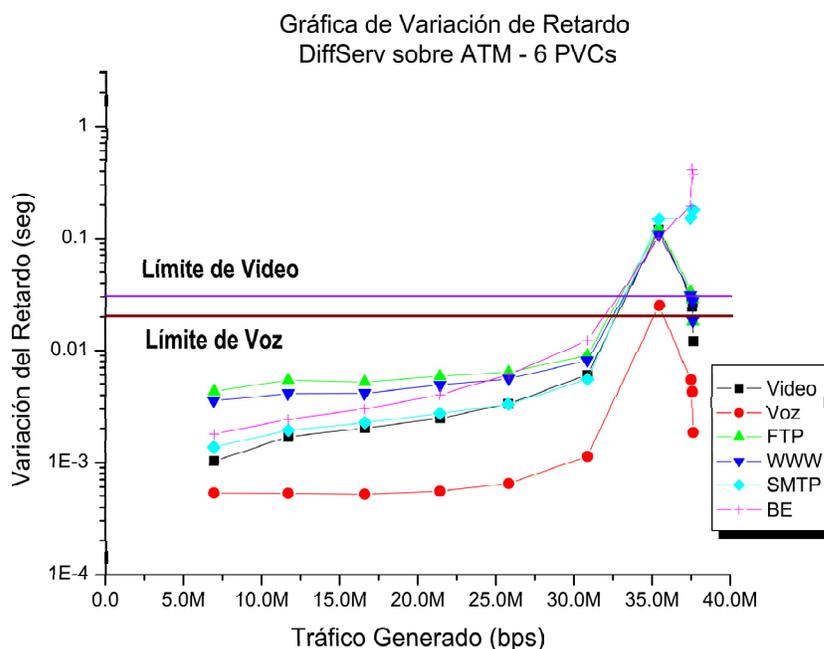


Figura 37. Variación del Retardo para el modelo DiffServ sobre ATM - 6 PVCs

En la gráfica se observa como los valores de variación del retardo para todos los tipos de servicios se mantienen estables para valores de tráfico generado de hasta 32 Mb/s. El tráfico de video es el primero en alcanzar su límite de variación de retardo, ocurriendo esto para un tráfico total de 33 Mb/s. En cuanto al tráfico de voz, a partir de los 35 Mb/s su variación de retardo alcanza su límite permitido.

Para un tráfico total de 35 Mb/s se presenta el valor máximo de variación de retardo para los flujos de tráfico de video, voz, FTP y WWW, pero para un tráfico mayor a

los 35 Mbps su variación de retardo disminuye, incluso debajo de los límites permitidos para el tráfico de video y voz, este comportamiento se presenta debido a que el enlace sigue transmitiendo a una tasa de 34 Mbps y las colas de estos flujos no presentan desbordamiento, lo que provoca que los paquetes experimenten retardos muy parecidos, teniendo como consecuencia la disminución de su variación del retardo. En cambio, para los flujos de tráfico SMTP y BE, sus valores de variación de retardo aumentan conforme se incrementa el tráfico total generado ya que estos flujos si presentan pérdida de paquetes debido al desbordamiento de sus colas, provocando que el retardo entre un paquete y otro cambie considerablemente aumentando su variación del retardo.

V.4.1.3 Probabilidad de Pérdida de Paquetes

En la figura 38 se presenta la gráfica obtenida para la probabilidad de pérdida de paquetes de los servicios de video, voz, FTP, WWW, SMTP y BE.

En la gráfica se observa que el tráfico de video y voz son los primeros en experimentar pérdida de paquetes, lo cual ocurre cuando se tiene un tráfico total de 32 Mbps aproximadamente, esto se debe a que para estos niveles de tráfico los límites en cuanto a retardo y variación del retardo para video y voz casi son alcanzados como puede observarse en las figuras 36 y 37 respectivamente.

En cuanto al tráfico SMTP, alcanza su límite de pérdida de paquetes para un tráfico de 32.5 Mbps, en cambio para tráfico FTP y WWW su límite es alcanzado hasta los 36 Mbps.

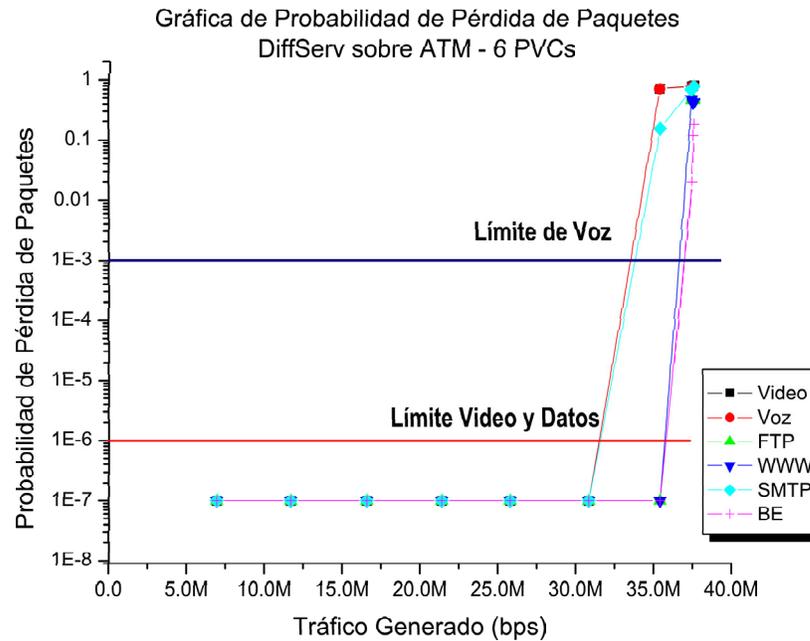


Figura 38. Probabilidad de Pérdida de Paquetes para el modelo DiffServ sobre ATM

V.4.1.4 Caudal Eficaz

La figura 39 presenta el comportamiento del caudal eficaz con respecto a la utilización del enlace (ρ), esta relación se deriva de la ecuación 2, la cual también involucra a la probabilidad de pérdida de paquetes para calcular el caudal eficaz, por lo que, en tanto no se presentan pérdidas de paquetes, el caudal eficaz tiene un comportamiento lineal como ocurre cuando la utilización del enlace es menor al 80% (27.2 Mbps), a partir de este punto los flujos de tráfico comienzan a sufrir pérdida de paquetes como se observa en la figura 38.

La reducción en el caudal eficaz de los distintos flujos de tráfico para un porcentaje de utilización del enlace menor al 100%, se debe principalmente a la segmentación de los paquetes en celdas ATM, agregando cada una su correspondiente encabezado de 5

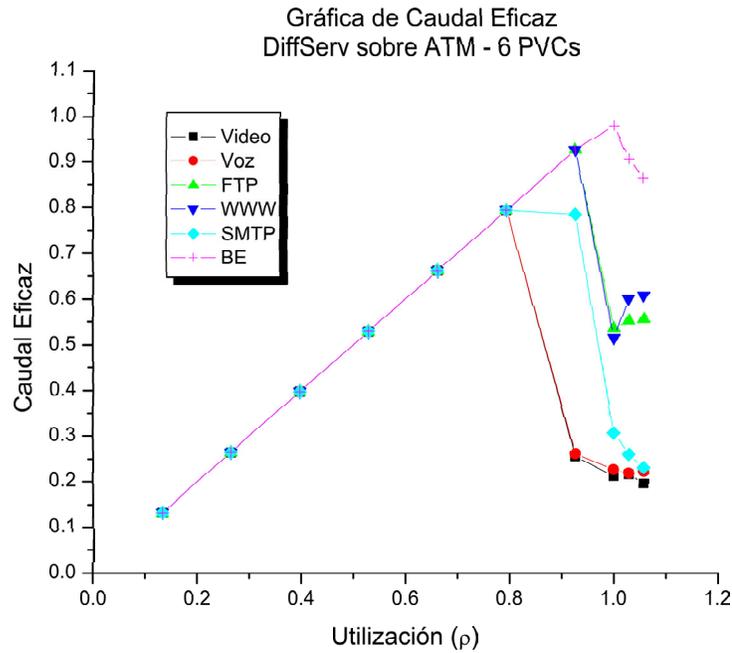


Figura 39. Caudal eficaz para el modelo DiffServ sobre ATM - 6 PVCs

bytes al tamaño del paquete, causando esto un incremento en el flujo de cada tipo de tráfico y disminuyendo su caudal eficaz.

V.4.2 MPLS sobre SONET Dorsal Tij - Gdl - D.F.

V.4.2.1 Retardo Extremo a Extremo

La figura 40 presenta los resultados obtenidos para el retardo extremo a extremo de los servicios de video, voz, FTP, WWW, SMTP y BE. Para escenarios con un tráfico generado entre los 6 Mbps y 18 Mbps se observa un contraste entre los valores de retardo para tráfico de video y voz, siendo el primero el mayor retardo y el segundo el menor,

ambos servicios pertenecen a la clase oro, la de mayor prioridad, lo que supone que sus retardos deben ser muy parecidos, ésta diferencia se debe al tamaño de sus paquetes, los paquetes de video son grandes por lo que tardan más tiempo en ser transmitidos por los LSR, a diferencia de los paquetes de voz cuyo tamaño es pequeño y su tiempo de transmisión es menor. De hecho, para este mismo intervalo de tráfico total, los valores de retardo para el tráfico FTP, WWW, SMTP y BE están determinados por su tamaño de paquete, ya que, ordenados de menor a mayor retardo se observan el tráfico SMTP, BE, WWW y FTP respectivamente, lo cual coincide con el tamaño de sus paquetes. Este comportamiento se presenta gracias a que al existir bastante ancho de banda disponible, el tráfico de menor prioridad puede tomar prestado ancho de banda del asignado al tráfico de mayor prioridad.

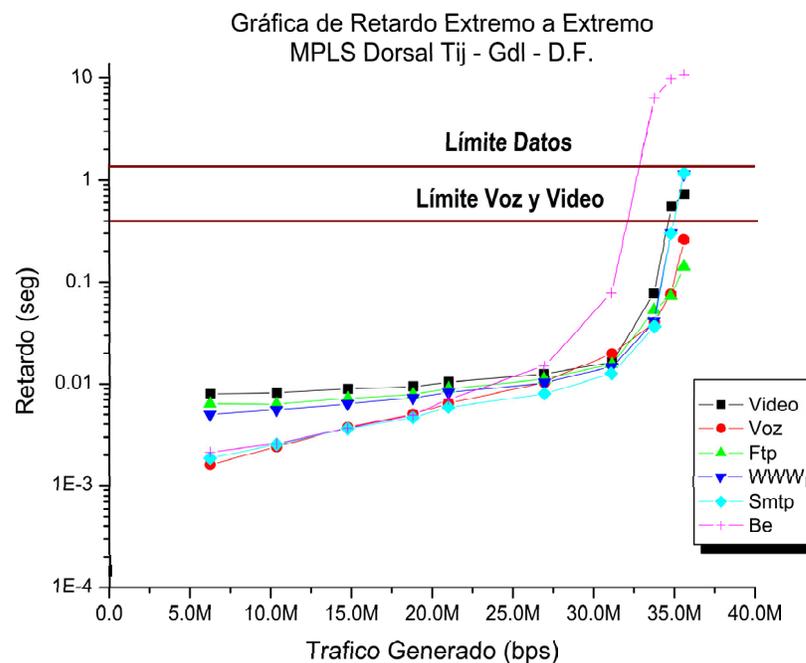


Figura 40. Retardo extremo a extremo para el modelo MPLS Dorsal Tij-Gdl-D.F.

Conforme aumenta el tráfico generado y las clases de tráfico utilizan un mayor ancho de banda, se observa como el retardo para el tráfico Best Effort, el de menor prioridad, aumenta considerablemente hasta alcanzar un máximo de 10.8 segundos para un tráfico total de 35.5 Mbps.

El retardo para el tráfico de video supera su límite permitido para un tráfico generado de 34.8 Mbps, en cambio, los valores de retardo para tráfico de voz, FTP, WWW y SMTP se mantiene debajo de sus límites de retardo para un tráfico generado de 35.6 Mbps aproximadamente. Por lo tanto, MPLS cumple con los requerimientos de retardo para estos servicios en tanto la capacidad del enlace no sea superada.

V.4.2.2 Variación del Retardo

En la figura 41 se presenta la gráfica obtenida para la variación del retardo de los servicios de video, voz, FTP, WWW, SMTP y BE. En la gráfica se observa como para escenarios de bajo tráfico generado, los valores de variación del retardo para el tráfico de video y voz es menor en comparación con los otros tipos de tráfico, este comportamiento era de esperarse ya éstos son los tipos de tráfico con mayor prioridad.

Al igual que en los resultados obtenidos de retardo extremo a extremo, conforme aumenta el tráfico generado los valores de variación del retardo para el tráfico Best Effort aumentan considerablemente, en cambio, la variación del retardo para los otros servicios se mantiene estable para valores de tráfico generado de hasta 32 Mbps, a partir del cual se incrementa su valor de variación del retardo.

Para un tráfico generado de 35 Mbps, los servicios de FTP y voz presentan su valor máximo de variación del retardo, superando el servicio de voz su límite permitido. En cuanto a los servicios de video, WWW, SMTP y BE, experimentan su mayor variación del retardo para un tráfico de 34 Mbps, disminuyendo su valor para un tráfico de 35 Mbps. Como ya se mencionó anteriormente, este comportamiento se debe a que el enlace se está utilizando a su máxima capacidad sin que se presente desbordamiento de las colas de estos servicios, lo cual tiende a disminuir la variación del retardo de los paquetes.

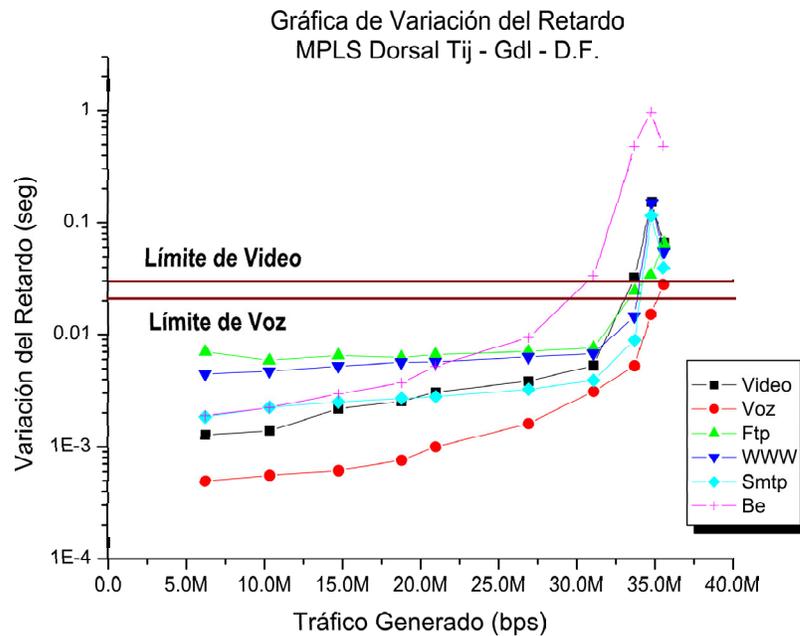


Figura 41. Variación del Retardo para el modelo MPLS Dorsal Tij-Gdl-D.F.

V.4.2.3 Probabilidad de Pérdida de Paquetes

En la figura 42 se presenta la gráfica obtenida para la probabilidad de pérdida de paquetes de los servicios de video, voz, FTP, WWW, SMTP y BE.

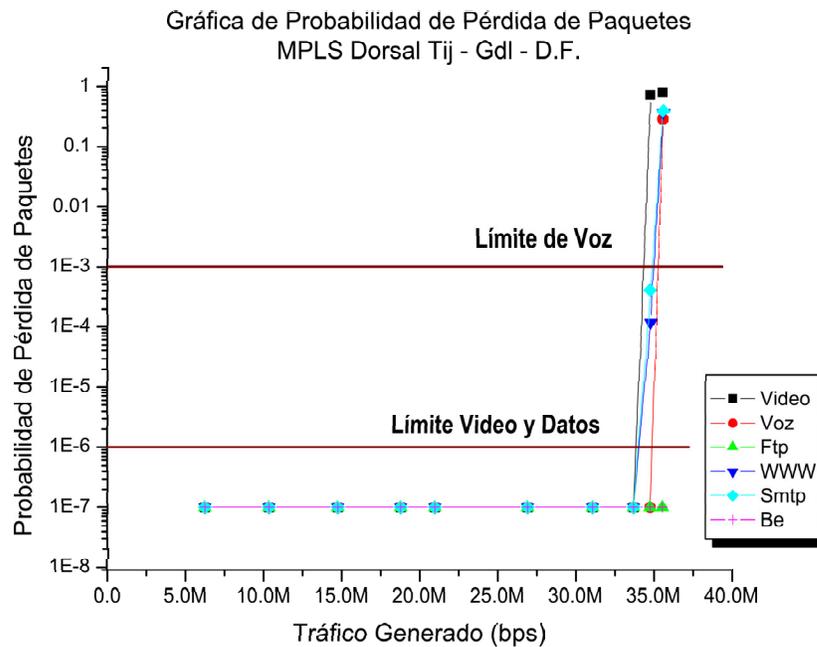


Figura 42. Probabilidad de Pérdida de Paquetes para el modelo MPLS Dorsal Tij-Gdl-D.F.

En la gráfica se observa como el tráfico de video, WWW y SMTP excede su límite de pérdida de paquetes para un tráfico total de 34.5 Mbps, en tanto, el tráfico de voz supera su límite permitido a partir de los 35.5 Mbps. El tráfico FTP y BE no experimenta pérdida de paquetes debido a que el flujo de tráfico inyectado por cada uno de ellos no es suficiente para desbordar su cola correspondiente, o en el caso del tráfico FTP, su retardo extremo a extremo se mantiene debajo de su límite permitido, evitando que estos paquetes sean descartados por los nodos de estadísticas.

Por lo tanto, se concluye que el modelo MPLS sobre SONET garantiza niveles de pérdida de paquetes debajo de su límite permitido para cada tipo de tráfico para porcentajes de utilización del enlace menores al 100%.

V.4.2.4 Caudal Eficaz

La figura 43 presenta el comportamiento del caudal eficaz con respecto a la utilización del enlace para cada tipo de tráfico. En ella se observa un comportamiento lineal del caudal eficaz en tanto la utilización del enlace sea menor al 100%, ya que a partir de este punto el tráfico de video, voz, WWW y SMTP presenta pérdidas de paquetes como puede observarse en la figura 42, teniendo como consecuencia una disminución en el caudal eficaz de estos tipos de tráfico.

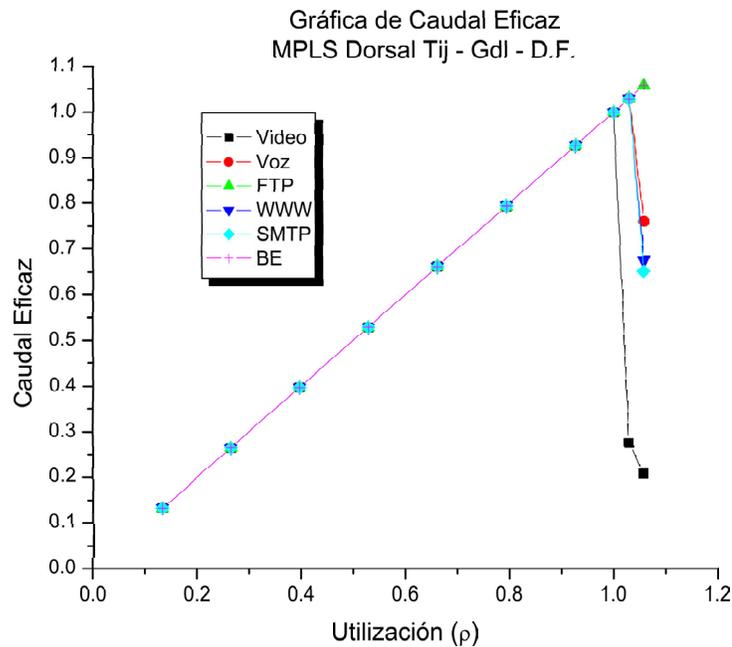


Figura 43. Caudal eficaz para el modelo MPLS Dorsal Tij-Gdl-D.F.

El tráfico de video es el más afectado cuando el tráfico generado excede el ancho de banda del enlace, ya que sus niveles de retardo y variación del retardo exceden de manera considerable sus límites permitidos provocando el descarte de paquetes de video por parte de los nodos de estadísticas, sumando a estos paquetes aquellos que se descarten por el desbordamiento de las colas de video, teniendo como consecuencia que este tipo de tráfico cuente con la mayor probabilidad de pérdida de paquetes y por lo tanto, el menor caudal eficaz en los períodos de congestión del enlace.

V.4.3 Comparación entre los modelos DiffServ sobre ATM y MPLS sobre SONET Dorsal Tij-Gdl-D.F.

Una vez que se ha llevado a cabo el análisis de resultados de acuerdo a los parámetros que miden la Calidad de Servicio, se realiza una comparación entre los resultados obtenidos para el modelo DiffServ sobre ATM - 6 PVCs y MPLS sobre SONET Dorsal Tij-Gdl-D.F.

V.4.3.1 Retardo Extremo a Extremo

En la figura 44 se presentan las gráficas del comportamiento del retardo extremo a extremo de los servicios de video, voz, FTP, WWW, SMTP y BE para los modelos mencionados anteriormente. En estas gráficas se observan niveles de retardo mayores (entre 10 y 20 mseg aproximadamente) para el modelo DiffServ sobre ATM, lo cual

es de esperarse debido a que en este modelo se realiza la segmentación de los paquetes en celdas ATM y su correspondiente reensamble lo que introduce un tiempo de procesamiento mayor para cada paquete en su paso por los enrutadores.

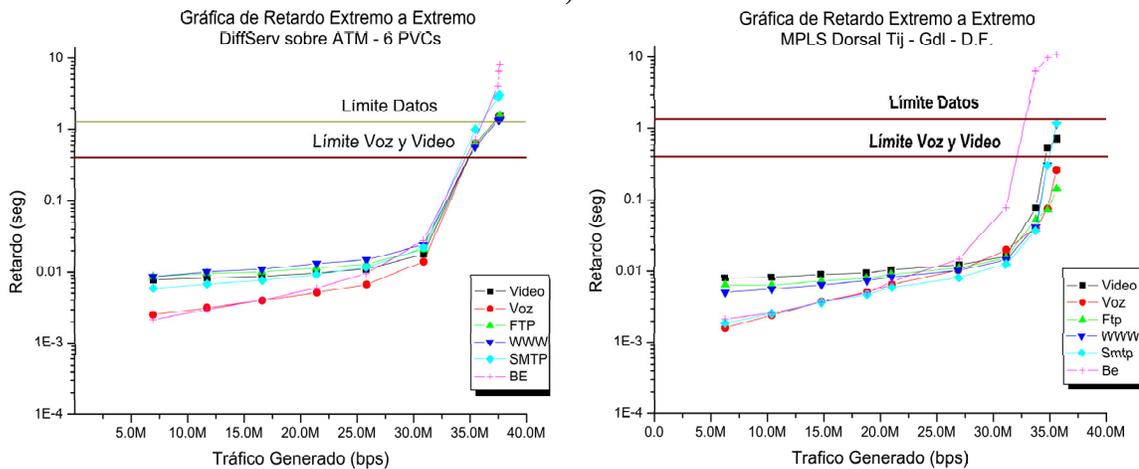


Figura 44. Comparación entre los modelos DiffServ sobre ATM y MPLS sobre SONET de acuerdo al retardo extremo a extremo de cada tipo de servicio.

En el modelo MPLS, los valores de retardo de los distintos tipos de servicios, con excepción de BE, se mantienen estables para un tráfico generado de hasta 34 Mbps, en cambio, en el modelo DiffServ, los valores de retardo se incrementan para un tráfico generado de 32 Mbps. Por lo tanto, MPLS hace un uso más eficiente del ancho de banda del enlace ya que reduce el sobreencabezado en los paquetes a diferencia de ATM.

V.4.3.2 Variación del Retardo

En la figura 45 se presentan las gráficas del comportamiento de la variación del retardo de los servicios de video, voz, FTP, WWW, SMTP y BE para los modelos mencionados anteriormente. Al igual que en los resultados para el retardo extremo a

extremo, los valores de variación del retardo para el modelo DiffServ sobre ATM son mayores que para el modelo MPLS sobre SONET.

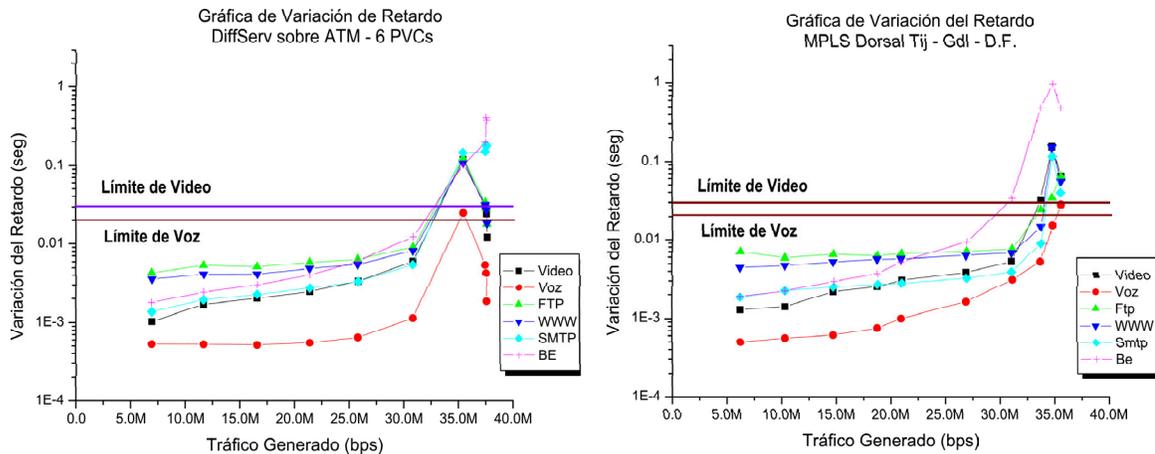


Figura 45. Comparación entre los modelos DiffServ sobre ATM y MPLS sobre SONET de acuerdo a la variación del retardo de cada tipo de servicio.

Los valores obtenidos de variación de retardo para el modelo DiffServ en cuanto a tráfico de video y voz alcanzan sus límites permitidos para un tráfico total de 32.5 Mbps y 34.5 Mbps, en cambio, para el modelo MPLS estos límites son alcanzados cuando se genera un tráfico de 33.5 Mbps y 35 Mbps respectivamente, por lo tanto, MPLS proporciona un mejor servicio a las aplicaciones de video y voz bajo niveles de congestión del enlace.

En cuanto a los tipos de tráfico FTP, WWW y SMTP, MPLS mantiene sus valores de variación del retardo en un nivel bajo hasta los 34 Mbps, una vez excedido este valor, sus valores de variación de retardo aumentan considerablemente, por el contrario, DiffServ sobre ATM solo es capaz de mantener sus niveles de variación de retardo estables para un tráfico de 31 Mbps.

En cambio, DiffServ sobre ATM proporciona un mejor servicio al tráfico Best Effort ya que sus valores de variación de retardo son bajos para un tráfico de 32.5 Mbps, mucho mejor que MPLS ya que éste solo lo consigue para un tráfico de 27.5 Mbps. Esto se debe a que el tráfico Best Effort es el de menor prioridad, por lo que sus paquetes se quedan en la cola de salida mayor tiempo en comparación con los tipos de tráfico de mayor prioridad.

V.4.3.3 Probabilidad de Pérdida de Paquetes

En la figura 46 se presentan las gráficas del comportamiento de la probabilidad de pérdida de paquetes para los servicios de video, voz, FTP, WWW, SMTP y BE.

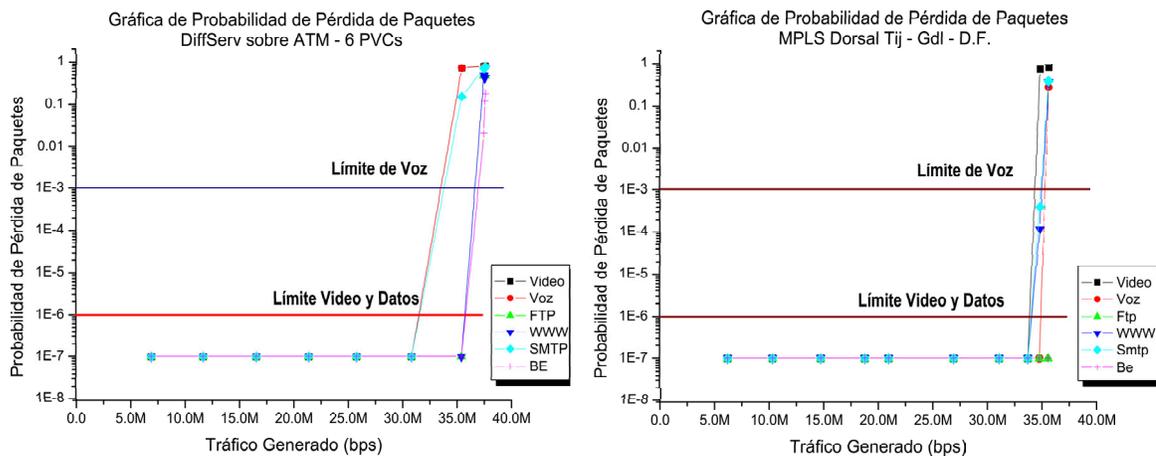


Figura 46. Comparación entre los modelos DiffServ sobre ATM y MPLS sobre SONET de acuerdo a la probabilidad de pérdida de paquetes de cada tipo de servicio.

Se observa como en el caso del modelo DiffServ sobre ATM, los primeros tipos de tráfico que exceden sus límites de pérdida de paquetes son el tráfico de video, SMTP y voz, haciéndolo cada uno de ellos para un tráfico de 31 Mbps, 31 Mbps y 33 Mbps

respectivamente. Para el modelo MPLS sobre SONET estos tres tipos de tráfico experimentan pérdidas de paquetes una vez que el tráfico generado es igual al ancho de banda del enlace (34 Mbps).

El tráfico WWW presentó pérdidas de paquetes para niveles de tráfico de 35 Mbps en el caso del modelo DiffServ sobre ATM y para niveles de 34 Mbps en el modelo MPLS sobre SONET.

El modelo MPLS no presenta pérdida de paquetes de tráfico FTP y BE, el primero debido a que nunca son alcanzados sus límites de retardo y variación de retardo y el segundo aunque experimenta los mayores niveles de retardo y variación de retardo, sus colas no presentan desbordamiento, por lo tanto no presenta pérdida de paquetes. Para el modelo DiffServ sobre ATM ambos tipos de tráfico sufren de pérdida de paquetes, ya sea por exceder sus límites permitidos o por desbordamiento de sus colas.

V.4.3.4 Caudal Eficaz

En la figura 47 se presentan las gráficas del comportamiento del caudal eficaz para los servicios de video, voz, FTP, WWW, SMTP y BE.

En las gráficas presentadas anteriormente se mencionó como para el caso del modelo DiffServ sobre ATM algunos tipos de tráfico superaban sus límites permitidos de retardo, variación del retardo y pérdida de paquetes para niveles de tráfico generado menores al ancho de banda del enlace, esto se ve reflejado en la disminución del caudal eficaz de los tráficos de video, voz y SMTP cuando la utilización del enlace

sobrepasa el 80% (27.2 Mbps) y para el tráfico FTP y WWW cuando el enlace está siendo utilizado al 98% (33.3 Mbps) de su capacidad. En cambio, para el modelo MPLS sobre SONET, todos los tipos de tráfico disminuyen su caudal eficaz cuando el enlace se utiliza al 100%. Por lo tanto MPLS garantiza a cada tipo de tráfico no reducir su caudal eficaz en tanto la utilización del enlace sea menor al 100%.

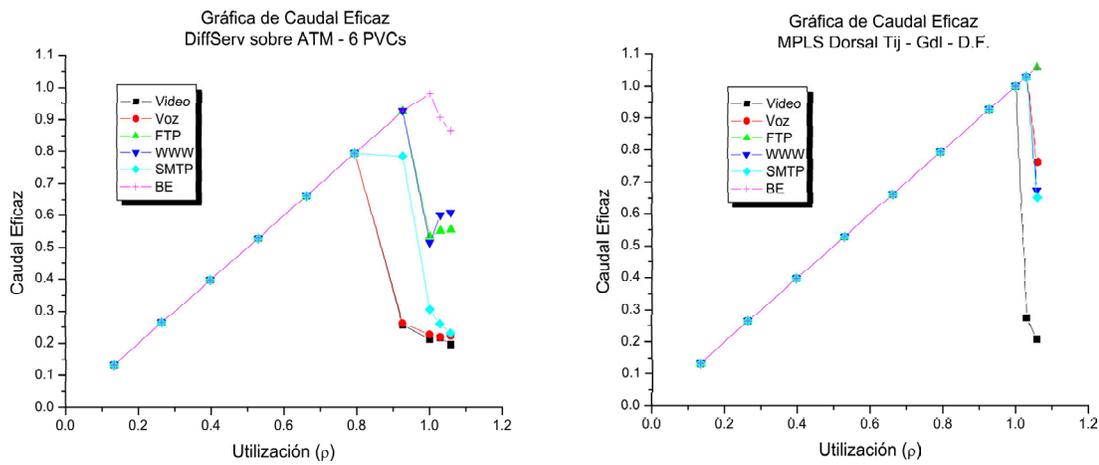


Figura 47. Comparación entre los modelos DiffServ sobre ATM y MPLS sobre SONET de acuerdo al Caudal Eficaz de cada tipo de servicio.

V.4.4 MPLS sobre SONET Dorsal Completa

V.4.4.1 Retardo Extremo a Extremo

En la figura 48 se presenta la gráfica obtenida para el retardo extremo a extremo de los servicios de video, voz, FTP, WWW, SMTP y BE.

En la gráfica se observan niveles estables de retardo extremo a extremo de los distintos tipos de tráfico para un tráfico generado de hasta 25 Mbps. A partir de este punto sus niveles de retardo comienzan a incrementarse, siendo el más afectado el tráfico

BE, el cual sufre un incremento considerable de su retardo hasta alcanzar un máximo de 13 segundos para un tráfico total de 35 Mbps.

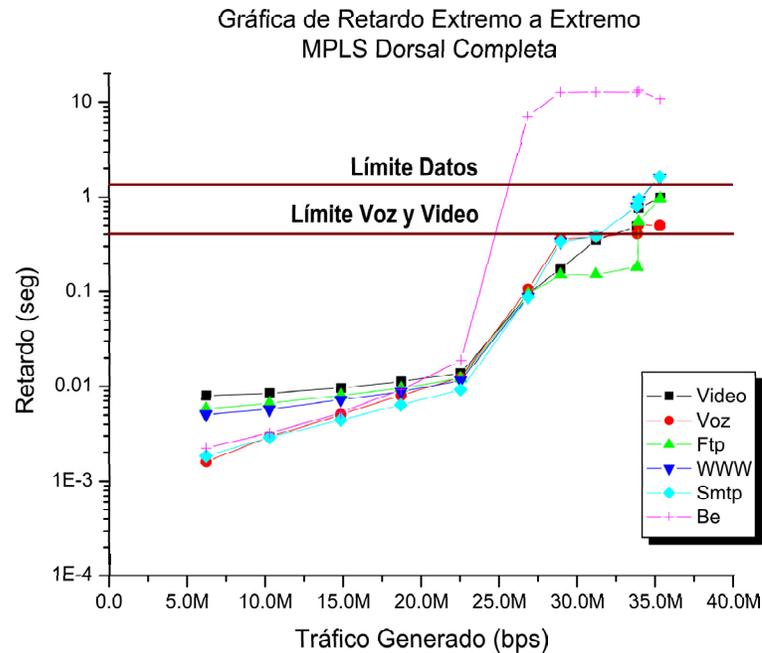


Figura 48. Retardo extremo a extremo para el modelo MPLS Dorsal Completa

En cuanto al tráfico de video y voz, ambos exceden sus límites permitidos para un tráfico de 34 Mbps, en cambio, el tráfico de WWW y SMTP alcanzan sus límites de retardo para un tráfico de 35 Mbps.

El incremento de los niveles de retardo para un tráfico generado de 25 Mbps se debe a que el tráfico total inyectado a la dorsal por parte de los 5 nodos de Asociado Académico es de 125 Mbps, tráfico que casi alcanza la capacidad de los 4 enlaces E3 de los nodos de captura de estadísticas (136 Mbps), provocando que el retardo en esta parte de la dorsal aumente y como consecuencia se incremente el retardo extremo a extremo.

V.4.4.2 Variación del Retardo

En la figura 49 se presenta la gráfica obtenida para la variación del retardo de los servicios de video, voz, FTP, WWW, SMTP y BE. Al igual que en los resultados obtenidos de variación del retardo para el modelo MPLS Dorsal Tij-Gdl-D.F., los valores de variación del retardo para el tráfico Best Effort aumentan considerablemente conforme aumenta el tráfico generado por los otros nodos, en cambio, la variación del retardo para los otros servicios se mantiene estable para valores de tráfico generado de hasta 32 Mbps.

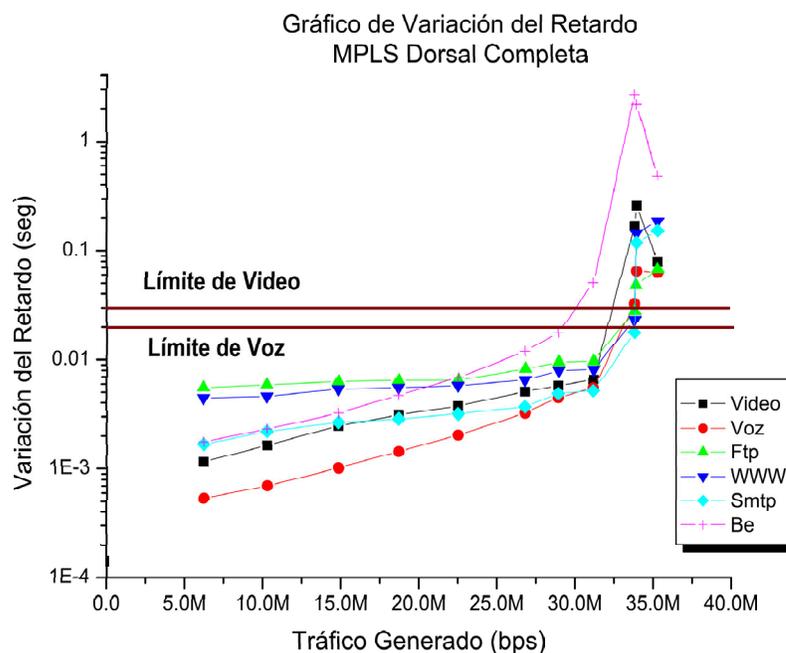


Figura 49. Variación del Retardo para el modelo MPLS Dorsal Completa

Para un tráfico generado de 32 Mbps, el tráfico de video excede su límite permitido, alcanzando su valor máximo para un tráfico de 34 Mbps. En cuanto al tráfico de voz,

excede su límite permitido para un tráfico generado de 33 Mbps, alcanzando su valor máximo a los 34 Mbps.

V.4.4.3 Probabilidad de Pérdida de Paquetes

En la figura 50 se presenta la gráfica obtenida para la probabilidad de pérdida de paquetes de los servicios de video, voz, FTP, WWW, SMTP y BE.

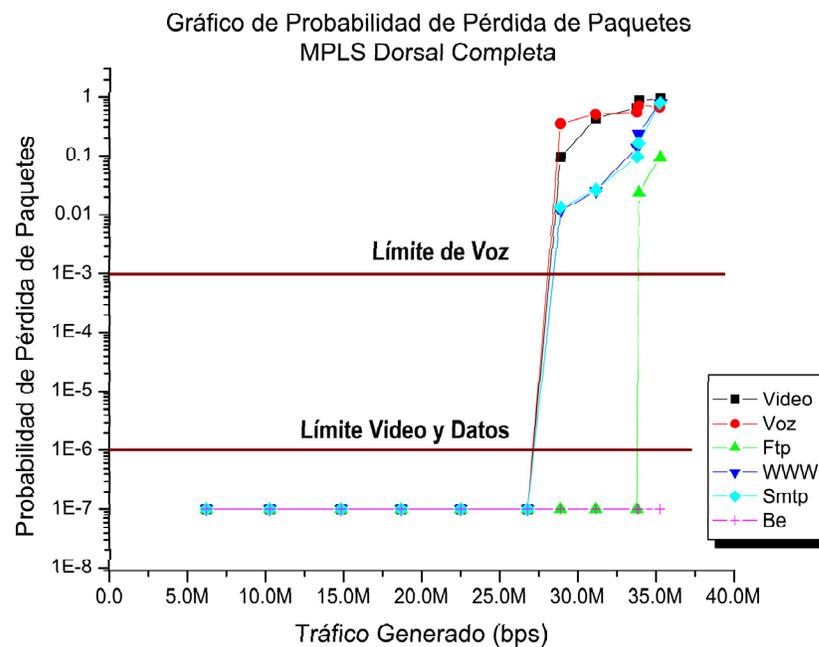


Figura 50. Probabilidad de Pérdida de Paquetes para el modelo MPLS Dorsal Completa

En la gráfica se observa como el tráfico de video, WWW y SMTP exceden sus límites de pérdida de paquetes para un tráfico generado de 27.5 Mbps, lo que equivale a un tráfico total de 137.5 Mbps inyectado a la dorsal por los 5 nodos de Asociado Académico, tal cantidad de tráfico excede el ancho de banda de 136 Mbps de los enlaces de los nodos

de captura de estadísticas, teniendo como consecuencia el desbordamiento de sus colas y por lo tanto el descarte de paquetes.

Cabe mencionar que la pérdida de paquetes también es una consecuencia de niveles de retardo y variación de retardo por arriba de los límites permitidos para cada tipo de tráfico.

V.4.4.4 Caudal Eficaz

La figura 51 presenta el comportamiento del caudal eficaz con respecto a la utilización del enlace para cada tipo de tráfico.

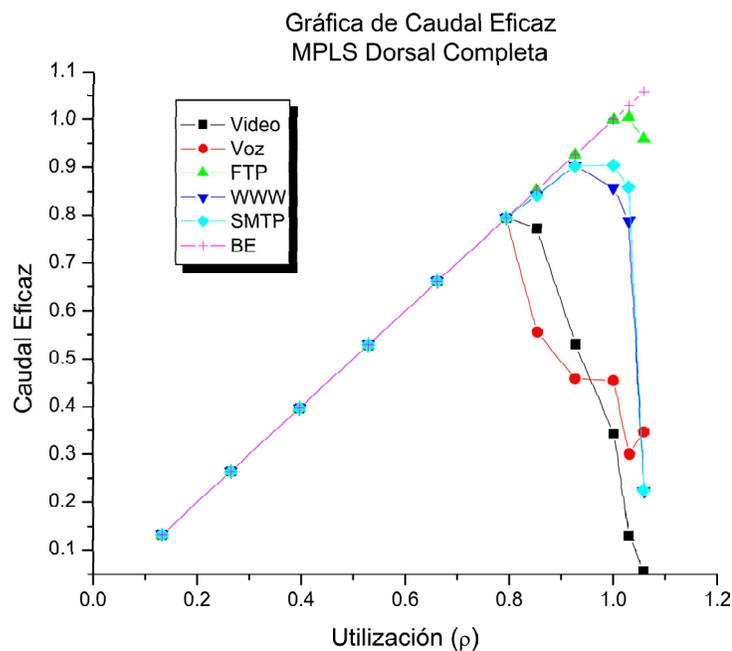


Figura 51. Caudal eficaz para el modelo MPLS Dorsal Completa

En la gráfica se observa una disminución del caudal eficaz de los tráficos de video y voz cuando el enlace se utiliza al 80% (27.2 Mbps) de su capacidad y experimentando su

menor caudal eficaz para una utilización del 105% (35.7 Mbps). Para el tráfico WWW y SMTP su caudal eficaz comienza a disminuir a partir de una utilización del 85% (28.9 Mbps) del enlace, en tanto el tráfico FTP es el que soporta porcentajes de utilización mayor del enlace, ya que su caudal eficaz se reduce una vez que el enlace se utiliza al 100% de su capacidad.

Cabe recordar que este caudal es medido respecto a la utilización del ancho de banda de los nodos generadores de tráfico, ya que si se midiera con respecto a los nodos de recepción de tráfico, el caudal aumenta a valores cercanos al 100%.

En el siguiente capítulo se presentan las conclusiones obtenidas durante la realización del presente trabajo de investigación, así como algunas propuestas sobre trabajos futuros que podrían derivarse del mismo.

Capítulo VI

Conclusiones

VI.1 Conclusiones

En base a los resultados obtenidos en este trabajo de investigación se concluye que se cumplieron satisfactoriamente los objetivos trazados al inicio del mismo, ya que se estudiaron y analizaron los mecanismos necesarios para la interoperabilidad de las arquitecturas de QoS de Servicios Diferenciados y MPLS, además de obtenerse los parámetros de operación óptimos de estos mecanismos para aplicaciones de video, voz y datos.

En cuanto a los niveles de retardo extremo a extremo, variación de retardo, probabilidad de pérdida de paquetes y caudal eficaz obtenidos para los distintos tipos de tráfico, MPLS garantiza mantenerlos debajo de sus límites permitidos en tanto la utilización del enlace sea menor al 100%.

La comparación entre los modelos de MPLS/PoS y DiffServ/ATM permitió observar que definir un PVC con un ancho de banda fijo para cada clase de tráfico (DiffServ/ATM) hace un uso menos eficiente de la red en períodos de congestionamiento (reduce el caudal eficaz), ya que no es posible la asignación dinámica de ancho de banda, a diferencia de MPLS/PoS que si lo permite.

El hecho de realizar un modelo que abarcara un esquema completo de la dorsal de la Red-CUDI, permitió obtener resultados que indican los límites de tráfico que pueden transportar los dos tipos de enlaces que utilizan los nodos de Asociado Académico y Gigapops para su interconexión manteniendo los parámetros de medición de Calidad de Servicio dentro de sus niveles aceptables.

Se concluye que la arquitectura de MPLS E-LSP representa una alternativa viable para ofrecer Calidad de Servicio en redes que utilicen distintas aplicaciones, cada una con diferentes requerimientos de recursos hacia la red.

La arquitectura E-LSP propuesta para ofrecer Calidad de Servicio en una dorsal MPLS, está limitada a la definición de un máximo de 8 PHBs, lo cual representa una desventaja si se toma en cuenta que Servicios Diferenciados permite definir hasta 64 PHBs. Por lo tanto, esta arquitectura cuenta con una menor granularidad en cuanto a definición de clases de tráfico. Sin embargo, como se muestra en este trabajo, 8 PHBs son suficientes para diferenciar los tipos de tráfico más comunes.

VI.2 Aportaciones

En este trabajo de tesis, se tomaron en cuenta las características del equipo que forma la dorsal de la Red-CUDI para realizar el modelado de los mecanismos de Calidad de Servicio, por lo que representa una buena referencia mediante la cual el Comité de Desarrollo de la Red-CUDI puede evaluar el desempeño de una arquitectura DiffServ -

MPLS como una alternativa para otorgar Calidad de Servicio a los usuarios de su red.

Otra aportación importante fue el estudio de un protocolo que actualmente tiene su principal aplicación en proporcionar Calidad de Servicio en las dorsales de los Proveedores de Servicio de Internet mediante la diferenciación de servicios o Ingeniería de Tráfico, por tal motivo, este trabajo de investigación aporta una arquitectura básica que sigue los lineamientos establecidos por la IETF para la implementación de redes con Calidad de Servicio.

Los resultados de este trabajo de tesis serán presentados en la Reunión de Otoño de Comunicaciones, Computación y Exposición Industrial (ROC&C) 2003 la cual es organizada por la IEEE en la ciudad de Acapulco, Guerrero y en la Reunión de Otoño de CUDI a realizarse en Puebla, Puebla.

VI.3 Recomendaciones

Uno de los grandes problemas que enfrentan la mayoría de los alumnos que requieren llevar al cabo modelado y simulación durante su trabajo de tesis es que desconocen la metodología y las técnicas que existen para realizarlos, agregando a esto el tiempo que les toma aprenderlas. Es por esta razón que se recomienda incluir una asignatura o en su defecto incluir dentro del temario de alguna de estas, material concerniente a las técnicas de modelado y simulación de las cuales puede ayudarse el alumno para realizar un buen trabajo de simulación.

VI.4 Trabajos Futuros

Modelar la arquitectura MPLS incluyendo protocolos de distribución de etiquetas como LDP o CR-LDP tomando en cuenta el establecimiento de rutas con restricciones, así como el estado del enlace para determinar la mejor trayectoria mediante la cual enviar los paquetes, es decir, aplicar la Ingeniería de Tráfico.

Realizar un análisis teórico sobre los otros mecanismos de clasificación, acondicionamiento, control de admisión y calendarización de tráfico que utilizan los enrutadores Cisco que forman la dorsal de la Red-CUDI, con el fin de modelarlos y compararlos con los resultados obtenidos en este trabajo de tesis.

Literatura Citada

- Barford, P. y Crovella, M. 1998. “*Generating Representative Web Workloads for Network and Server Performance Evaluation*”, ACM SIGMETRICS 1998. Madison, Wisconsin: 151-160 p.
- Black, U. 2002. “*MPLS and Label Switching Networks*”, Prentice Hall PTR. Segunda Edición. Upper Saddle River, NJ. 314 pp.
- Bong, R. 1998. “*The importance of long-range dependence of VBR video traffic in ATM traffic engineering: Myths and Realities*”, Department of Electrical Engineering and Center for Telecommunications Research, Columbia University New York: 1-23 p.
- Caballero Cárdenas, X. G. 2002. “*Análisis y modelado de mecanismos de servicios diferenciados (DiffServ) para la implementación de redes con calidad de servicio (QoS)*”. Departamento de Electrónica y Telecomunicaciones, CICESE. Ensenada, B. C. Tesis de Maestría en Ciencias. 107 pp.
- Cisco Systems. 2001. “*Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2*”, Cisco Press: 1-476 p.
- Cisco Systems. 2003. “*Does the PA-A1 ATM Port Adapter Support Traffic Shaping?*”, Cisco Systems: 1-10 p.
- Cruz Patiño, H. R. 2001. “*Análisis y modelado de mecanismos para la implementación de redes con calidad de servicio*”. Departamento de Electrónica y Telecomunicaciones, CICESE. Ensenada, B. C. Tesis de Maestría en Ciencias. 80 pp.
- Ferguson, Paul y Huston, Geoff. 1998. “*Quality of Service*”, John Wiley & Sons, Inc. Segunda Edición. New York. 365 pp.
- Le Faucher, F., Wu, L., Davie, B., Davari, S., Vaananen, P., Krishnan, R., Cheval, P. y Heinanen, J. 2002. “*RFC 3270: Multiprotocol Label Switching (MPLS) Support of Differentiated Services*”, Internet Engineering Task Force: 1-64 p.
- RACE Specification D-511. 1994. “*Quality of Service Parameters for Videoconferencing*”, IBC Common Functional Specification. 13 pp.
- RACE Specification D-732. 1994. “*Mobile Communications: Service Aspects*”. IBC Common Functional Specification. 37 pp.
- Rosen, E., Viswanathan, A. y Callon, R. 2001. “*RFC 3031: Multiprotocol Label Switching Architecture*”, Internet Engineering Task Force: 1-61 p.

- Rouhana, N. y Horlait, E. 2000. *“Differentiated Services And Integrated Services use of MPLS”*, Fifth IEEE Symposium on Computers and Communications. Antibes, Francia: 194-199 p.
- Semeria, C. 2002. *“Supporting Differentiated Service Classes: Multiprotocol Label Switching (MPLS)”*, Juniper Networks White Paper. 8(2): 1-18 p.
- Tappan, D., Rosen, E., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T. y Conta, A. 2001. *“RFC 3032: MPLS Label Stack Encoding”*, Internet Engineering Task Force: 1-23 p.
- Thomas, S. A. 2001. *“IP Switching And Routing Essentials: Understanding RIP, OSPF, BGP, MPLS, CR-LDP, And RSVP-TE”*, John Wiley & Sons, Inc. Primera Edición. New York. 352 pp.
- Wang, Z. 2001. *“Internet QoS: Architectures and Mechanisms for Quality of Service”*, Morgan Kaufmann Publishers. Primera Edición. San Francisco, CA. 345 pp.
- Weiss, W. 1998. *“QoS with Differentiated Services”*, Bell Labs Technical Journal. 3(4): 48-62 p.

Apéndice A

Modelos de Tráfico

A.1 Introducción

En el presente trabajo de tesis se habla acerca de un modelado de fuentes de tráfico de video, voz, FTP, WWW y SMTP por lo que en las siguientes secciones se presenta una breve descripción del modelado de cada una de las fuentes.

A.2 Modelo para Fuente de Tráfico de Voz

En una conversación telefónica las personas no hablan continuamente, sino que en promedio una persona habla de un 35% a un 40% del tiempo de duración de la llamada. Por esta razón el modelado de una fuente de tráfico de voz se realiza mediante una fuente ON-OFF.

Una fuente ON-OFF alterna entre dos estados ON y OFF, manteniéndose en cada estado un tiempo determinado. Los parámetros para modelar una fuente ON-OFF se basan en una distribución de los periodos ON y OFF, así como en los tiempos de Inter-salida e Inter-arribo.

Matemáticamente el modelo ON-OFF se representa por una cadena de Markov de

tiempo continuo de dos estados. El tiempo de duración de los estados ON y OFF es exponencialmente distribuido con media α^{-1} y β^{-1} respectivamente. Por lo tanto α^{-1} representa el tiempo promedio que la fuente se mantendrá en estado ON y β^{-1} representa el tiempo promedio que la fuente se mantendrá en el estado OFF. Las siguientes ecuaciones definen los tiempos mencionados anteriormente.

$$\text{Estado ON} = F_{\alpha}(t) = 1 - e^{-\alpha t} \quad (3)$$

$$\text{Estado OFF} = F_{\beta}(t) = 1 - e^{-\beta t} \quad (4)$$

$F(t)$ representa la distribución acumulativa en ambos estados y además modela el proceso para las ráfagas de voz de una fuente.

A.3 Modelo para Fuente de Tráfico de Video

El modelado de la fuente de tráfico de video se realizó de acuerdo a las especificaciones de la recomendación H.323 para videoconferencia, específicamente se utilizó el codificador H.263.

H.263 soporta cinco tipos de resoluciones, QCIF es la que posee mayor resolución ya que las tramas manejan una secuencia de bloques de 176X144 pixeles (176 para información de luminancia y 144 para información de cromancia). Por lo tanto este

tipo de resolución fue la elegida para fines del modelado de la fuente de tráfico de video. La tasa de transmisión para este tipo de resolución será entonces de 30 tramas por segundo. Por lo tanto se generan una trama de 50Kbits cada 33.33mseg.

El modelado de la fuente de tráfico de video, también se realizó mediante una fuente ON-OFF.

A.4 Modelo para Fuente de Tráfico FTP

Las conexiones FTP se encuentran formadas por conjuntos de datos en ráfaga y la distribución para los tamaos de ráfaga dadas en bytes es del tipo heavytailed, encontrando que la distribución que mas se ajusta al comportamiento del tráfico FTP es la de Pareto con un parámetro de forma que puede estar entre $0.9 \leq \alpha \leq 1.4$ para la distribución del tamaño de los paquetes y $\alpha = 0.95$ para el tiempo de espera entre la llegada de un paquete y otro.

El tráfico auto-similar puede ser modelado multiplexando un gran número de fuentes del tipo ON-OFF, donde la duración de los periodos ON u OFF son del tipo heavy-tailed [Barford y Crovella, 1998].

En la figura 52 se observa el modelo para fuentes FTP programado en OPNET, donde podemos observar que éste se encuentra conformado por dos fenómenos del tipo ON-OFF. El primer fenómeno ON-OFF representa la duración de un inicio de sesión. Dentro del estado ON (ON activo) se tiene otro fenómeno ON-OFF, donde los estados

ON representan la generación y envío de un archivo FTP y el tiempo OFF (OFF activo), representa el tiempo de espera entre los arribos FTP.

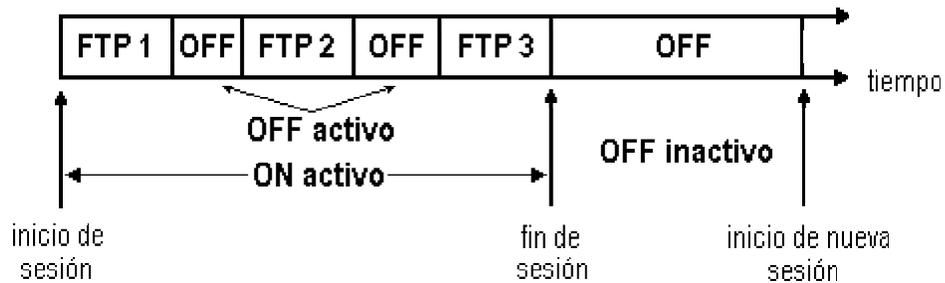


Figura 52. Modelo ON-OFF utilizado para la fuente de tráfico FTP

A.5 Modelo para Fuente de Tráfico WWW

El tráfico WWW posee propiedades auto-similares y puede ser construido multiplexando un gran número de fuentes ON-OFF, donde la duración de los estados ON y OFF representa procesos del tipo heavy-tailed.

En la figura 53 se presenta el modelo ON-OFF utilizado para la generación del tráfico WWW, en donde el periodo ON activo corresponde a la duración de la transmisión de un archivo individual WWW, y el tiempo OFF inactivo corresponde al intervalo entre las transmisiones. Dentro del intervalo de tiempo ON activo se generan peticiones URL, las cuales dependen de los objetos que tenga la página solicitada por el usuario y esto se modela mediante el uso de otra fuente ON-OFF, donde el estado ON representa la generación de un URL y el estado OFF activo, el tiempo de espera entre la generación

de un URL y otro [Barford y Crovella, 1998].

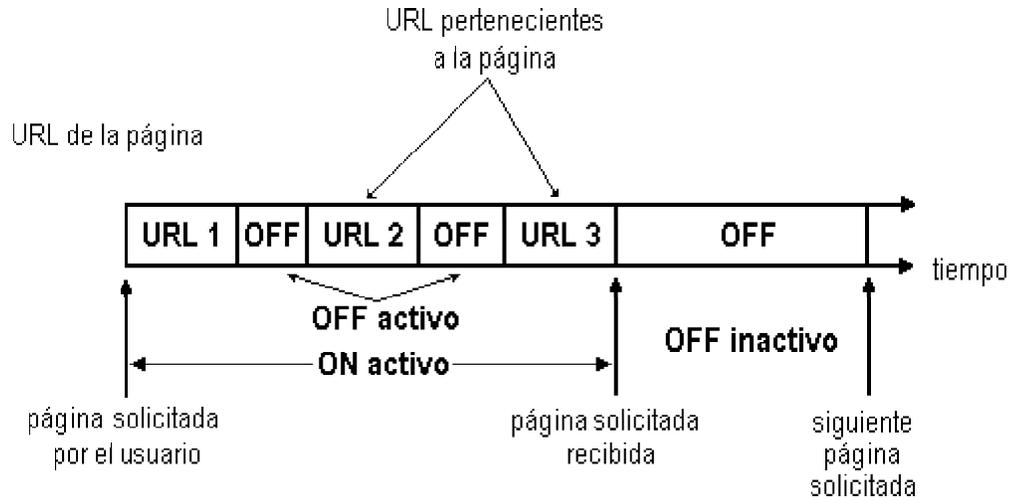


Figura 53. Modelo ON-OFF utilizado para la fuente de tráfico WWW

A.6 Modelo para Fuente de Tráfico SMTP

Este servicio es sólo para la transferencia de correo electrónico, el cual debería ser sólo de mensajes cortos, lo que conllevaría a la generación de tráfico que posea tamaños de ráfaga pequeños. No obstante, en estudios realizados sobre la medición de tráfico en algunas redes, se encontró que este tipo de servicio es también usado para la transferencia de archivos. Por tal motivo este tipo de tráfico presenta un comportamiento bimodal.

Para modelar este comportamiento se usaron dos funciones de distribución Log-normal, una para modelar el tráfico que se encuentre por abajo del 80% y otra para

modelar el tráfico que se encuentre en el 20% restante. Este comportamiento se observa en la figura 54, donde podemos notar que el tráfico por abajo del 80%, presenta tamaños de ráfaga menores que el tráfico que se encuentra dentro del 20% restante. La línea horizontal indica a partir de dónde se usa una distribución y dónde otra.

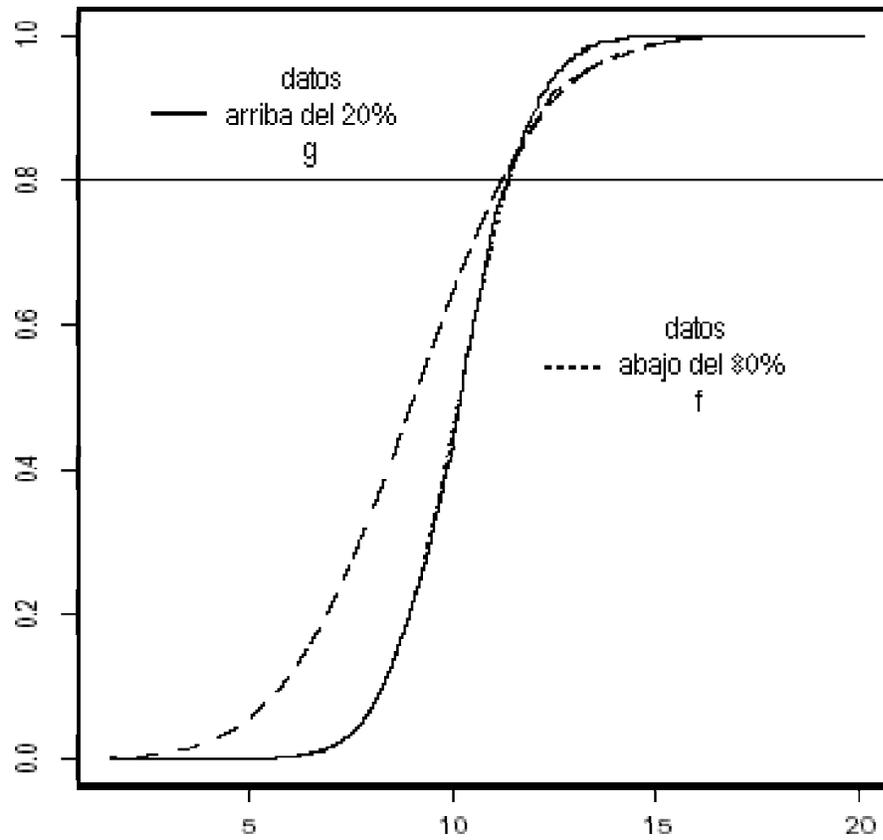


Figura 54. Comportamiento bimodal de la fuente de tráfico SMTP

Lista de Acrónimos

| | |
|----------|--|
| AF | Assured Forwarding |
| AQS | Average Queue Size |
| ATM | Asynchronous Transfer Mode |
| BA | Behavior Aggregate |
| BE | Best Effort |
| BGP | Border Gateway Protocol |
| CICESE | Centro de Investigación Científica y de Educación Superior de Ensenada |
| CLP | Cell Loss Priority |
| CoS | Class of Service |
| CR-LDP | Constraint-Based LDP |
| CSR | Cell Switching Router |
| CUDI | Corporación Universitaria para el Desarrollo de Internet |
| DiffServ | Differentiated Services |
| DSCP | DiffServ Codepoint |
| EF | Expedited Forwarding |
| E-LSP | EXP Inferred PSC LSP |
| EXP | Experimental Field |
| FEC | Forwarding Equivalence Class |
| FR | Frame Relay |
| FTN | FEC to NHLFE |
| FTP | File Transfer Protocol |
| IETF | Internet Engineering Task Force |

| | |
|---------|---|
| ILM | Incoming Label Map |
| IntServ | Integrated Services |
| IP | Internet Protocol |
| IPN | Instituto Politecnico Nacional |
| ISP | Internet Service Provider |
| ITESM | Instituto Tecnológico y de Estudios Superiores de Monterrey |
| LDP | Label Distribution Protocol |
| L-LSP | Label Inferred PSC LSP |
| LSP | Label Switched Path |
| LSR | Label Switching Router |
| MF | Multifield |
| MPLS | Multiprotocol Label Switching |
| NHLFE | Next Hop Label Forwarding Entry |
| OA | Ordered Aggregate |
| OPNET | Optimum Network Performance |
| OSI | Open System Interconnection |
| PBS | Peak Burst Size |
| PCR | Peak Cell Rate |
| PHB | Per Hop Behavior |
| PIR | Peak Information Rate |
| PLR | Probability Loss Rate |
| PoS | Packets over SONET |
| PPP | Point to Point Protocol |
| PSC | PHB Scheduling Class |
| PVC | Private Virtual Circuit |

| | |
|--------|---|
| QoS | Quality of Service |
| RSVP | Resource Reservation Protocol |
| SDH | Synchronous Digital Hierarchy |
| SLA | Service Level Agreement |
| SMTP | Simple Mail Transfer Protocol |
| SONET | Synchronous Optical Network |
| ToS | Type of Service |
| TTL | Time To Live |
| U de G | Universidad de Guadalajara |
| UACJ | Universidad de Ciudad Juarez |
| UAM | Universidad Autónoma de Mexico |
| UANL | Universidad Autónoma de Nuevo León |
| UBR | Unspecified Bit Rate |
| UCSD | University Of California, San Diego |
| UDLA | Universidad de Las Américas |
| UNAM | Universidad Nacional Autónoma de Mexico |
| VCI | Virtual Circuit Identifier |
| VPI | Virtual Path Identifier |
| VPN | Virtual Private Network |
| WAN | Wide Area Network |
| WFQ | Weighted Fair Queuing |
| WRED | Weighted Random Early Detection |
| WWW | World Wide Web |