ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

"MANEJO DE LA CALIDAD DE SERVICIO EN REDES BASADAS EN MPLS (MULTIPROTOCOL LABEL SWITCHING), BAJO PLATAFORMA LINUX"

TESIS DE GRADO

PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN

SISTEMAS INFORMÁTICOS

ISABEL CRISTINA AGUIRRE VELOZ

MARTHA LUCÍA ORTIZ VACA

RIOBAMBA – ECUADOR

- 2010 -

AGRADECIMIENTO

En primer lugar queremos agradecer a Dios por proveer los medios necesarios para la consecución de nuestra tesis. Y de una forma especial a nuestros padres: Isabel y Jorge, y Lucía y Miguel así como a nuestros hermanos Jorge y Verónica quienes nos han apoyado incondicionalmente brindándonos su soporte moral, económico y ayuda en los momentos más difíciles.

Finalmente queremos agradecer a nuestros amigos, docentes y técnicos de la institución por la comprensión y ayuda generosa en todo momento.

DEDICATORIA

Dedico este trabajo a la memoria de mi querido padre quién con su ejemplo y constancia fueron un pilar primordial y fuente de motivación para la consecución de mis objetivos en la vida.

Cristina Aguirre

Este trabajo va dedicado a mi familia amorosa que es mi fortaleza, mi razón de ser y apoyo completo en todo momento.

Martha Ortiz

FIRMAS RESPONSABLES Y NOTAS

DR. ROMEO RODRIGUEZ _____

DECANO DE LA FACULTAD DE

INFORMÁTICA Y ELECTRÓNICA

ING. IVAN MENES _____

DIRECTOR DE LA ESCUELA

DE INGENIERÍA EN SISTEMAS

ING. PATRICIO MORENO _____

DIRECTOR TESIS

ING. DIEGO ÁVILA _____

MIEMBRO DE TESIS

LCDO. CARLOS RODRIGUEZ _____

DIRECTOR DEL CENTRO

DE DOCUMENTACIÓN

RESPONSABILIDAD DEL AUTOR

Nosotros, Isabel Cristina Aguirre Veloz y Martha Lucía Ortiz Vaca, somos los responsables de las ideas, doctrinas y resultados expuestos en esta Tesis y el patrimonio intelectual de la misma pertenecen a la Escuela Superior Politécnica de Chimborazo.

_____ _____

Isabel Cristina Aguirre Veloz Martha Lucía Ortiz Vaca

ÍNDICE DE ABREVIATURAS

ATM	Asynchronuos Transfer Mode
CBWFQ	Class Based Weighted Fair Queuing
CIFS	Common Internet File System
CLI	Command line interface
CoS	Clases de Servicio.
DIFFSERV	Differentiated Services
DSCP	Differenciated Service Code Point
EIS	Escuela Ingeniería en Sistemas
ESPOCH	Escuela Superior Politécnica de Chimborazo
FEC	Forwarding Equivalence Class
FIFO	First Input First Output
HTTP	Protocolo de Transferencia de Hipertexto
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
INTSERV	Integrated Services
LDP	Label Distribution Protocol

LER	Label Edge Router
LSA	Link-State Advertisements
LSP	Label Switched Path
LSR	Label Switching Router
MPLS	Multi-Prototocol Label Switching
OSPF	Open Short Path First
PC	Personal Computer
QoS	Calidad de Servicio.
RA	Reenvío Asegurado
RR	Reenvío Rápido
RTP	Real Time Protocol
SMB	Server Message Block
SSH	Secure Shell
TCP/IP	Transmission Control Protocol/Internet Protocol
TOS	Type of Service
TTL	Time to Live
WFQ	Weighted Fair Queuing

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRAFICOS

INTRODUCCIÓN

Hoy por hoy la realidad nos dice que las redes informáticas, se han vuelto indispensables, tanto para las personas como organizaciones. Les da oportunidad de interactuar con el resto del mundo, ya sea por motivos comerciales, personales o emergencias.

La optimización en el uso de los sistemas informáticos es uno de los elementos de interacción y desarrollo que rige los destinos de la ciencia informática.

Las redes informáticas resultan ser uno de los elementos tecnológicos más importantes al momento de definir un sistema informático en una organización.

Con la implantación de calidad de servicio (QoS), es posible ofrecer mayor garantía y seguridad para las aplicaciones avanzadas, cuando el tráfico de estas aplicaciones pasa a tener prioridad en relación con aplicaciones tradicionales.

En el capítulo I Marco Referencial se propone el estudio de sistemas operativos, o herramientas de software libre: Fedora, Debian Mikrotik, que permitan la configuración y simulación de un router e incorporen Calidad de Servicio.

En el capítulo II Marco Teórico, se realiza un estudio de los conceptos necesarios para entender el funcionamiento y la implementación de la Calidad de Servicio en redes, se

describe aquellas herramientas que se consideraron apropiadas para la implementación de la misma.

En el capítulo III Marco Propositivo, se describe la herramienta utilizada, se establece a demás el escenario sobre el cual se desarrollaran las configuraciones e implementación de QoS, con sus respectivos parámetros, permitiendo predecir el comportamiento de la red en presencia de carga y evaluar el impacto de diferentes políticas en dicho funcionamiento,

En el capítulo IV Análisis de Resultados, se examinan los resultados obtenidos, que incluyen las cabeceras de los paquetes generados en los escenarios de simulación. También se realiza la comprobación de la hipótesis utilizando la fórmula del Chi cuadrado.

CAPÍTULO I

MARCO REFERENCIAL

1.1 Introducción

En el presente capítulo se plantea el estudio y análisis previo de sistemas operativos, o herramientas de software libre: Fedora, Debian Mikrotik, debido a que estos permiten la implementación y simulación de routers para la configuración de escenarios que incorporen el protocolo OSPF para la generación de la ruta más corta y la implementación de MPLS que adapta los flujos de tráfico a los recursos físicos de la red

Se detalla los lineamientos y directrices que ayudaran a desarrollar el proyecto de una forma eficaz y objetiva. Se define las metas principales de este proyecto para cumplir con la planificación establecida de recursos como: recursos financieros, recursos humanos, recurso tiempo.

1.2 Problematización

1.2.1 Planteamiento

1.2.1.1 Descripción

El crecimiento imparable de la Internet, así como la demanda sostenida de nuevos y más sofisticados servicios, supone cambios tecnológicos fundamentales respecto a las prácticas habituales desarrolladas a mitad de los años 90. Nuevas tecnologías de transmisión, proporcionan una eficaz alternativa al ATM para multiplexar múltiples servicios sobre circuitos individuales. Los tradicionales conmutadores ATM están siendo desplazados por una nueva generación de rotures con funciones especializadas en el transporte de paquetes en el núcleo de las redes. Esta situación se complementa con una nueva arquitectura de red de reciente aparición, conocida como Multi-Prototocol Label Switching (MPLS).

MPLS es un estándar emergente del IETF que surgió para consensuar diferentes soluciones de conmutación multinivel, MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM. También como un protocolo para hacer túneles, o bien como una técnica para acelerar el encaminamiento de paquetes, que trabaja en la capa 2 y la capa 3, razón por la cual se dice que es de capa 2.5.

MPLS se considera como el avance más reciente en la evolución de las tecnologías de routing y forwarding en las redes IP, lo que implica una evolución en la manera de construir y gestionar estas redes. Los problemas que presentan las soluciones actuales de IP sobre ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes separadas y tecnológicamente diferentes, quedan resueltos con MPLS.

1.2.1.2 Análisis

MPLS es una solución clásica y estándar al transporte de información en las redes, aceptado por toda la comunidad de Internet, para el envío de información, utilizando routing de paquetes con ciertas garantías de entrega.

Uno de los principales beneficios de los servicios basados en MPLS reside en su capacidad para aplicar calidades de servicio (QoS) mediante la priorización del tráfico en tiempo real, una prestación clave cuando se quiere introducir voz y vídeo en las redes de datos. Por ser una tecnología altamente escalable y menos compleja que sus predecesores, las empresas ganan además en flexibilidad y en reducción y control de costes, y carga de trabajo

En la carrera de Ingeniería en Sistemas de ESPOCH, existe la asignatura de Redes de Computadores II, entre los contenidos tratados en la materia se imparte la enseñanza referente a redes WAN, siendo uno de los subtemas MPLS.

1.2.2 Formulación

¿De qué manera influye la configuración e implementación del protocolo MPLS en la mejora de la QoS de redes?

1.2.3 Sistematización

¿Qué sistemas operativos permiten la simulación de routers sobre máquinas de escritorio?

¿Cuáles son las ventajas y desventajas de utilizar software que simule el trabajo de equipos router propietarios?

¿Cómo solucionar los problemas de calidad de servicio y aprovechar los recursos de la red?

¿Existen estudios realizados de configuración de Calidad de Servicio sobre el protocolo MPLS utilizando Mikrotik RouterOS ?

1.3 Justificación

MPLS es una tecnología de reciente implementación, ofrece nuevas posibilidades en la gestión de routers de backbones, utilizados por los proveedores de servicios de Internet como CNT, Impsat, entre otros.

En la actualidad comprar routers con tecnología MPLS resultan costosos, para universidades públicas como en el caso de la ESPOCH, por lo que los estudiantes se ven limitados al uso de simuladores para el aprendizaje y desarrollo de determinadas prácticas, estos últimos dan una visión general de lo que constituye el uso de esta tecnología, siendo de vital importancia realizar configuraciones en escenarios reales para obtener un conocimiento más práctico en lo que son los MPLS.

Mediante la configuración de una red MPLS simulando un router sobre una PC de escritorio, y con la utilización de técnicas y herramientas de Calidad de Servicio (QoS), se puede investigar los beneficios que ofrecen este tipo de redes.

Esto va a constituir un aporte a la enseñanza en la ESPOCH en la materia de Redes de Computadores II que se dicta en la EIS.

En primera instancia se quiso desarrollar el manejo del escenario bajo el sistema operativo Linux, se realizaron las primera pruebas sobre Fedora 5, en esta distribución se tuvieron problemas de compatibilidad del kernel con los paquetes MPLS necesarios para su configuración, se produjo una serie de errores al momento de la compilación del núcleo, lo que provocó que los módulos necesarios para la configuración no se instalen de forma adecuada.

Al investigar sobre alternativas que nos permitan la consecución de los objetivos encontramos que una opción para la implementación es Mikrotik RouterOS, siendo un sistema operativo el cual convierte a una PC Intel ó un Mikrotik RouterBOARD en un router dedicado.

El sistema operativo se basa en el Kernel de Linux 2.6, es muy estable y a demás ofrece la posibilidad de implementar MPLS, por lo que se puede realizar la configuración de la red a través de equipos hardware como PCs que tengan este S.O

Para la construcción del escenario se configuró en primera instancia el protocolo de enrutamiento OSPF, con el cual los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente, mientras que MPLS adapta los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén supra utilizados, con posibles puntos

calientes y cuellos de botella, mientras otros puedan estar infrautilizados, en síntesis no establece el camino más corto sino el menos congestionado.

La estructura física de la nube MPLS, se constituye básicamente por cinco máquinas cada una con el S.O, Mikrotik RouterOS , con tres tarjetas de red en dos pc routers, y dos tarjetas de red en las tres pc routers sobrantes para la conexión entre estas como se muestra en el **Gráfico I.1**.

Las cinco máquinas simulan ser routers, estableciéndose una configuración en cada máquina con el escenario planteado, se genera tráfico estableciendo la comunicación entre las máquinas cliente y servidor conectados a la nube MPLS y medir el tráfico basándose en los parámetros de QoS: ancho de banda, retardo explícito, pérdida de paquetes.

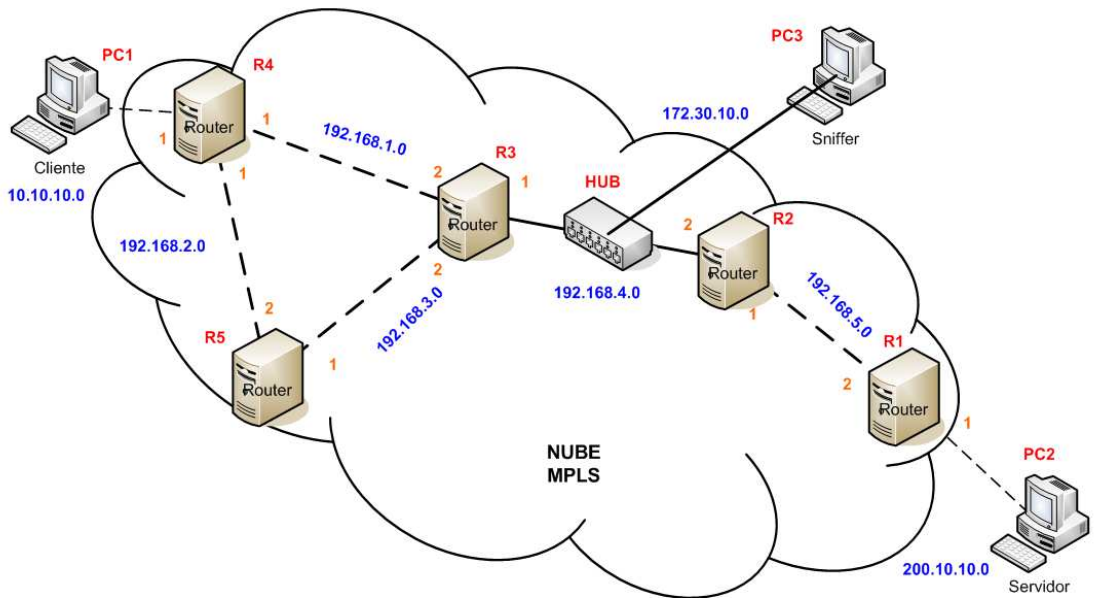


Gráfico I.1 Escenario propuesto

1.4 Objetivos

1.4.1 General

Determinar la calidad de servicio en redes MPLS (Multiprotocol Label Switching), bajo el análisis de los parámetros: ancho de banda, retardo, pérdida de paquetes, jitter.

1.4.2 Específicos

- Simular cinco Routers físicos en computadores de escritorio mediante la utilización del Sistema Operativo Mikrotik RouterOS.

- Analizar la funcionalidad, estructura, características del protocolo MPLS, entendiendo la razón de su existencia y su forma de trabajo.

- Investigar la configuración de los comandos de referencia para la administración de OSPF, MPLS y QoS en Mikrotik RouterOS.

- Desarrollar un manual para la instalación y configuración de redes MPLS sobre plataforma Linux, de utilidad para los estudiantes de la materia de Redes de Computadores II.

1.5 Hipótesis

"El manejo de la calidad de servicio en redes basadas en MPLS bajo plataforma Linux, permitirá la administración de manera más eficiente de las redes WAN".

1.6 Métodos y Técnicas

En este apartado se analiza el uso de los métodos y técnicas empleadas para el desarrollo de la tesis.

1.6.1 Métodos

1.6.1.1 Método Científico

Se utilizará este método para la recolección de información y desarrollo de la investigación.

1.6.1.2 Método Experimental

Se fundamenta en el método científico, comprueba en forma objetiva una ley o una verdad científica, enriquece la calidad de información, datos y vivencias que contribuyen a interpretar la realidad y a actuar sobre ella conscientemente. En la práctica se experimentará en un escenario formado por varias PCs, configuradas, en el cual se podrá aceptar o rechazar la hipótesis formulada.

1.6.2 Técnicas

- **Encuestas y Entrevistas:** Se usará esta técnica para obtener información de empresas que emplean el protocolo MPLS.
- **Revisión de Documentación:** Utilizaremos esta técnica para la recolección de información más importante para nuestro análisis y configuración del protocolo bajo Linux.
- **Consultas bibliográficas:** Se utilizara para la recolección de información.
- **Pruebas prácticas:** Se utilizará para determinar la funcionalidad en tiempo real del entorno de trabajo de QoS en MPLS.

CAPÍTULO II

MARCO TEÓRICO

2.1 Introducción

En el presente capitulo se detalla los conceptos básicos que permitan un mejor entendimiento del funcionamiento de los protocolos de enrutamiento de paquetes OSPF y del protocolo de conmutación de etiquetas MPLS, así como de la importancia de la calidad de servicio (QoS) en redes IP, esencial para la administración de tráfico en la red.

Se conceptualiza los aspectos generales de MPLS, sus características y funcionamiento necesarios para administrar el tráfico y de la misma forma se analiza el protocolo OSPF.

Se hace también una introducción al estudio de la Calidad de Servicio, entendiéndose sus inicios, los protocolos que se relacionan a este y sus beneficios de implementar una arquitectura basada en MPLS.

2.2 Conceptos

2.2.1 Aspectos Generales de MPLS

MPLS fue inventada en los años 90's y ha tomado diferentes aportes o propiedades de IP Switching (Ipsilon), Cell Switching Enrutador (Toshiba), Tag Switching (Cisco) y switcheo IP basado en rutas agregadas o ARIS (IBM). Las anteriores empresas o tecnologías utilizaban conmutación de etiquetas como un método para el envío de datos. La idea central de MPLS es adicionar una etiqueta a cada paquete que se quiere enviar. A estos paquetes se les asigna un par de valores de longitud corta que sintetizan el origen y destino de dicho paquete.

MultiProtocol Label Switching (MPLS) es una solución versátil dirigida a los actuales problemas al nivel de redes como la velocidad, escalabilidad, calidad de servicio y aplicación de la ingeniería de tráfico.

MPLS ha surgido como una solución inteligente al manejo de ancho de banda y requerimientos de servicio proveyendo una eficiente asignación, envío y conmutación de información o datos a través de redes.

MPLS se encuentra situado entre los niveles de enlace y de red del modelo de referencia OSI; por tanto se podría decir que es un protocolo de nivel 2.5. El **Gráfico II.2** muestra el nexo entre los protocolos de red y el protocolo de nivel de enlace.

Gráfico II.2 Modelo de Referencia de Interconexión de sistemas abiertos OSI

MPLS intenta conseguir las ventajas de ATM, pero sin sus inconvenientes. Asigna a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los routers intermedios (solo se mira la etiqueta, no la dirección de destino).

Las principales aplicaciones de MPLS son:

- Funciones de ingeniería de tráfico (a los flujos de cada usuario se les asocia una etiqueta diferente)
- Policy Routing
- Servicios de VPN
- Servicios que requieren QoS

2.2.2 Características

MPLS (Multiprotocol Label Switching) es una especificación de la IETF que apunta a corregir los problemas asociados al enrutamiento de tráfico en el nivel de red4. Ante la necesidad de consultar la dirección IP de la cabecera en cada salto, MPLS plantea un etiquetado de los paquetes para proceder a un switching de los mismos en cada salto. Esto es una solución versátil que permite aportar velocidad, escalabilidad y mayor control sobre la QoS.

Las características de MPLS son:

- Especifica un mecanismo para administrar tráfico entre diversas maquinas, hardware y aplicaciones.
- Permanece independiente de las niveles 2 y 3.
- Provee un medio para asignar o mapear direcciones IP a etiquetas (valor de segundo nivel) usadas para el reenvío de información o datos.
- Aprovecha las implementaciones existentes para enrutamiento como OSPF (la ruta más corta) y RSVP (protocolo de reservación de recursos).
- Soporta en el nivel dos tecnologías como ATM, Frame Relay, PPP e Ethernet entre otras.

2.2.3 Arquitectura MPLS

Cada router analiza la cabecera del paquete y ejecuta un algoritmo de routing, basándose en la información de esta cabecera.

Las cabeceras de los paquetes contienen mucha más información que la necesaria para elegir el siguiente salto. Elegir el siguiente salto puede ser visto como la composición de dos funciones:

Particionar el conjunto de posibles paquetes en clases de envío equivalentes (**FEC**s).

Asociar cada uno de estos FECs con algún destino.

En lo que respecta a la decisión de reenvío, diferentes paquetes clasificados dentro de un mismo FEC son considerados idénticos. Todos los paquetes pertenecientes a un mismo FEC seguirán el mismo camino.

En el envío IP, un router considerará a dos paquetes dentro del mismo FEC si hay algún prefijo de dirección X en la tabla de routing del router el cuál sea la mayor concordancia para la dirección de destino de los paquetes.

A medida que el paquete sigue circulando por la red, cada router realiza la misma operación de asignación en un FEC.

En MPLS, esta asignación se efectúa solamente cuando el paquete entra en la Red, como se observa en el **Gráfico II.3** Esquema funcional de MPLS.

Tras esto, el FEC al que el paquete ha sido asignado se codifica en un valor llamado Etiqueta.

Cuando un paquete va a ser enviado al siguiente nodo, se le añade la etiqueta. En el resto de los nodos del camino, no se necesitará realizar análisis de la cabecera del paquete. La etiqueta que acompaña al paquete servirá para encontrar el siguiente salto y una nueva etiqueta, procediendo así a repetir el proceso de envío.

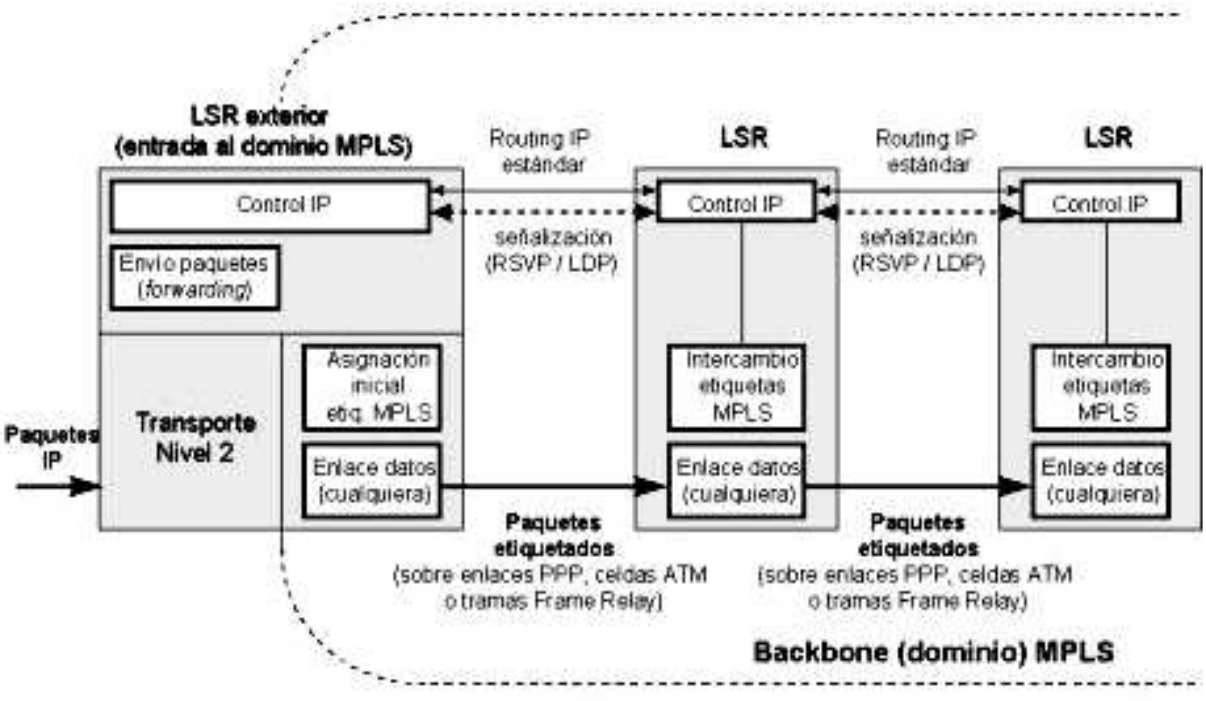


Gráfico II.3 Esquema funcional de MPLS.

A veces se desea forzar un paquete a seguir un camino determinado. Esto puede hacerse para llevar a cabo políticas de envío, o porque se está llevando a cabo ingeniería del tráfico. Para llevarlo a cabo, basta con que una etiqueta represente la ruta, todos los paquetes clasificados según nuestro criterio, seguirán la ruta que hemos creado con la etiqueta.

Un router que soporta MPLS es denominado Router Conmutador de Etiquetas o **LSR** (Label Switched Router).

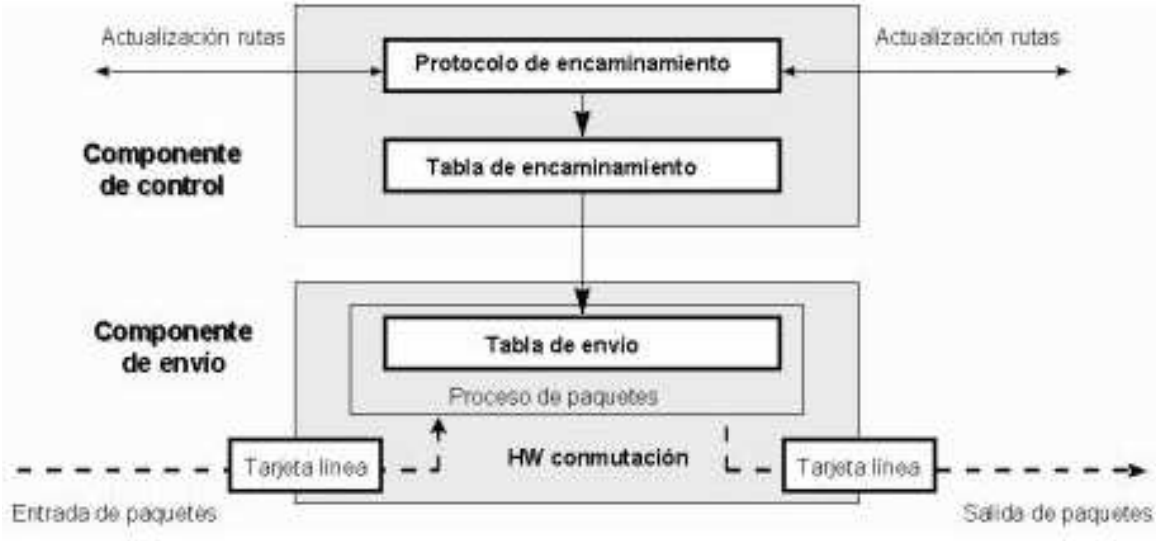


Gráfico II.4 Componente de Control y Envío de Etiquetas.

En el **Gráfico II.4** indica el componente de Envío de Etiquetas, esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control, según se verá más adelante. Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada, que se utilizan para

acompañar a cada paquete que llega por esa interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola).

En el **Gráfico II.5**, se ilustra un ejemplo del funcionamiento de un LRS del núcleo MPLS. A un paquete que llega al LSR por la interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

Gráfico II.5 Detalle de la tabla de envío de un LSR.

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En el **Gráfico II.6** es un ejemplo de envío de un paquete por un LSP, el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 192.168.255.1

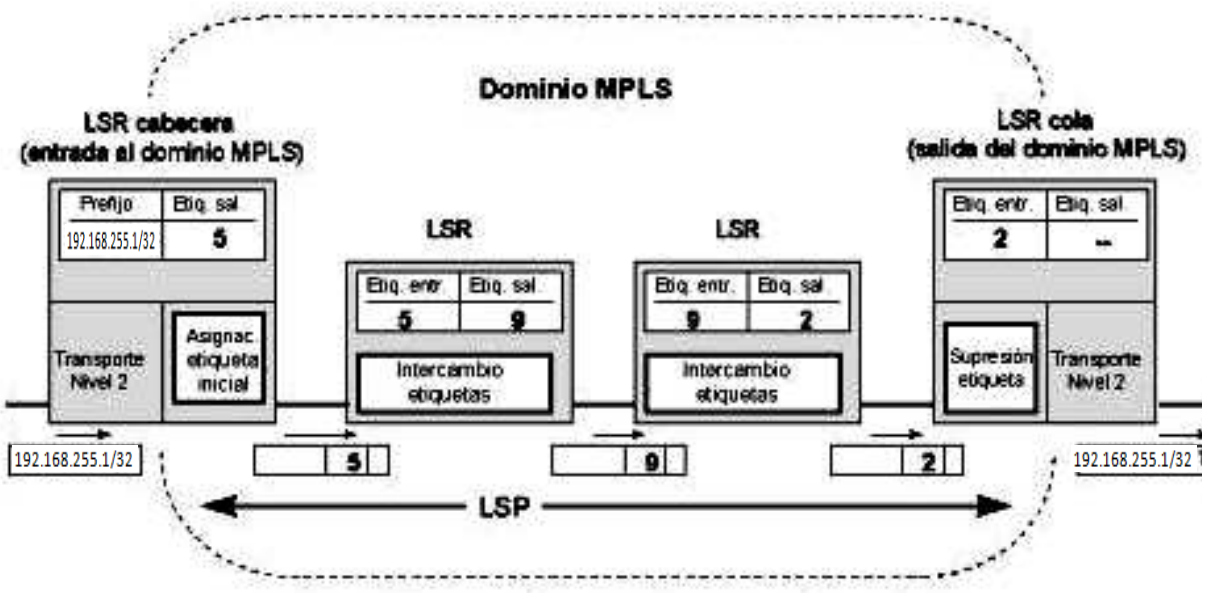


Gráfico II.6 Ejemplo de envío de un paquete por un LSP.

El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo 192.168.255.1/32. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP.

Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar el paquete al LSR de cola. (Salida), ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas quita ésta y envía el paquete por routing convencional.

Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no “mira” sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los caminos LSP. Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3.

Según las especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. Por ello, si el protocolo de transporte de datos contiene ya un campo para etiquetas, se utilizan esos campos nativos para las etiquetas. Sin embargo, si la tecnología de nivel 2 empleada no soporta un campo para etiquetas p. ej. Enlaces PPP o LAN), entonces se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete (nivel 3).

2.2.4 Trama MPLS

La cabecera de un paquete MPLS se encuentra también entre dos niveles, como muestra el **Gráfico II.7**, por tanto, entre la cabecera de nivel de enlace y la cabecera de nivel de red; de esta forma, para el protocolo de nivel de enlace un paquete MPLS serán datos empaquetados de nivel superior del modelo.

Las tecnologías de conmutación multiprotocolos como MPLS separan las características o funcionalidades de envío y control en dos distintos componentes bien distinguibles. El primer componente se encarga de la construcción y mantenimiento de la tabla de envío. El componente de envío es quien realmente está encargado del envío de paquetes. El segundo componente es el esquema de señalización para establecer las etiquetas a lo largo del camino entre el nodo origen y el nodo destino.

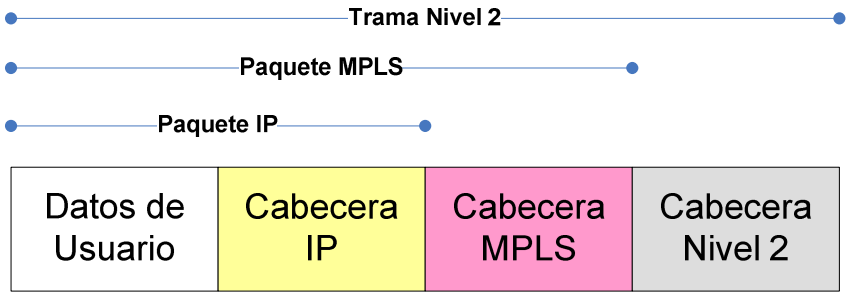


Gráfico II.7 Ubicación de la cabecera MPLS I.

El **Gráfico II.8** muestra la cabecera de un paquete MPLS tiene un tamaño fijo de 32 bits (4 octetos). Ningún campo es de tamaño variable y además siempre se encuentran localizados en la misma posición. La cabecera MPLS como ya se comentó, se situará siempre después de la cabecera de nivel de red y ante de la cabecera de nivel de enlace. Los encaminadores y conmutadores MPLS siempre leerán estos 4 octetos tras la redundancia de enlace.

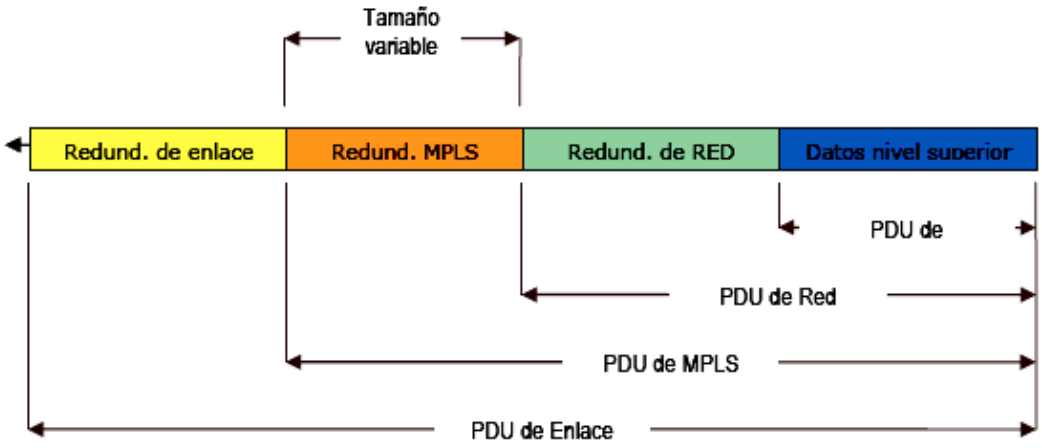


Gráfico II.8 Ubicación de la cabecera MPLS II.

2.2.4.1 Campos

Los campos del paquete MPLS son 4, como se muestra el **Gráfico II.9** a continuación:

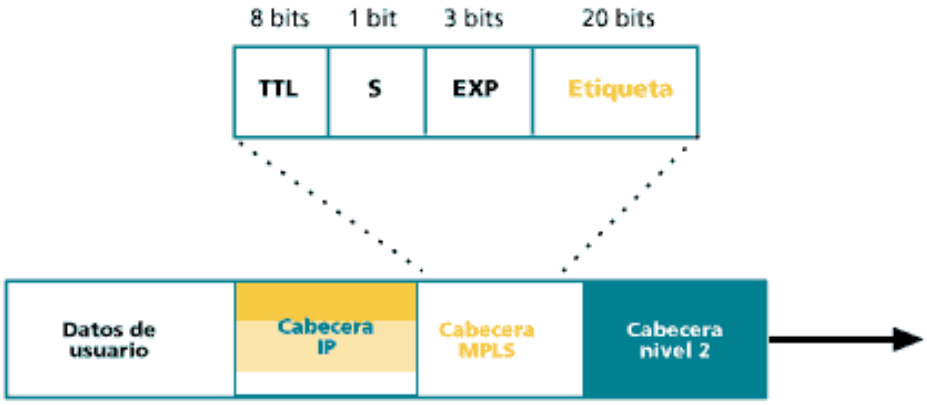


Gráfico II.9 Estructura de la cabecera genérica MPLS.

TTL (Time to Live): Este campo tiene una longitud de 8 bits y es utilizado para indicar el valor de vida del paquete. Es el típico campo de casi cualquier paquete de datos que especifica el número máximo de encaminadores que el paquete puede dar antes de ser descartado.

Como máximo podrá ser en este caso 65536 saltos. El campo TTL puede tomar el valor del campo TTL del protocolo de red del paquete (si procede) e irse decrementando en cada salto por los encaminadores del dominio MPLS para posteriormente sustituir al valor de TTL del paquete original al salir del dominio MPLS. También se acepta que el paquete de nivel de red queda encapsulado en un paquete MPLS y el TTL de uno no tiene que ver con el TTL del otro.

S (Stack Bottom): cuando está a 1 indica que esta cabecera MPLS es la última que hay antes de encontrarse con la redundancia de red. Si esta a 0, indica que tras esta cabecera MPLS se encuentra otra cabecera MPLS y no la cabecera de red.

EXP (Experimental): estos bits están reservados para el uso experimental al nivel de clase de servicio (CoS). Sin embargo veremos que se han redefinido para albergar información sobre calidad de servicio del paquete.

LABEL: es la etiqueta MPLS, la que da nombre al protocolo. Cuando un paquete ingresa en un dominio MPLS se le asigna una etiqueta que marcará el resto de su viaje a través de la red MPLS, contiene el valor actual o real para la etiqueta.

2.2.5 Funcionamiento

Una red MPLS consiste de un conjunto de Enrutadores de Conmutación de Etiquetas (*LSR*) que tienen la capacidad de conmutar y rutear paquetes en base a la etiqueta que se ha añadido a cada paquete. Cada etiqueta define un flujo de paquetes entre dos puntos finales. Cada flujo es diferente y es llamado

Clase de Equivalencia de Reenvío (*FEC*), así como también cada flujo tiene un camino específico a través de los LSR de la red, es por eso que se dice que la tecnología MPLS es "orientada a conexión". Cada FEC, además de la ruta de los paquetes contiene una serie de caracteres que define los requerimientos de QoS del flujo. Los routers de la red MPLS no necesitan examinar ni procesar el encabezado IP, solo es necesario reenviar cada paquete dependiendo el valor de su etiqueta. Esta es una de las ventajas que tienen los routers MPLS sobre los routers IP, en donde el proceso de reenvío es más complejo.

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

Diagrama de Operación MPLS

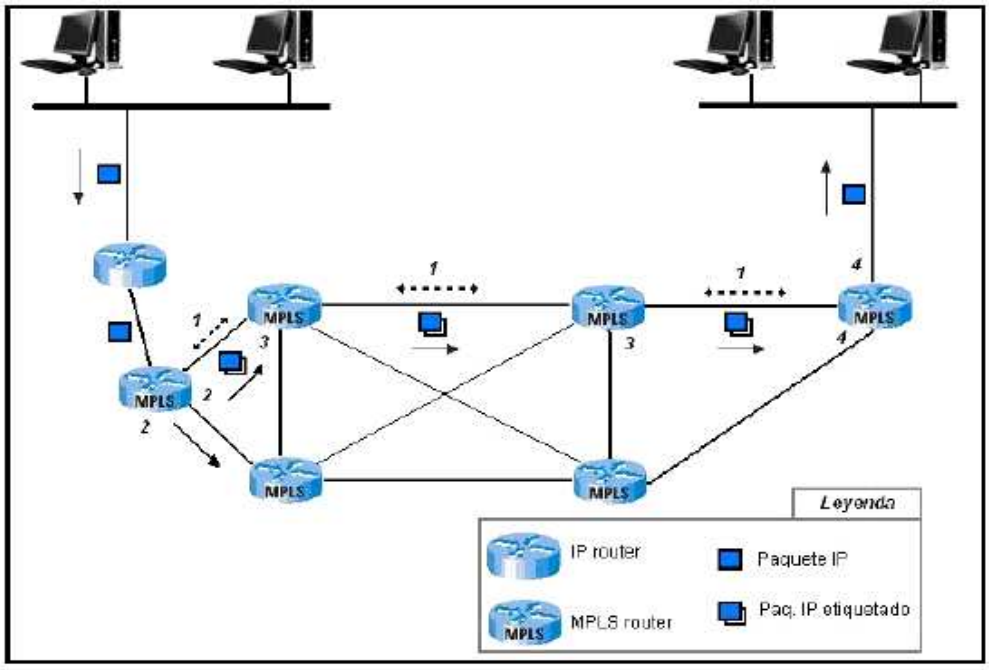


Gráfico II.10 Diagrama de operación MPLS.

El **Gráfico II.10** indica el modo de funcionamiento de MPLS, como se detalla a continuación:

1. Antes de mandar la información por el flujo es necesario establecer un Camino de Conmutación de Etiquetas (*LSP*) entre los routers que van a transmitir la FEC. Dichos LSP

sirven como túneles de transporte a lo largo de la red MPLS e incluyen los parámetros QoS específicos del flujo. Estos parámetros sirven para determinar dos cosas:

a. La cantidad de recursos a reservar al LSP.

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

Para lograr los puntos anteriores se utilizan dos protocolos para intercambiar información entre los routers de la red. Se le asignan etiquetas a cada flujo FEC particular para evitar el uso de etiquetas globales que dificultan el manejo y la cantidad de las mismas. Por esta razón las etiquetas solo hacen referencia al flujo específico. La asignación de nombres y rutas se puede realizar manualmente o bien se puede utilizar el Protocolo de Distribución de Etiquetas (*LDP*).

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

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

a. Se desecha la etiqueta de entrada y se le añade la nueva etiqueta de salida al paquete.

b. Se envía el paquete al siguiente LSR dentro del LSP.

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

2.2.6 Ventajas MPLS sobre otras arquitecturas

- MPLS es un esquema de reenvío que es independiente tanto de la tecnología de nivel de red que esté sobre él, como de la de enlace que esté por debajo. Esto posibilita que se puedan aprovechar las tecnologías existentes mientras se emigra a otras más modernas, facilitando así la recuperación de las inversiones en infraestructura de red.

- Es una tecnología escalable. Debido a la estructura de la pila de etiquetas MPLS es fácil construir jerarquías de dominios MPLS por lo que se puede pasar de ámbitos más reducidos a ámbitos más globales de forma casi transparente.

- Permite aplicar técnicas de ingeniería de tráfico con lo que la red deja de ser un simple elemento físico de transporte de información y se vuelve mucho más versátil.

- Permite usar cualquier protocolo de distribución de etiquetas tradicional o de última generación.

- Permite usar cualquier protocolo de encaminamiento tradicional o de última generación.

- Soporta el modelo de servicios diferenciados del IETF.

- Es orientado a la conexión por que los paquetes llegan en orden desde el origen del dominio MPLS hasta el destino.

- No encapsula las tramas de red sino que les coloca una etiqueta, dejándolas con el mismo tamaño y propiedades que como le llegaron.

- Proporciona una conmutación basada en etiquetas que es muy rápida y eficiente.

- Realiza una única clasificación de los paquetes entrantes al dominio MPLS por lo que este proceso reduce enormemente con respecto a tecnologías como IP.
- Proporciona un mecanismo eficiente para la realización de túneles. Los caminos LSP pueden ser usados como tales por lo que el proceso es bastante sencillo cuando se entiende ya MPLS.
- Ofrece caminos virtuales con calidad de servicio y ancho de banda asegurados si se usan los protocolos de enrutamiento y señalización de etiquetas convenientes.

2.3 Aspectos Generales de OSPF

En este apartado se especifica de manera más detallada la forma que trabaja el protocolo OSPF y sus ventajas al momento de usarlo.

2.3.1 Introducción

Open Short Path First versión 2, es un protocolo de routing interno basado en el estado del enlace o algoritmo Short Path First, estándar de Internet, que ha sido desarrollado por un grupo de trabajo del Internet Engineering task Force, cuya especificación viene recogida en el RFC 2328.

OSPF, ha sido pensado para el entorno de Internet y su pila de protocolos TCP/IP, como un protocolo de routing interno, es decir, que distribuye información entre routers que pertenecen al mismo Sistema Autónomo.

OSPF es la respuesta de IAB a través del IETF, ante la necesidad de crear un protocolo de routing interno que cubriera las necesidades en Internet de routing interno que el protocolo RIP versión 1 ponía de manifiesto:

- Lenta respuesta a los cambios que se producían en la topología de la red.
- Poco bagaje en las métricas utilizadas para medir la distancia entre nodos.
- Imposibilidad de repartir el tráfico entre dos nodos por varios caminos si estos existían por la creación de bucles que saturaban la red.
- Imposibilidad de discernir diferentes tipos de servicios.
- Imposibilidad de discernir entre host, routers, diferentes tipos de redes dentro de un mismo Sistema Autónomo.

Algunos de estos puntos han sido resueltos por RIP versión 2 que cuenta con un mayor número de métricas así como soporta CIRD, routing por subnet y transmisión multicast.

Pero el desarrollo de OSPF por parte del IETF se basa fundamentalmente en la introducción de una algoritmia diferente de la utilizada hasta el momento en los protocolos estándar de routing interno en TCP/IP para el cálculo del camino mínimo entre dos nodos de una red:

Algoritmo de Dijkstra

El algoritmo puede ser descrito como:

N= conjunto de nodos en la red.

S = nodo origen.

M = conjunto de nodos incorporados en un instante t por el algoritmo.

D ij = el coste del enlace del nodo i al nodo j. Teniendo en cuenta que:

Dii = 0;

Dij = infinito si los dos nodos no están conectados directamente.

Dn = coste del camino de coste mínimo desde un nodo s hacia un nodo n que es conocido por el algoritmo.

El algoritmo tiene tres pasos; los pasos 2 y 3 son repetidos hasta que M = N, es decir, se han calculado todos los caminos posibles con todos los nodos de la red.

1.- Inicializar:

M = {s}

Dn = dsn para n<>s

2.- Encontrar el nodo vecino que no está en M tal que

Dw = min DjDw = min Dj

Y j no pertenece a M.

Añadir w a M.

3.- Actualizar el camino de coste mínimo:

Dn = min [Dn, Dw + dwn] para todo n no perteneciente a M.

Si el último término es el mínimo, el camino desde s hasta n es ahora el camino desde s hasta w concatenado con el enlace desde w hasta n.

2.3.2 Características

Las principales características son:

- **Respuesta rápida y sin bucles ante cambios**

La algoritmia SPF sobre la que se basa OSPF permite con la tecnología actual que existe en los nodos un tiempo de respuesta en cuanto tiempo de computación para el cálculo del mapa local de la red mucho más rápido que dicho calculo en el protocolo RIP. Además como todos los nodos de la red calculan el mapa de manera idéntica y poseen el mismo mapa se genera sin bucles ni nodos que se encuentren contando en infinito; principal problema sufrido por los protocolos basados en la algoritmia de vector distancia como RIP.

- **Seguridad ante los cambios**

Para que el algoritmo de routing funcione adecuadamente debe existir una copia idéntica de la topología de la red en cada nodo de esta. Existen diversos fallos que pueden ocurrir en la red como fallos de los protocolos de sincronización o inundación, errores de memoria, introducción de información errónea.

El protocolo OSPF especifica que todos los intercambios entre routers deben ser autentificados. El OSPF permite una variedad de esquemas de autentificación y también permite seleccionar un esquema para un área diferente al esquema de otra área. La idea detrás de la autentificación es garantizar que sólo los routers confiables difundan información de routing.

- **Soporte de múltiples métricas**

La tecnología actual hace que sea posible soportar varias métricas en paralelo.

Evaluando el camino entre dos nodos en base a diferentes métricas es tener distintos mejores caminos según la métrica utilizada en cada caso, pero surge la duda de cuál es el mejor. Esta elección se realizara en base a los requisitos que existan en la comunicación.

Diferentes métricas utilizadas pueden ser:

- Mayor rendimiento
- Menor retardo
- Menor coste

- **Mayor fiabilidad**

La posibilidad de utilizar varias métricas para el cálculo de una ruta, implica que OSPF provea de un mecanismo para que una vez elegida una métrica en un paquete para realizar su routing esta sea la misma siempre para ese paquete, esta característica dota a OSPF de un routing de servicio de tipo en base a la métrica.

- **Balanceado de carga en múltiples caminos**

OSPF permite el balanceado de carga entre los nodos que exista más de un camino. Para realizar este balanceo aplica:

- Una versión de SPF con una modificación que impide la creación de bucles parciales.
- Un algoritmo que permite calcular la cantidad de tráfico que debe ser enviado por cada camino.

- **Escalabilidad en el crecimiento de rutas externas.**

El continuo crecimiento de Internet es debido a que cada vez son más los sistemas autónomos que se conectan entre sí a través de routers externos. Además de tener en cuenta la posibilidad de acceder al exterior del sistema autónomo a través de un determinado router externo u otro se debe tener en cuenta que se tiene varios proveedores de servicios y es más versátil elegir en cada momento el router exterior y servicio requerido que establecer una ruta y servicio por defecto cuando se trata de routing externo como se tenía hasta ahora.

OSPF soluciona este problema permitiendo tener en la base de datos del mapa local los denominados “gateway link state records”. Estos registros nos permiten almacenar el valor de las métricas calculadas y hacen más fácil el cálculo de la ruta óptima para el exterior. Por cada entrada externa existirá una nueva entrada de tipo “gateway link state records” en la base de datos, es decir, la base de datos crecerá linealmente con el número de entradas externas tal como ocurre con los protocolos de vector distancia, pero el coste del cálculo de las rutas crecerá en función de N*log*N para OSPF y no en función de N^2 como ocurre en los protocolos de vector distancia.

2.3.3 Mensajes OSPF

Existen cinco tipos de mensajes del protocolo OSPF:

- ***HELLO*** o Saludo se usa para:

  Identificar a los vecinos, para crear una base de datos en mapa local.

  Enviar señales de <estoy vivo>, al resto de routers para mantener el mapa local

  Elegir un router designado para una red multienvío

  Encontrar al router designado existente.

  Enviar señales de <estoy vivo>

- ***Database Description Packets*** o Descripción de la base de datos se usa para:

  Intercambiar información para que un router pueda descubrir los datos que le faltan durante la fase de inicialización o sincronización cuando dos nodos han establecido una conectividad.

  Link State Request o Petición del estado del enlace se usa para pedir datos que un router se ha dado cuenta que le faltan en su base de datos o que están obsoletos durante la fase de intercambio de información entre dos routers.

  Link State Request o Actualización del estado del enlace se usa como respuesta a los mensajes de Petición de estado del enlace y también para informar dinámicamente de los cambios en la topología de la red. El emisor retransmitirá hasta que se confirme con un mensaje de ACK.

Link State ACK o ACK del estado del enlace se usa para confirmar la recepción de una Actualización del estado del enlace.

2.3.4 Funcionamiento

El fundamento principal en el cual se basa un protocolo de estado de enlace es en la existencia de un mapa de la red el cual es poseído por todos los nodos y que regularmente es actualizado.

Para llevar a cabo este propósito la red debe de ser capaz de entre otros objetivos de:

Almacenar en cada nodo el mapa de la red.

Ante cualquier cambio en la estructura de la red actuar rápidamente, con seguridad si crear bucles y teniendo en cuenta posibles particiones o uniones de la red.

Mapa de Red Local

La creación del mapa de red local en cada router de la red se realiza a través de una tabla donde:

Fila: representa a un router de la red; y cualquier cambio que le ocurra a ese router será reflejado en este registro de la tabla a través de los registros de descripción.

Columna: representa los atributos de un router que son almacenados para cada nodo. Entre los principales atributos por nodo tenemos: un identificador de interfase, el número de enlace e información acerca del estado del enlace, o sea, el destino y la distancia o métrica.

Con esta información en todos los router de la red el objetivo es que cada router sea capaz de crear su propio mapa de la red, que sean todos idénticos lo cual implicará que no se produzcan bucles y que la creación de este mapa de red local se realiza en los router lo más rápido posible.

Ejemplo

A --- 1 --- B --- 2 --- C --- 4 --- D --- 3 --- A

DE	A	ENLACE	DISTANCIA
A	B	1	1
B	C	2	1
C	D	4	1
D	A	3	1
B	A	1	1
C	B	2	1
D	C	4	1
A	D	3	1

Los routers envían periódicamente mensajes HELLO para que el resto de routers, tanto si pertenecen al mapa local como a un circuito virtual para sepan que están activos.

Para que un router sepa que sus mensajes se están escuchando los mensajes HELLO incluyen una lista de todos los identificadores de los vecinos cuyos saludos ha oído el emisor.

Protocolo de Chequeo de Mapas: Bringing Up Adjacencies

Se basa en la existencia de que existen identificadores de enlace y número de versiones, a partir de estos OSPF forma unos paquetes de descripción del mapa local e inicializa un proceso de sincronización entre un par de routers de la red que tiene dos fases:

Intercambio de paquetes de descripción del mapa local entre los nodos y en cada nodo creación de una lista de nodos especiales a tener en cuenta o bien porque su número de

versión es mayor que la copia local o bien porque no existía en ese mapa local el identificador del enlace.

Creación en cada nodo de paquetes con información acerca de esos nodos especiales que se envían a sus vecinos para que corroboren la información.

Tras terminar este intercambio de información, ambos routers conocen:

- Nodos que son obsoletos en su mapa local.
- Nodos que no existían en su mapa local.

Los mensajes que se usan para solicitar todas las entradas que necesiten actualización son los Link State Request o mensajes de petición de estado de enlace.

Los mensajes de respuesta son los Link State Update.

2.3.5 Ventaja de OSPF

Una de las grandes ventajas de OSPF es que este ha sido diseñado para adaptarse al máximo a los protocolos TCP/IP.

Redes Locales

La existencia de redes locales formadas por host que se conectaban a un router para acceder al exterior era un hecho patente cuando se creó OSPF y siguiendo el procedimiento explicado anteriormente cada nodo hubiese tenido que especificar su enlace con el router.

OSPF introduce un nuevo enlace el “link to a stub network” que es una variante del “router link” que basándose en el concepto de subred del modelo IP permite asignar a la red local un número de subred y especificar solamente un enlace entre el router y la subred.

El enlace hacia un vecino es identificado por la dirección IP de su vecino y el enlace hacia la red local es identificado por su red o número de subred.

Redes Broadcast

OSPF da soporte a los servicios broadcast para ello implementa un mecanismo que simula el funcionamiento broadcast que se basa en la elección de un router como maestro a través del cual se pasaran todas las comunicaciones entre dos routers, es decir se establece el “designated router” y se crea un “virtual node”.

Para realizar el mapa local cada router tendrá dos enlaces:

Un enlace de él hacia su propia red broadcast cuyo enlace conocerá el propio router.
Un enlace de él hacia el “virtual node”, que será identificado por el router designado o”designated router”

La presencia del “designated router” es la de simplificar el procedimiento broadcast, ya que cuando un router quiere enviar un mensaje envía un mensaje al “designated router” usando la dirección multicast “all-designated router” (224.0.0.6).Si es un nuevo mensaje el “designated router” lo reenvia a la red usando la dirección multicast “all-OSPF-routers” (224.0.0.5).

Si el “designated router” tiene problemas de funcionamiento todo este procedimiento fallará, por ello cuando se elige al “designated router” OSPF también elige al mismo tiempo al“backup designated router” con el cual también mantienen enlaces virtuales todos los routers, que en caso de fallo asumirá el rol de router designado y otro router será elegido como backup.

El router de backup permanece siempre en escucha de todos los mensajes cuya dirección multicast es “all-designated-router” a la espera del fallo del “designated router”, que es detectado por el protocolo HELLO del OSPF.

Redes No Broadcast

En la documentación de OSPF este tipo de redes son aquellas que ofrecen conectividad entre todos sus miembros pero no permiten un servicio broadcast o multicast como pueden ser redes “frame-relay o”ATM”.

OSPF trata este tipo de redes con un mecanismo parecido al explicado en redes broadcast, eligiendo al “designated router” y al “backup router”, pero estableciendo los circuitos virtuales entre routers solo bajo demanda.

En estas redes los mensajes son enviados punto a punto, del “designated router” a cada uno de los routers. De igual modo cuando un router envía un mensaje al “designated router” lo envía también al “backup designated”.

Routing Jerárquico

El routing jerarquico surge de la necesidad de resolver el problema debido al aumento del tamaño de las redes que implica un mayor coste en calculo de rutas, tiempo de transmisión de datos, memoria.

OSPF establece una jerarquía en la red y la parte en “áreas”, existiendo un área especial denominada “backbone área”.

En un “área” se aplica el protocolo OSPF de manera independiente como si de una red aislada se tratase, es decir, los routers del área solo contiene en su mapa local la topología del área, así que el coste en calculo es proporcional al tamaño del área y no de la totalidad de la red.

Cada área incluye un conjunto de subredes IP. La comunicación entre routers de un área se resuelve directamente a través del mapa local de área que cada router posee.

Estas áreas se conectan entre sí a través del “backbone área”, mediante routers que pertenecen normalmente a una “área” y al “backbone area”. Estos routers se denominan “area-border routers” y como mínimo existe uno entre un área y el backbone.

Los “area-border routers” mantienen varios mapas locales de estado de enlaces, uno por cada área a las cuales pertenecen. Estos emiten unos registros de estados de enlaces para anunciar que conjunto de subredes IP son accesibles a través de ellos.

Cuando un router de un área quiere intercambiar tráfico con un router de otra área, estos deben realizarlo a través de los “area-border routers”. Estas se denominan “inward routes”.

Existe otro tipo de router el que realiza el intercambio de tráfico con routers de otros sistemas autónomos. La información almacenada en cada router externo es idéntica para cada una de ellos

La sumarización de registros representa los enlaces entre un “area-border router” y una red en el “backbone area” o en otra área. La métrica utilizada es la longitud del camino entre el “area-border router” y la red. Este mecanismo va a permitir que diferentes “area-border router” establezcan para un destino diferentes caminos, según el resultado de su métrica pero con la salvedad de que no producirán bucles, debido a que la estricta jerarquía de OSPF solo permite que se conecten áreas a través del backbone.

OSPF provee en su jerarquía de routing la posibilidad de que un área se divida en dos a causa de algún fallo en los enlaces o en los routers pero siempre se quedan los fragmentos conectados directamente al “backbone area” a través de dos condiciones:

Los “area-border router” guardan los enlaces de las redes y subredes que son alcanzables por ese router en un momento determinado. El “backbone area” se guarde información de las redes que componen cada área aunque no de su topología.

El mecanismo OSPF para solucionar el caso de una partición del “area backbone” está un poco sujeto a por donde se realiza está partición ya que este podrá ser cubierto siempre y cuando existan “area-border router” que sean capaces de establecer caminos virtuales por dentro de sus áreas para establecer nuevos caminos de intercambio de información.

Estos describirán enlaces virtuales que deben ser almacenados en la base de registros del “area backbone”.

La métrica del enlace virtual será calculada teniendo en cuenta el coste de los enlaces reales por los que pasa el enlace virtual en el área local donde se realiza el enlace virtual.

A partir de este enlace virtual deben ser sincronizados y actualizados todos los routers del “area backbone”.

Stub Areas:

El problema del incremento de rutas externas que debían ser sumarizadas en multitud de áreas pequeñas ha quedado resuelto con la introducción del concepto de “stub area” un área donde todas las rutas externas son sumarizadas por una ruta por defecto.

Una stub area funciona exactamente igual que un área normal de OSPF con unas cuantas restricciones, acerca de prohibir la entrada de rutas externas en las bases de datos de los routers.

Una stub área puede estar conectada por más de un “area-border router”all backbone, pero no se podrá elegir para salir del área el router, ni configurar un enlace virtual sobre una stub área.

También no se podrá conectar un “border route” con una “stub area”. Esto es lógico si nosotros consideramos que los “border routers” conectan los sistemas autónomos con Internet y normalmente deberían estar sujetos a la “backbone area”

2.4 Calidad de Servicio (QoS)

El multiprotocolo de conmutación de etiquetas (MPLS) reduce significativamente el procesamiento de paquetes que se requiere cada vez que un paquete ingresa a un enrutador en la red, esto mejora el desempeño de dichos dispositivos y del desempeño de la red en general. Dicho protocolo se puede considerar en desarrollo constante ya que en los últimos años la demanda de esta tecnología ha ido creciendo. Las capacidades más relevantes de dicho protocolo son cuatro: Soporte de Calidad sobre servicio (QoS),

Ingeniería de tráfico, soporte para Redes Privadas Virtuales (VPNs) y soporte multiprotocolo.

La implantación de calidad de servicio (QoS) en redes IP es esencial para el éxito de aplicaciones avanzadas, como telemedicina, videoconferencia y VoIP (voz sobre IP o telefonía sobre IP). Estas aplicaciones demandan, además de gran ancho de banda, un servicio diferenciado. En muchos casos es necesario garantizar que la transmisión de los datos sea realizada sin interrupción o pérdida de paquetes

Normalmente las redes trabajan con la filosofía del mejor esfuerzo: cada usuario comparte ancho de banda con otros y por lo tanto, la transmisión de sus datos corriente con las transmisiones de sus datos importantes concurre con las transmisiones de los demás usuarios. Los datos empaquetados son encaminados de la mejor forma posible, conforme las rutas y bandas disponibles. Cuando hay congestionamiento, los paquetes son descartados sin diferenciación de la aplicación a la que corresponde, por lo tanto no hay garantía que el servicio sea realizado con éxito. Entretanto, aplicaciones como voz sobre y videoconferencia necesitan de tales garantías.

Con la implantación de calidad de servicio (QoS), es posible ofrecer mayor garantía y seguridad para las aplicaciones avanzadas, una vez que el tráfico de estas aplicaciones pasa a tener prioridad en relación con aplicaciones tradicionales.

Con el uso del QoS los paquetes son marcados para distinguir los tipos de servicios y los enrutadores son configurados para crear filas distintas para cada aplicación, de acuerdo

con las prioridades de las mismas. Así, una faja de ancho de banda, dentro del canal de comunicación, es reservada para que, en el caso de congestionamiento, determinados tipos de flujos de datos o aplicaciones tengan prioridad en la entrega.

Existen dos modelos de implementación de QoS: servicios integrados (IntServ) y servicios diferenciados (DiffServ). InterServ es basado en reserva de recursos, en cuanto DiffServ es una propuesta en la cual los paquetes son marcados de acuerdo con las clases de servicios predeterminadas.

2.4.1 Servicios integrados (IntServ)

La arquitectura de Servicios Integrados (IntServ) o RFC 1633 se ocupa de administrar el ancho de banda durante la congestión de la red. Permite ampliar la arquitectura IP existente para soportar sesiones en tiempo real, manteniendo el servicio de mejor esfuerzo existente. La idea de IntServ es pretender implementar calidad de servicio realizando la clasificación del tráfico, asignación de prioridades y una reserva de recursos mediante un protocolo de señalización.

IntServ utiliza para administrar la congestión un conjunto de mecanismos de control de tráfico subyacentes. Un control de admisión, ejecutado por un protocolo de reserva, es capaz de poder comprobar si es viable la petición y determinar si se dispone de recursos para ofrecer la QoS a un flujo. IntServ no define ningún método de control a utilizar pero normalmente se relaciona con el RSVP (RFC2205).

El mecanismo de encaminamiento, encargado de proporcionar la información del siguiente router para cada dirección destino.

El clasificador de paquetes, el cual analiza los campos de direcciones y puertos para determinar el flujo al que pertenece el paquete. El algoritmo de encolado gestiona la transmisión de los paquetes por un enlace de salida dentro de un router. Una norma de descarte, que proporciona un mecanismo uniforme que indica las condiciones bajo las cuales se descartan los paquetes.

IntServ ofrecen tres tipos de servicios: garantizados, de carga controlada y del mejor esfuerzo. Los dos primeros emulan a los circuitos dedicados, garantizando los parámetros de la especificación del tráfico del emisor. El tercero suministra mejor esfuerzo que el mejor esfuerzo de IP.

La forma de garantizar estos servicios se centra en el protocolo RSVP, ya que hace posible la asignación de recursos (ancho de banda, fluctuación de fase, ráfaga máxima, etc.) a través de una red IP. RSVP representa un protocolo de señalización el cual está dirigido a sistemas terminales y especialmente al sistema terminal receptor. La razón es que cuando un emisor transmite un mensaje llamado Path (Trayecto) para solicitar recursos a los sistemas terminales receptores. La ruta que deben seguir estos mensajes es la misma que siguen los datos de usuario; determinada por el protocolo de enrutamiento, de lo contrario para nada serviría RSVP.

Cuando el receptor (o receptores) recibe el mensaje Path, esté envía el mensaje Resv (reserva) como respuesta a los mensajes PATH, y solicitan a la red (a los routeres RSVP) las correspondientes reservas de recursos para soportar la comunicación con cierta QoS, fluyendo hasta la fuente datos del usuario emisor. Las reservas de recursos no son permanentes y deben ser refrescadas periódicamente con mensajes PATH y RESV. A todo ello, el mensaje Resv es realmente el que realiza la solicitud de recursos a los dispositivos intermedios entre extremo a extremo.

2.4.2 Servicios diferenciados (DiffServ)

Los servicios diferenciados (DiffServ) o RFC 3289, es una forma de ofrecer diferentes servicios a flujos de tráfico distintos. Es una manera sencilla y tosca de clasificar los servicios de las aplicaciones. Sin embargo, es una solución escalable, más apropiada para grandes entornos como Internet. Se basa en marcar los paquetes IP y la red (los routeres) los tratará en base a esa marca. Define y utiliza diferentes tipos de routers. Esta diferenciación depende de si se trata de un nodo interior o un nodo frontera.

El marcado del tráfico lo realizan los routeres de frontera, aunque también los sistemas terminales pueden realizarlo. La versión IPv6 contempla este marcado de paquetes, mediante el campo DS (campo de servicio diferenciado) de la cabecera IP. IPv4 permite marcar paquetes, a través del byte ToS (Tipo de Servicio) y en tal caso se utiliza este como byte DS

2.4.2.1 El campo DiffServ (DS*)*

El código de *DiffServ* (DSCP) tiene 7 bits, lo que le permite disponer de 64 clases de servicio, reemplazando el campo obsoleto de TOS de la cabecera IP como se indica seguidamente en el **Gráfico II.11**.

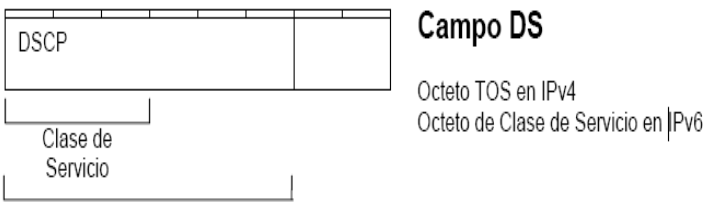


Gráfico II.11 Punto de código de Diffserv.

Per Hop Behaviour

El PHB es una descripción de las clases de servicios asociados a la codificación de *DiffServ.* Sobre esta descripción aparecen diferentes aplicaciones de políticas de clases para la transmisión de paquetes.

Conforme con la descripción PHB se proponen algunas clases de servicios propios de *DiffServ*:

• BE (*Best Effort*). Servicio sin requerimientos de ningún SLA.

• EF (*Expedited Forwarding*). Esta clase de servicio acoge al tráfico con mayor prioridad. La información de gestión y las transmisiones de voz/video se suelen clasificar como EF.

• AF*xy* (*Assured Forwarding*). Dentro de este grupo se acogen varios tipos de tráfico. Su clasificación depende de los requerimientos de los SLA a los que estén ligados.

En la aplicación de QoS con ¨Diffserf, es necesario configurar las siguientes técnicas de QoS:

• Clasificación y Marcado

• Shaping y policing

• Técnicas de Encolamiento

• Call admisión Control

Clasificación y Marcado

Como se mencionó anteriormente, es necesario proporcionar los recursos necesarios a las aplicaciones críticas. La idea de separar el tráfico se llama DiffServ, y consiste en un proceso de dos Partes:

1. Detectar el Tráfico de Interés
2. Marcar el Tráfico de Interés

Para marcar el tráfico, se debe analizar en detalle la estructura del paquete IP. Al interior del mismo existe el campo llamado Type of Service (ToS). Este campo consta de un Byte, leídos de izquierda a derecha. La utilización de los bits es hecha en base a dos técnicas.

IP Precedence: se utilizan los tres primeros bits
DSCP (Differenciated Service Code Point): se utilizan los seis primeros bits

Por tanto, al momento de establecer o distinguir el tráfico de interés, se procede a colocar una marca en el campo ToS del paquete IP asociada al nivel de importancia que le merece.

Otra forma de marcar tráfico, es a nivel de Ethernet, al interior del mismo, existe el campo TAG y dentro de él otro denominado “Class Of Service” (COS).

El subcampo COS consta de tres bits, leídos de Izquierda a derecha. La utilización de estos bits es hecha de manera similar a lo que es TOS.

Detección del Tráfico de Interés

Para la detección del tráfico de interés, se recomienda hacerlo en el router que limita con la red WAN. El policing es para limitar la tasa de tráfico al ingreso del router, provocando retransmisiones a nivel de TCP, mientras que el shaping limita la tasa de tráfico a la salida con buffering (delay, drop).

Técnicas de Encolamiento

En el normal de los casos, es decir sin congestión, los equipos despacharán los paquetes hacia la red según orden de llegada, lo que se conoce como FIFO (First Input First Output). En el caso de experimentar congestión el router debe almacenar temporalmente los paquetes en buffer, para luego despacharlos según los criterios establecidos por el tipo de encolamiento empleado.

La técnica de encolamiento WFQ (weighted Fair Queuing), es una técnica de priorización dinámica, ya que la información a su llegada al router es clasificada según: dirección IP (fuente/destino), Puerto (fuente/destino), Ip precedence, posteriormente se le asigna un peso relativo de acuerdo a cada clasificación. Finalmente el router despachará primero aquellos paquetes de los flujos que tengan un peso relativo más importante.

La técnica de encolamiento CBWFQ (Class Based Weighted Fair Queuing), es cuando la información es clasificada por dirección IP (fuente/destino), Puerto

(fuente/destino), Ip precedence. El tráfico es separado en tantos grupos como aplicaciones existan y cada grupo puede recibir una porción de ancho de banda asignada arbitrariamente.

2.4.2.2 Funcionamiento del DiffServ

El funcionamiento de DiffServ se basa en clasificar los datos a la entrada de la red con relación a un determinado servicio (ver **Gráfico II.12**), después se aplica el proceso de preparación del tráfico. La clasificación a la entrada en la red está basada en el análisis de uno o varios campos de la cabecera del paquete.

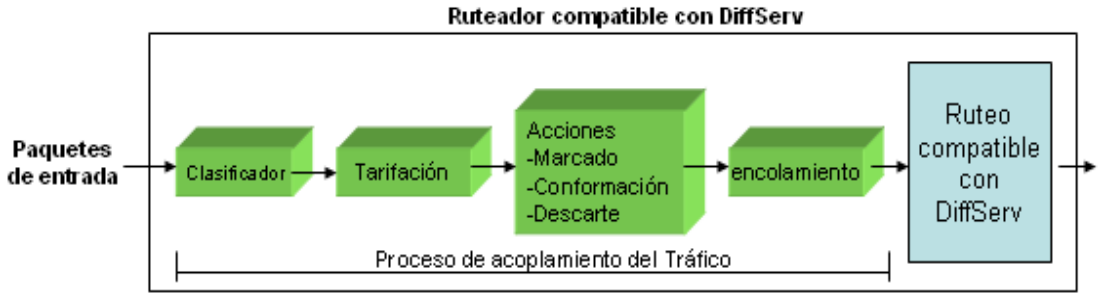


Gráfico II.12 Proceso de entrada a un nodo externo de Servicios Diferenciados.

Después el paquete se marca, como perteneciente a una determinada clase de servicio. Los enrutamientos centrales sólo examinan el campo donde se marcó el paquete y le dan el tratamiento correspondiente a esa clase de servicio. Finalmente, antes de salir de la red se suprime la marca.

Se han definido dos tipos de servicio de DiffServ con garantía de QoS: Reenvío Rápido (RR) y Reenvío Asegurado (RA). El primero equivale a una línea arrendada virtual, por lo que se garantiza cierto ancho de banda y reducida demora de cola. RA permite que los paquetes se etiqueten con 12 posibilidades, descritos por el campo DS, pues tiene 4 clases con 3 procedimientos en cada clase que determinan como descartar tráfico. Cuando hay congestión en un router los paquetes con mayor precedencia son descartados primero.

Además, la utilización de RA asume la existencia de un acuerdo entre el usuario y la red, en el nivel de servicio (NdS). El NdS define el perfil del tráfico (ancho de banda, retardo, jitter y tasa de pérdidas) y la política (tiempo de disponibilidad, penalizaciones, etc.).

Una vez se establece el NdS, se espera que el tráfico enviado por el cliente sea conformado y marcado en la entrada en la red de acuerdo con lo acordado en el NdS y cualquier tráfico no conforme no tendrá calidad de servicio.

2.4.3 El comparativo entre IntServ y DiffServ

Si bien, para garantizar la calidad de servicio en una red IP se puede utilizar ya sea IntServ o DiffServ. Se hace evidente entonces, la necesidad de tener encuentra los atributos y debilidades de cada uno de estos protocolos (ver la Tabla II.1), con la intención de emplearlos en los contextos correctos.

La descripción de estos dos protocolos de QoS (ver **Tabla II.1**) podría hacer pensar que son excluyentes, pero no es así, de hecho se complementan. En la práctica, es muy frecuente encontrar muchas posibles combinaciones entre estas dos arquitecturas y más aún, pueden combinarse con otras tecnologías para dar soporte a la QoS extremo a extremo.

Aparte de estos dos protocolos, también existe la conmutación de etiquetas multiprotocolo (MPLS) que es similar a DiffServ en algunos aspectos, dentro de sus múltiples funcionalidades, realiza la ingeniería de tráfico, el control del ancho de banda y la priorización de aplicaciones.

Servicios Integrados (IntServ)	**Servicios Diferenciados (DiffServ)**
Son aplicables en redes pequeñas	Presenta un buen desempeño tanto en redes pequeñas como grandes
Funciona en el nivel 4 del modelo OSI	Trabaja en el nivel 3 del modelo OSI, el cual lo hace transparente para el usuario
Deja que los usuarios puedan realizar explícitamente peticiones de QoS	Tiene solo 12 posibilidades de servicios.
Permite solicitudes de calidad de servicio con gran granularidad	Los tipos de servicio son permanentes
Necesita periódicamente refrendar el tipo de servicio	Los recursos son asignados en el router de frontera.
Utilizan un protocolo de reserva para designar recursos	Los nodos internos procesan los paquetes de acuerdo al campo DS
Posee un mecanismo más complejo y exigente.	Tiene una forma sencilla de clasificar y priorizar el tráfico.

Tabla II.1 Tabla comparativa entre las dos principales arquitecturas de QoS

2.4.4 MPLS QoS

Las nuevas aplicaciones que han ido surgiendo en los últimos años requieren más de lo que la actual tecnología IP puede proporcionar: altos requerimientos de ancho de banda, necesidad de transmisión con bajo retardo o sin pérdidas, etc. Para responder a estos requerimientos se han desarrollado varias formas de dotar a las redes IP de QoS.

Una de las propuestas más importantes es DiffServ y otra tecnología es MPLS, que aunque por sí misma no proporcione QoS, es muy útil para realizar Ingeniería de Tráfico.

Tal y como se argumentará posteriormente, una confluencia de estos dos modelos es una buena línea para mejorar las redes IP, puesto que MPLS actúa al nivel de enlace-red proporcionando un método de envío rápido por su conmutación de etiquetas y sus caminos LSP (Label Switched Path); y DiffServ realiza la diferenciación y priorización del tráfico necesaria para dotar a IP de QoS.

Este es el marco en el que se desarrolla nuestro trabajo, realizando un estudio que permita obtener una mejora de la red mediante la integración de los dos modelos citados (MPLS y DiffServ). Con ello se persigue, por un lado, conseguir que las redes IP permitan al usuario disponer de calidad de servicio, sin necesidad de migrar a otras tecnologías como ATM (Asynchronuos Transfer Mode), sin que se interrumpa el funcionamiento actual en la red y con el menor perjuicio posible para los usuarios.

Además, mediante la integración de los modelos MPLS y DiffServ obtenemos una arquitectura en la que MPLS se sitúa en el nivel de red-enlace, y sirve para evitar la congestión de la red, aportando sus características de ingeniería de tráfico. Mientras, DiffServ asegura unos ciertos parámetros de calidad de servicio realizando una distinción y priorización del tráfico. Por último, la incorporación a esta arquitectura de un elemento gestor del dominio aportará ventajas como ingeniería de tráfico, optimización de recursos y control del uso de los recursos.

La utilización de MPLS para aplicar ingeniería de tráfico promete proporcionar QoS mientras se optimizan los recursos de la red. Sin embargo, MPLS por sí solo no puede proporcionar diferenciación de tráfico, siendo este requisito imprescindible para la provisión de garantías QoS. Por ello, puede complementarse con DiffServ para aplicar esta diferenciación.

MPLS DiffServ

Dos métodos son posibles:

- Usando los bits del campo EXP en la cabecera MPLS y mapeando DSCP a EXP conveniente para la Interfaz basadas en tramas.

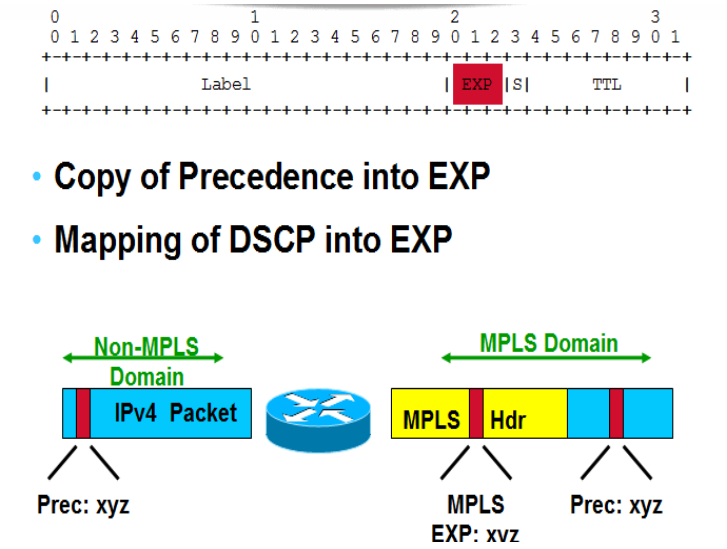


Gráfico III.13 Usando bits de Precedencia del camp DSCP en campo EXP de MPLS

- Mapeando una etiqueta por-CoS por-FEC conveniente para interfaz basada en ATM. En nuestro caso se aplicó por la asignación de las etiquetas de la cabecera MPLS y dando priorización de las Clases de Servicio.

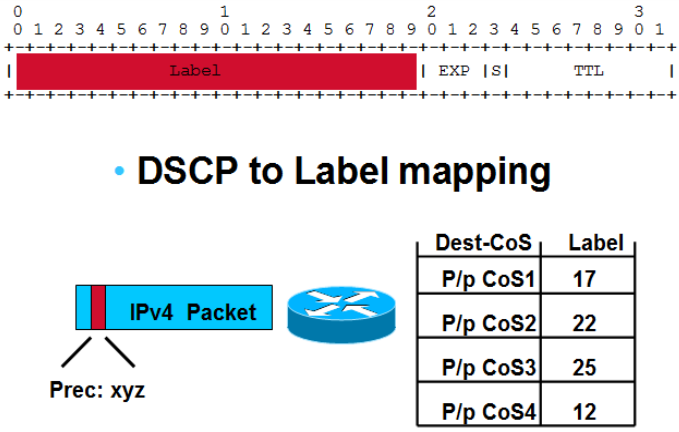


Gráfico III.14 Usando Labels de la cabecera MPLS para mapeo de CoS

2.4.5 Generación de pérdidas, retardos y jitter

Las pérdidas tienen dos causas fundamentales: los errores de transmisión, debido por ejemplo al ruido en el canal de comunicación y las pérdidas de paquetes en los buffer.

Con la tecnología actual de transmisión, por ejemplo la transmisión óptica, y con algoritmos de recuperación de errores en las capas debajo de IP, las pérdidas debidas a los errores de transmisión son muy poco significativas.

La política 'best effort' implica que si existe más tráfico del que puede ser transportado por un enlace, el sobrante se envía a una cola de donde se irán sacando los paquetes para ser enviados. Si esta cola se llena, los paquetes son descartados.

En cuanto al retardo, el problema es similar. Existen tres fuentes fundamentales de retardo: el retardo de transmisión, el retardo de procesamiento en los enrutadores o switches, y el retardo de las colas de los enlaces. Los dos primeros con la tecnología existente son cada vez menos relevantes.

Por otra parte los retardos en enrutadores o switches vienen derivados fundamentalmente del procesamiento de los paquetes. Uno de los procesamientos que genera un retardo es la búsqueda en las tablas de ruteo para decidir el próximo enrutador al que debe enviarse el paquete. Hoy en día estos procesos que antes se hacían por software pueden ser hechos por hardware y a altas velocidades de procesamiento.

El jitter, en telefonía IP o voz sobre Ip es muy importante, por lo que la variación de los retardos de los paquetes debe ser siempre muy baja para no afectar las aplicaciones de telefonía sobre una red de Datos.

De lo anterior concluimos que el problema fundamental para asegurar calidad de servicio es mantener las colas 'casi vacías'. Ahora bien la pregunta es entonces ¿porqué se llenan las colas? Las colas se llenan porque la capacidad del enlace es momentáneamente menor que la cantidad de tráfico que pretende usar dicho enlace.

Una solución obvia a este problema es asegurar una capacidad tal en todos los enlaces de manera que nunca la velocidad de arribo de paquetes sea mayor que la capacidad del enlace. Pero aquí interviene nuevamente la economía. No es razonable económicamente sobredimensionar toda la red. Pero por otra parte si se realizara

2.4.6 ¿Cómo solucionar los problemas de calidad de servicio y aprovechar los recursos de la red?

Entendemos por congestión en este contexto la situación en la cual la diferencia entre la tasa de arribo de paquetes y la capacidad del enlace es de tal magnitud que no pueden ser

satisfechos los envíos de paquetes. Por lo tanto la congestión se generar porque no se tiene capacidad suficiente para transportar todo el tráfico y satisfacer sus requerimientos de calidad de servicio o porque el tráfico está mal distribuido en la red sobrecargando ciertos enlaces y dejando sub-utilizados otros.

Dentro del tráfico en muchos casos existen diferentes tipos de tráfico con diferentes requerimientos. Si se divide la capacidad de los enlaces separando el tráfico de distintas clases por diferentes 'partes' de la capacidad de cada enlace, se puede lograr cumplir con los requerimientos de QoS de cada clase. Esto se puede lograr a través de la aplicación conjunta de tres mecanismos:

- Dividir el volumen total del tráfico en clases con requerimientos diferentes.
- Aplicar mecanismos para controlar el volumen de tráfico de cada clase que ingresa la red.
- Aplicar políticas de despacho y descarte de paquetes en los enlaces de forma de dividir la capacidad total del enlace en las capacidades necesarias para cumplir los requerimientos de cada clase.

En este último enfoque, se basan modelos de QoS sobre IP como por ejemplo el modelo de Servicios Diferenciados DiffServ.

2.4.7 Soporte QoS

QoS permite a los administradores de redes el uso eficiente de los recursos de sus redes con la ventaja de garantizar que se asignaran más recursos a aplicaciones que así lo necesiten, sin arriesgar el desempeño de las demás aplicaciones. En otras palabras el uso de QoS le da al administrador un mayor control sobre su red, lo que significa menores costos y mayor satisfacción del cliente o usuario final.

¿Por qué la importancia de QoS?

En los últimos años el tráfico de redes ha aumentado considerablemente, la necesidad de transmitir cada vez más información en menos tiempo, como video y audio en tiempo real (streaming media). La solución no es solo aumentar el ancho de banda (bandwidth) cada vez más, ya que en la mayoría de los casos esto no es posible y el además es limitado. Es aquí donde la administración efectiva de recursos que provee QoS entra a relucir.

2.4.8 Beneficios principales de QoS

QoS trabaja a lo largo de la red y se encarga de asignar recursos a las aplicaciones que lo requieran, dichos recursos se refieren principalmente al ancho de banda. Para asignar estos recursos QoS se basa en prioridades, algunas aplicaciones podrán tener más prioridades que otras, sin embargo se garantiza que todas las aplicaciones tendrán los recursos necesarios para completar sus transacciones en un periodo de tiempo aceptable.

En resumen QoS otorga mayor control a los administradores sobre sus redes, mejora la interacción del usuario con el sistema y reduce costos al asignar recursos con mayor eficiencia (bandwidth). Mejora el control sobre la latencia (Latency y jitter) para asegurar

la capacidad de transmisión de voz sin interrupciones y por ultimo disminuye el porcentaje de paquetes desechados por los enrutadores: confiabilidad (Reliability).

MPLS impone un marco de trabajo orientado a conexión en un ambiente de Internet basado en IP (Internet Protocol) y facilita el uso de contratos de tráfico QoS exigentes.

2.4.9 Detalles de MPLS basado en la Arquitectura de QoS

Mediante el servicio QoS se eliminan las colas de los modem y se trasladan al enrutador de administración de ancho de banda; una vez aquí se jerarquizan y administran adecuadamente, colocando delante los paquetes aleatorios de los servicios interactivos, sin obligarlos a esperar turno detrás de los paquetes generados por el tráfico de subida y bajada de archivos. Simultáneamente se define el ancho de banda máximo del total disponible que cada servicio debe consumir.

En organizaciones grandes con oficinas remotas la priorización del tráfico WAN es crítica. Los enlaces WAN son costosos y muy limitados en ancho de banda. Muchas aplicaciones críticas como ERP, voz sobre IP, servidores remotos de aplicaciones, consultas a información crítica, etc., requieren de anchos de banda definidos y garantizados. Sin una priorización de los servicios y una repartición adecuada del ancho de banda estos servicios colapsan y los tiempos muertos o fuera de servicio son cada vez más frecuentes e interminables.

Utilizando servicios QoS el ancho de banda de la red puede ser garantizado para los servicios esenciales durante los períodos de alta congestión. Utilizando esquemas de

priorización de tráfico que se modifiquen en el tiempo se logra una mejor administración y uso de los recursos de ancho de banda limitados.

Cuando hay excesivo tráfico y congestión se priorizan los servicios esenciales y se les entrega la mayor disponibilidad del ancho de banda; luego al disminuir la carga o cuando los servicios esenciales no están en uso, el ancho de banda se retorna automáticamente al resto de los solicitadores de recursos.

Con servicios QoS las organizaciones que ofrecen servicios de "hosting" o "application server" pueden limitar el ancho de banda de los servicios ofrecidos por el servidor en una amplia gama de opciones tales como dirección de origen o destino, tipo de aplicación, puerto o protocolo de transmisión. Con la capacidad de fijar niveles fijos absolutos de ancho de banda y niveles variables que se ajustan según la disponibilidad del ancho de banda.

Mediante el control de acceso utilizando cortafuegos basados en identificación, filtrado y eliminación de paquetes se puede garantizar la seguridad de la red y servicios de acceso remotos y protegerlos contra intrusiones erradas o maliciosas

Las políticas de seguridad de tráfico pueden definirse por usuario, grupo de trabajo, hora del día, tipo de servicio, dirección de origen, dirección de destino, puerto de origen, puerto de destino, protocolo de comunicación, etc.

Mediante la traslación de espacios de direcciones es posible utilizando direcciones virtuales aislar la red interna del mundo exterior representado por Internet, pero sin

perder la ventaja de que cada estación puede estar en la red manteniendo las garantías requeridas de seguridad.

En aquellos casos en que por razones de volumen de tráfico o conexiones sea necesario aumentar la capacidad de interconexión o de servidores, sin necesidad de adquirir equipos más poderosos, sino ampliando individualmente la capacidad mediante el agregado de nuevos elementos en paralelo (cluster) es posible actuar gradualmente utilizando QoS sin perder la inversión inicial de equipos y permitiendo la escalabilidad, redundancia y disponibilidad de las instalaciones.

Frecuentemente un portal colapsa debido al incremento paulatino del tráfico y la solución no implica necesariamente adquirir un nuevo servidor más poderoso y desechar el anterior o en su defecto adquirir equipos costosísimos de balanceo. Los servicios QoS permiten ampliar la capacidad de sus instalaciones adquiriendo nuevos equipos, pero conservando los anteriores, mediante esquemas de balanceo de carga en líneas y servidores.

Adicionalmente estableciendo políticas de enrutamiento de tráfico mediante reglas estáticas basadas en el criterio humano se mejora el balanceo de la carga en horas pico permitiendo una racionalización y mejor utilización de los recursos de la red. Mediante la utilización de túneles encriptados puede entubarse el tráfico crítico enrutando directamente los paquetes IP desde los clientes a los servidores utilizados y viceversa. Los túneles permiten también que dos o más redes internas en localidades remotas puedan verse y trabajar como si fueran las misma red (VPN), utilizando a Internet como asiento del túnel o en su defecto líneas muertas de comunicación entre las localidades.

CAPÍTULO III

MARCO PROPOSITIVO

3.1 Introducción

En el presente capítulo, se describe la funcionalidad de la herramienta seleccionada y utilizada para el desarrollo de la parte aplicativa, se establece a demás los escenarios sobre los cuales se desarrollan las configuraciones e implementación de OSPF sin MPLS y el segundo de OSPF con MPLS.

Se detalla de manera técnica la forma de instalación del Sistema Operativo RouterOS, sus características y configuración a través de modo gráfico y mediante línea de comandos.

A demás se establece los parámetros considerados para el análisis del comportamiento de la red en presencia de carga y se evalúa el impacto de diferentes políticas en dicho funcionamiento.

3.2 Descripción de la Herramienta utilizada para la configuración del escenario

El RouterOS es un sistema operativo y software que convierte a una PC en un router dedicado, bridge, firewall, controlador de ancho de banda, punto de acceso inalámbrico o cliente y mucho más.

El RouterOS puede hacer casi cualquier cosa que tenga que ver con las necesidades de red, además de cierta funcionalidad como servidor.

- Basado en kernel de Linux.
- Puede ejecutarse desde discos IDE o módulos de memoria flash.
- Diseño modular.
- Módulos actualizables.
- Interface grafica amigable.

3.2.1 Características

- Ruteo. Estático o dinámico, políticas de enrutamiento.
- Bridging. Protocol Spanning tree, interfaces multiples bridge, firewall en el bridge
- Servidores y clientes: DHCP, PPPoE, PPTP, PPP, Relay de DHCP.
- Cache: Web-proxy, DNS
- Gateway de HotSpot

- Lenguaje interno de scripts
- Filtrado de paquetes por
- Origen, IP de destino
- Protocolos, puertos
- Contenidos (seguimiento de conexiones P2P)
- Puede detectar ataques de denegación de servicio (DoS)
- Permite solamente cierto número de paquetes por periodo de tiempo
- Que pasa enseguida si el límite es desbordado o sobrepasado

3.2.2 Instalación del Router Mikrotik

El router MikroTik puede ser instalado usando:

- Floppy disks
- CD creado desde una imagen ISO, contiene todos los paquetes.
- Vía red usando netinstall, la pc donde se instalará debe botear con un floppy, o usando Protocolos PXE o EtherBoot desde algunas ROMS de ciertas tarjetas de red.
- Con imagen de Disco
- Con Memoria Flash/IDE

Requisitos mínimos:

- Pentium III
- 128 MB en RAM
- Disco IDE

A continuación se muestra paso por paso como se realiza la instalación de Mikrotik sobre una plataforma x86. Utilizamos la versión 2.9.27 *Nivel 6* del software Mikrotik RouterOs:

Se Bootea con un CD que contenga la imagen del Mikrotik RouterOs ya quemada. Luego nos aparece el menú de instalación que nos preguntará que paquetes deseamos instalar.

Para desplazarnos por el menú utilizamos las tecla ´P´ o ´N´ o sino las flechas del teclado. Para seleccionar o deseleccionar los paquetes a instalar utilizamos la Barra Espaciadora. Luego se presiona la tecla ´I´ para comenzar la instalación local en nuestra plataforma.

Se debe instalar primero la versión 2.9.27, para luego ser crakeado a la versión 3.22 de Mikrotik por la estabilidad que éste ofrece.

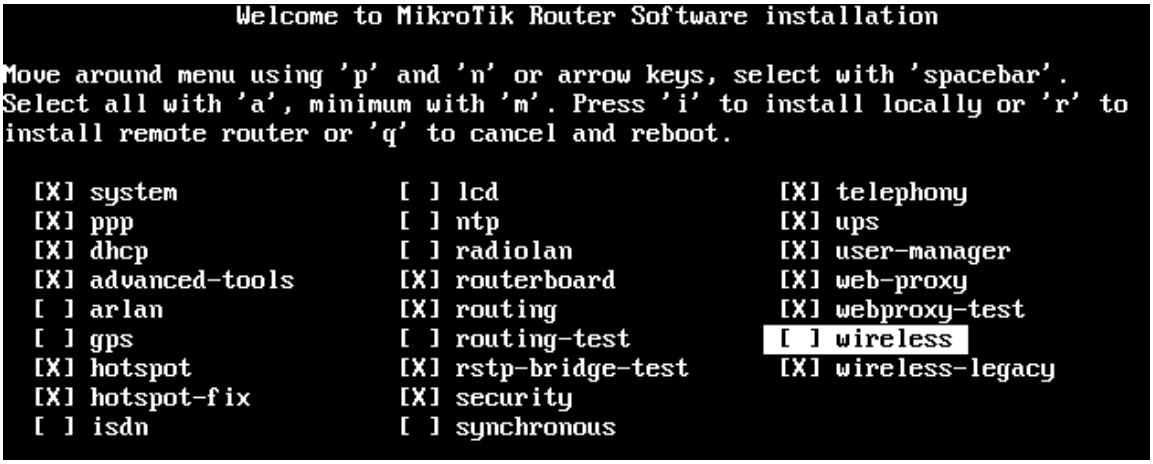


Gráfico III.15 Personalización de la instalación de la herramienta Mikrotik I.

Aquí se detalla los paquetes seleccionados, que el **Gráfico III.15** nos indica:

- System: Paquete principal que posee los servicios básicos al igual que los drivers básicos.
- Ppp: Provee de soporte para PPP, PPTP, L2TP, PPPoE e ISDN PPP.
- Dhcp: Servidor y cliente DHCP.
- Hotspot: provee de un Hot Spot.
- Hotspot-fix: Provee el parche para actualizar el modulo hot spot que tiene problemas en las versión 2.9.27.
- Ntp: Servidor y cliente NTP.
- Routerboard: provee de las utilidades para el routerboard.
- Routing: Provee soporte para RIP, OSPF y BGP4.
- Rstp-bridge-test: prove soporte para Rapid Spanning Tree Protocol.
- Security: Provee soporte para IPSEC, SSH y conectividad segura con Winbox.
- Telephony: Provee soporte para H.323.
- Ups: provee soporte para UPS APC.
- User-manager: Servicio de usuario del RouterOs
- Web-Proxy: Paquete para realizar un Web Proxy.
- Wireless-legacy: Provee soporte para placas Cisco Aironet, PrismII, Atheros entre otras.

Luego la instalación nos pregunta se desea mantener la configuración anterior, se contesta que no ´N´ (ver **Gráfico III.16**).

La siguiente pregunta hace referencia a que perderemos todos los datos que se encuentran en el disco fijo´, contestamos que si ´Y´.

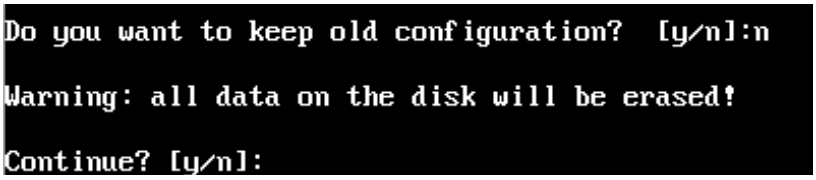


Gráfico III.16 Personalización de la instalación de la herramienta Mikrotik II.

A continuación comienza el proceso de particionado y formateado del disco fijo que es automático. Se presiona ´Enter´, para que el sistema se reinicie. Seguidamente nos pregunta si deseamos chequear la superficie del disco fijo le contestamos que si ´Y´.

Luego comienza la instalación de los paquetes seleccionados con anterioridad. Al finalizar dicho proceso, se presiona ´Enter´ nuevamente para reiniciar el sistema, el **Gráfico III.17** nos muestra a continuación:

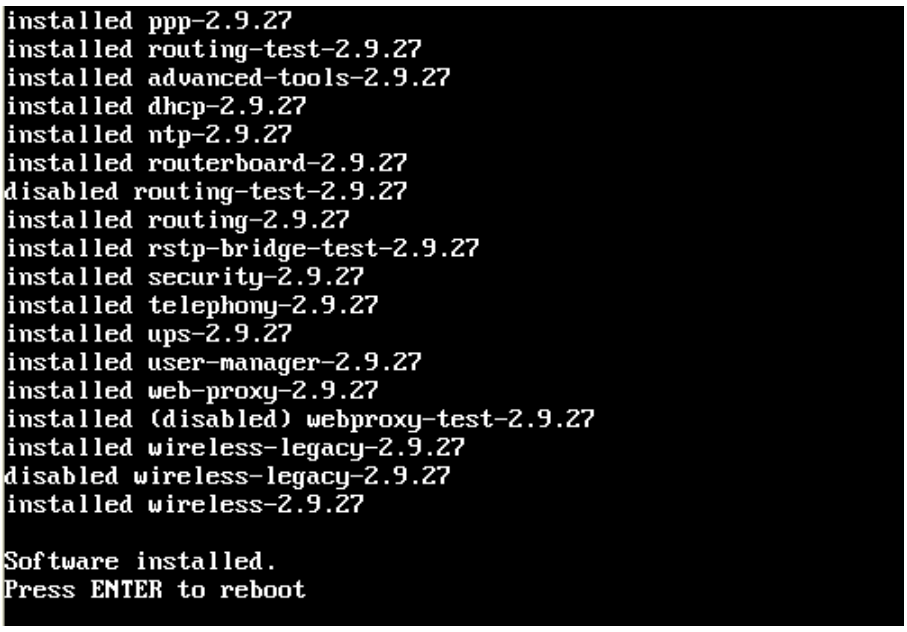


Gráfico III.17 Instalación de paquetes en Mikrotik.

Con el sistema reiniciado e instalado, la consola pide nombre de usuario y contraseña (ver **Gráfico III.18**). Por defecto dicho nombre de usuario es: *admin* y para la contraseña se deja el casillero en blanco y se presiona ´Enter´.

Gráfico III.18 Pantalla de Logueo en Mikrotik.

A continuación nos da la bienvenida y pregunta se desea leer la licencia lo cual se contesta que si ´Y´. Luego de haber leído la licencia (ver **Gráfica III.19**) nos queda la consola para comenzar a configurar Mikrotik.

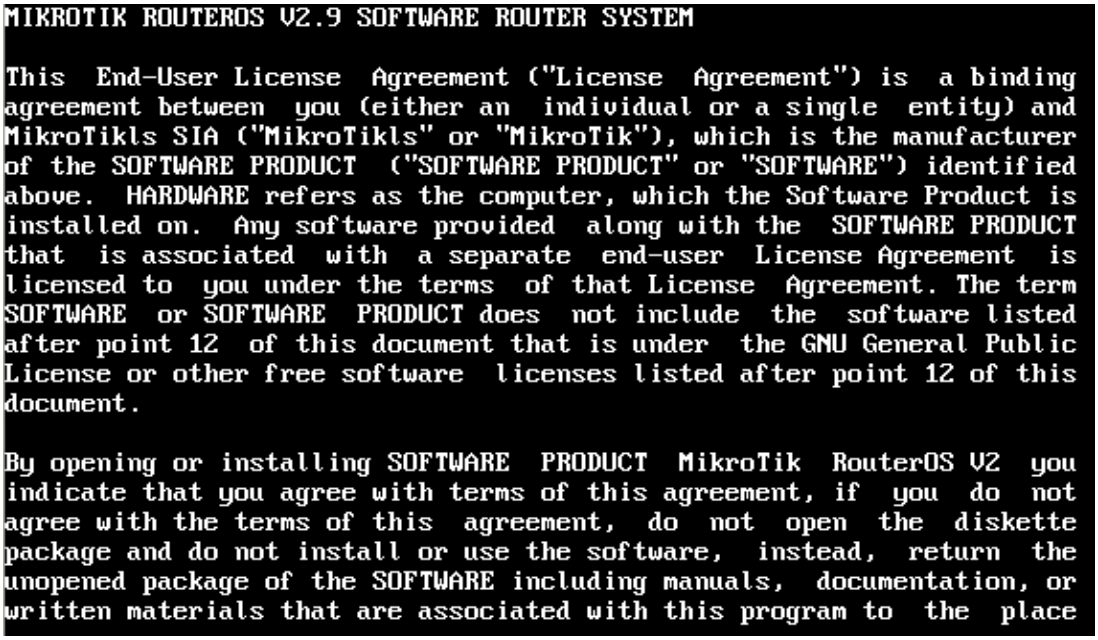


Gráfico III.19 Términos de Licencia

Se debe generar el código para el Licenciamiento (ver **Gráfico III.20**) con el comando:

[admin@MikroTik]> **mikrotik generate**

Gráfico III.20 Generación de Licencia

Se reinicia la máquina y luego se procede a instalar la versión 3.22 de Mikrotik con un cd booteable, seleccionamos todos los paquetes (opción a) que necesitemos menos MPLS test y Xen que dan errores en el proceso de instalación. Se presiona con la opción i para empezar a instalar.

Pregunta si se desea conservar la configuración anterior a lo que se responde que si ´Y´ (ver **Gráfico III.21**). Se crea la partición, se formatea el disco y se instalan los paquetes seleccionamos.

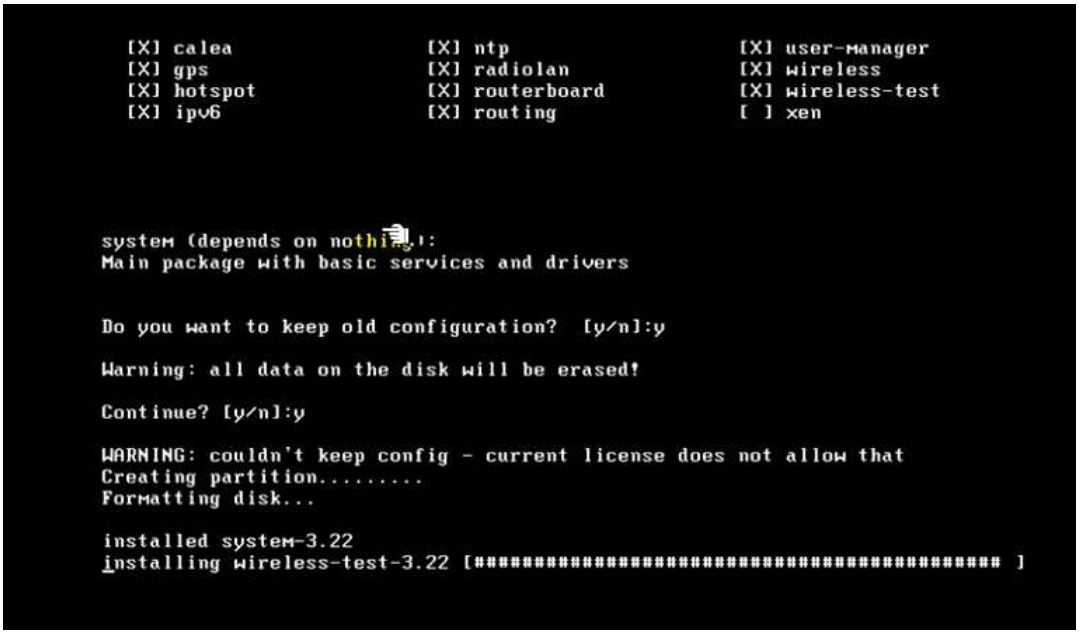


Gráfico III.21 Instalación de Mikrotik 3.22.

Una vez instalado se puede acceder a la máquina a través de la herramienta Winbox 2.2.15 (ver **Gráfica III.22**) previamente descargada de la página www.mikrotik.com, para registrar el producto:

Gráfico III.22 Herramienta Winbox 2.2.15.

En esta ventana permite introducir las direcciones Mac o ip de la placa del Mikrotik a la cual nos conectamos.

Se hace clic en (…) para que el software nos devuelva las direcciones Mac de las interfaces de red que posean un Mikrotik instalado y corriendo.

Seleccionamos la interface y luego utilizaremos de Login: admin y como Password: (nada) de igual forma que se configuró en modo consola de la máquina Mikrotik RouterOS (Ver **Gráfico III.18**). Al finalizar esta carga de datos hacemos clic en Connect.

Luego cuando el soft se conecta al Mikrotik automáticamente empieza a descargar los plugins instalados en el Mikrotik para poder administrarlos remotamente, como muestra el **Gráfico III.23** a continuación:

Gráfico III.23 Descarga de plugins instalados para administrar Mikrotik.

Al finalizar la descarga de los plugins nos aparece la pantalla de configuración del Mikrotik (ver **Gráfico III.24**). En la cual a mano izquierda se encuentra el menú de configuración de cada uno de los módulos instalados.

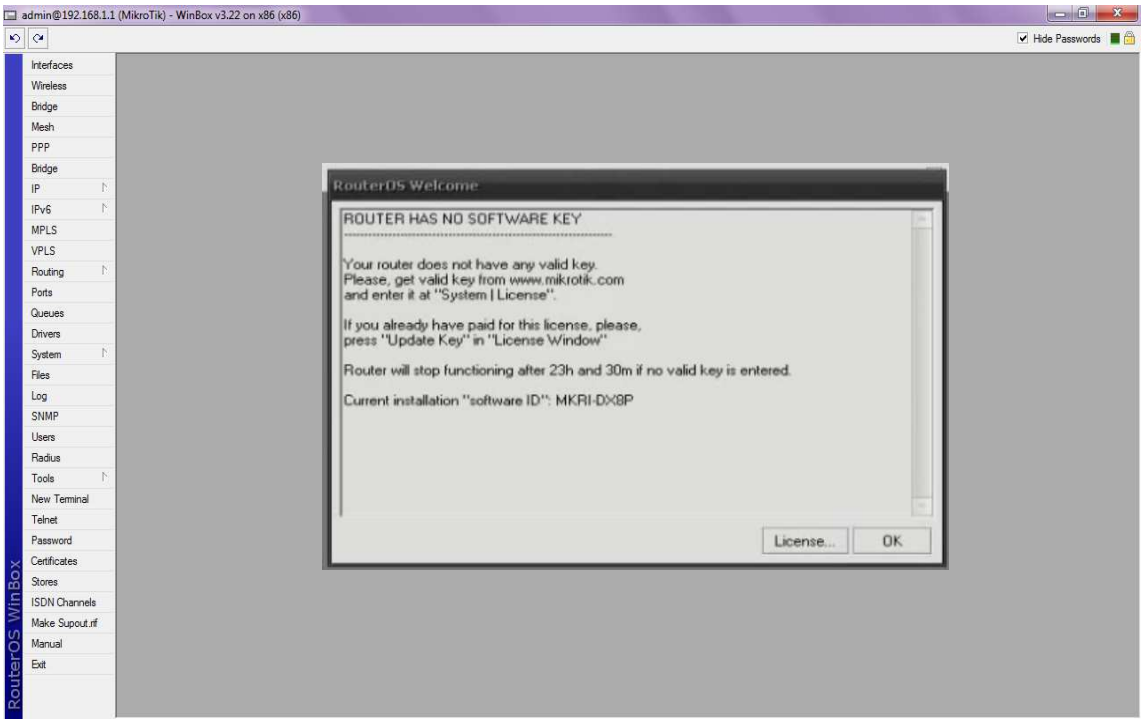


Gráfico III.24 Pantalla de configuración de Mikrotik

Descargamos de internet las llaves de licenciamiento para Mikrotik 3.22, y haciendo referencia al código generado anteriormente (ver **Gráfico III.20**), copiamos el texto correspondiente a dicho nivel de licenciamiento del archivo plano que nos indica el **Gráfico III.25** a continuación.

Gráfico III.25 Pantalla de licenciamiento Mikrotik I

Se hace clic en License de la ventana de bienvenida de Mikrotik y se importa el archivo que contiene la llave de licenciamiento (ver **Gráfico III.26**), que lo ubicamos en Mis Documentos, en este archivo generado pegamos el texto anteriormente copiado de los niveles de las llaves de licenciamiento, se trabajó con niveles 5 y 6 de licenciamiento.

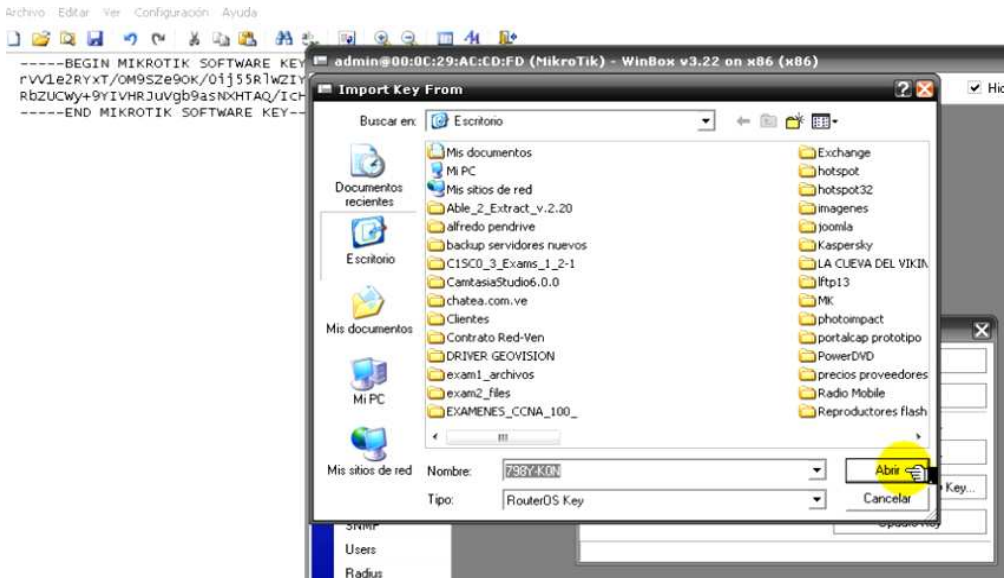


Gráfico III.26 Pantalla de licenciamiento Mikrotik II

Para que el cambio de la llave de licenciamiento sea efectuado, se debe reiniciar el router (ver **Gráfico III.27**).

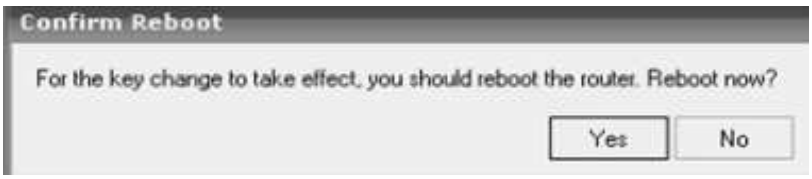


Gráfico III.27 Reinicio del Router después de licenciamiento

3.2.3 Licenciamiento

La Licencia es por instalación

Algunas funcionalidades requieren de cierto nivel de licenciamiento.

La Licencia nunca expira, esto significa que el router funcionara “de por vida”.

EL router puede ser actualizado durante el periodo de actualización (1 año después de la compra de la licencia).

El periodo de actualización puede ser extendido a un 60% del costo de la licencia.

Niveles de licenciamiento

Nivel 0: DEMO, GRATIS, tiene todas las funcionalidades sin límite, funciona solo 24 hrs, después de ello debe de ser REINSTALADO

Nivel 1: Licencia SOHO, GRATIS, pero requiere registrarse en www.mikrotik.com , tiene limitaciones, (1src-nat, 1dst-nat, 1 pppoe, …)

Nivel 4: WISP, cliente inalámbrico, Punto de Acceso Inalámbrico, gateway de HotSpot.

Nivel 5: WISP AP, Access Point inalámbrico y cliente, Gateway de HotSpot (mas conexiones soportadas)

Nivel 6: CONTROLLER, Todo sin límite

Nota: Una Licencia basta para cualquier número de interfaces inalámbricas en el router.

3.2.4 Formas de Acceder al Router

Los routers Mikrotik pueden ser accedidos vía:

- Monitor y teclado
- Terminal Serial
- Telnet
- Telnet de MAC
- SSH
- Interface grafica Winbox
- Winbox GUI

WinBox es mucho más fácil que el CLI, al ser una interface grafica.

winbox.exe es un pequeño programa que se ejecuta desde una estación de trabajo conectada al router.

winbox.exe corre bajo WINE en Linux, usa el puerto TCP 8291 para conectarse al router. La comunicación entre el winbox y el router está encriptada.

3.3 Configuración del Escenario

En este apartado se especifica los equipos y dispositivos utilizados para el establecimiento del escenario, así como la configuración de las PC Router Mikrotik en los protocolos OSPF y MPLS, y tratando la QoS en este contexto.

3.3.1 Equipos y dispositivos de red

Equipos

Id PC	Tipo	Sistema Operativo	No. Tarjetas de red	RAM	DD
Pc1	Cliente	Windows XP	1	512MB	80
R1	PC Router	Mikrotik RouterOS	2	512MB	80
R2	PC Router	Mikrotik RouterOS	2	512MB	80
R3	PC Router	Mikrotik RouterOS	3	512MB	80
R4	PC Router	Mikrotik RouterOS	3	512MB	80
R5	PC Router	Mikrotik RouterOS	2	512MB	80
Pc2	Servidor	Windows XP	1	1GB	250
Pc3	Monitor de red	Windows 7	1	1GB	160

Tabla III.2 Tabla de equipos.

Dispositivos de Red

- 1 Hub Encore ENH708
- 6 Cables Cruzados
- Cables Directos

3.3.2 Especificación de la Topología

La estructura física de la nube MPLS, se encuentra constituida básicamente por cinco máquinas cada una con el S.O, Mikrotik RouterOS, con tres y dos tarjetas respectivamente ubicadas para el enlace entre ellas dentro de la configuración del escenario.

Por un lado se ubica el Cliente enlazado a la máquina Router R4, la misma que se enlaza a las máquinas Router R3 y R5; y de otro lado se encuentra el Servidor enlazado a la máquina Router R1, dicha máquina se enlaza al Router R2. Para la unión de las máquinas Router R2 y R3 se utilizó cables directos ya que en éste enlace se pretende medir el tráfico mediante un Hub (ver **Gráfico III.28**)

Se agregó un Hub, colocado en el centro de la nube MPLS, en el que se reúnen las PC Routers Mikrotik, que permite la captura y medición del flujo de paquetes que se genera dentro de la red establecida, por una máquina que posee los sniffers: Wireshark y Colasoft Capsa que logran dicho propósito.

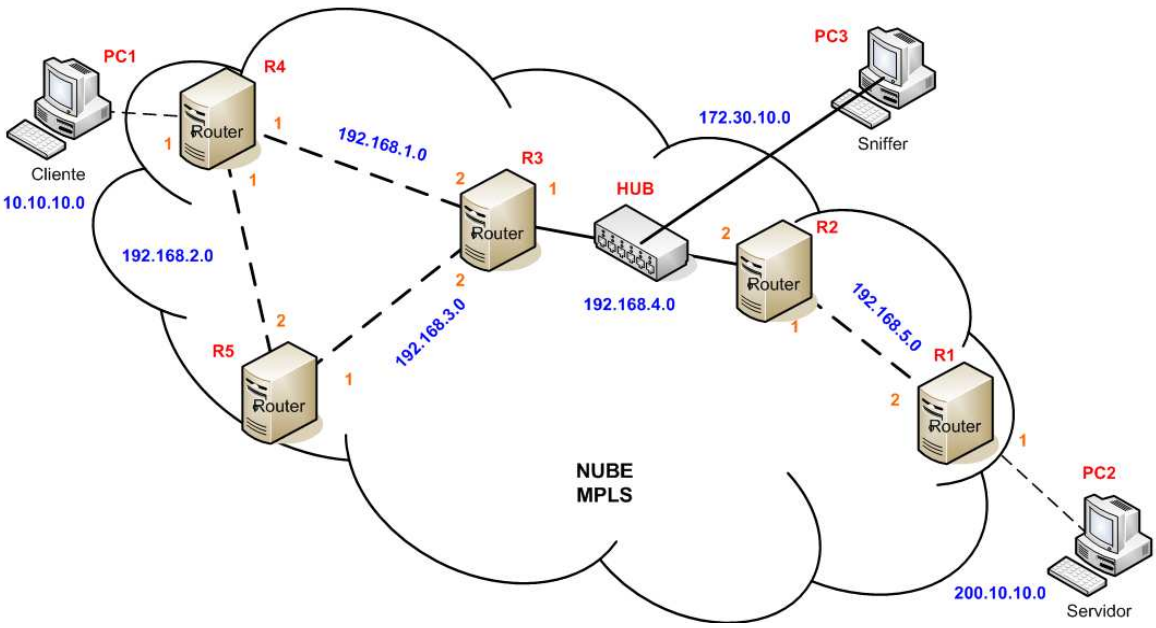


Gráfico III.28 Topología de la Red.

3.3.3 Configuración de los PC Routers en Mikrotik

En este apartado se indica la configuración de los PC Router Mikrotik, desde el establecimiento de sus interfaces de red, en cada máquina, así como la configuración propia de los protocolos OSPF para el establecimiento del ruteo y el protocolo MPLS que se lo aplica para luego manipular y clasificar el tráfico dando garantías de QoS en el escenario planteado.

3.3.3.1 Configuración de las Interfaces de Red

Como se indicó anteriormente se procede a configurar los Router Mikrotik de dos formas: por Interfaz Gráfica y por Líneas de Código, para un mejor entendimiento.

POR INTERFAZ GRÁFICA

Accedemos al menú principal de la Ventana Winbox, se hace clic en la pestaña IP – Addresses del menú principal, se hace clic en el botón  para añadir una interfaz, donde se llena los campos de dirección y la interfaz a la que corresponde, el **Gráfico III.29** nos indica a continuación:

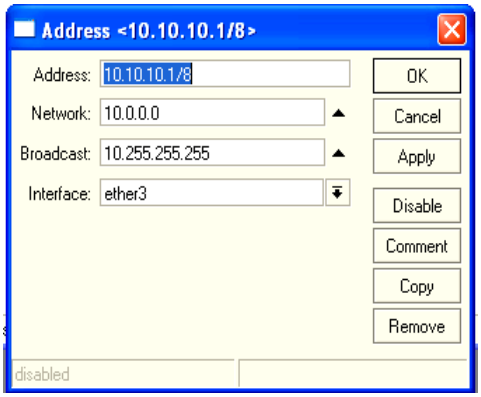


Gráfico III.29 Añadir Interfaces con Winbox.

El **Gráfico III.30** muestra todas las interfaces configuradas del Router R4:

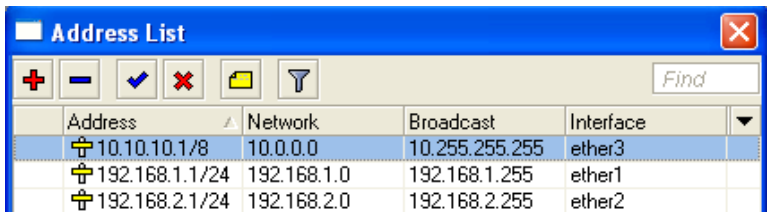


Gráfico III.30 Interfaces configuradas en el Router R4.

POR LÍNEAS DE CÓDIGO

A continuación se muestra la configuración de todas las interfaces de los Routers Mikrotik:

R1

[admin@R1]> ip address add address=192.168.5.2/24 interface=ether1

[admin@R1]> ip address add address=200.10.10.1/24 interface=ether2

R2

[admin@R2]> ip address add address=192.168.4.2/24 interface=ether1

[admin@R2]> ip address add address=192.168.5.1/24 interface=ether2

R3

[admin@R3]> ip address add address=192.168.1.2/24 interface=ether1

[admin@R3]> ip address add address=192.168.3.2/24 interface=ether2

[admin@R3]> ip address add address=192.168.4.1/24 interface=ether3

R4

[admin@R4]> ip address add address=192.168.1.1/24 interface=ether1

[admin@R4]> ip address add address=192.168.2.1/24 interface=ether2

[admin@R4]> ip address add address=10.10.10.1/8 interface=ether3

R5

[admin@R5]> ip address add address=192.168.2.2/24 interface=ether1

[admin@R5]> ip address add address=192.168.3.1/24 interface=ether2

Se puede ver las interfaces añadidas (ver **Gráfico III.31**) mediante el comando:

[admin@R4]> **ip address print**

```
[admin@R4] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #    ADDRESS            NETWORK         BROADCAST        INTERFACE
 0    192.168.1.1/24     192.168.1.0     192.168.1.255    ether1
 1    192.168.2.1/24     192.168.2.0     192.168.2.255    ether2
 2    10.10.10.1/8       10.0.0.0        10.255.255.255   ether3
```

Gráfico III.31 Impresión de Interfaces del Router.

3.3.3.2 Configuración de OSPF

MikroTik RouterOS implementa OSPF Versión 2 (RFC 2328). Debemos verificar que el paquete routing debe ser instalado(ver **Gráfico III.32**), con el comando:

[admin@MikroTik]> **system package print**

Si no está instalado, subimos el paquete de la misma versión del router 'routing-2.x.x.npk' y reiniciamos el router. OSPF usa protocolo 89 para comunicarse con sus vecinos, debemos asegurarnos que la cadena input del firewall no lo filtre.

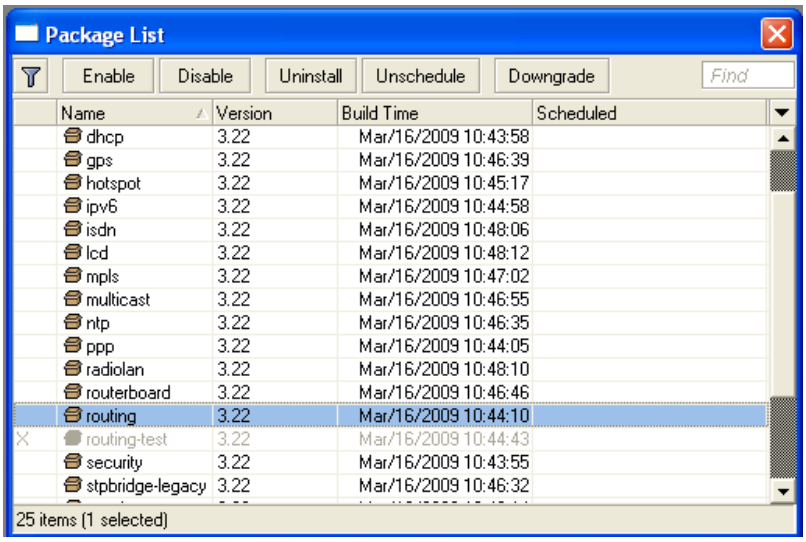


Gráfico III.32 Impresión de Interfaces del Router.

POR INTERFAZ GRÁFICA

Se procede a configurar OSPF y se puede encontraro en la opción Routing- OSPF del menú princiipal y se configura los parámetros de setting, el **Gráfico III.33** muestra los parámetros de configuración:

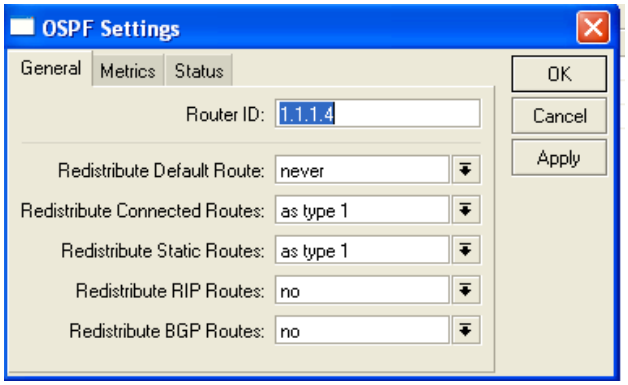


Gráfico III.33 Configuración de los parámetros settings de OSPF.

En la configuración del protocolo de enrutamiento dinámico OSPF, a cada punto de la red se le asigna una prioridad mediante el parámetro router-id para poder crear adyacencias correctamente. La siguiente es la lista de equivalencias entre router-id y puntos de la red, y estos parámetros se detallan a continuación:

router-id –(ID del Router) El Router ID. Si no lo especificó (valor predeterminado 0.0.0.0), OSPF usa la dirección de IP más grande configurada en las interfaz como su ID del router.

redistribute-connected –(Redistribuir Conectadas) si establece, el router distribuirá la información sobre todos los routers conectados, es decir, rutas a redes que pueden alcanzarse directamente del router(como-tipo-1, como-tipo-2,no)

Ospf soporta 2 tipos de métricas:

• **type1 -** Métricas externas se expresan en las mismas unidades como costo de la interfaz OSPF. En otras palabras, el router espera que el costo de un vínculo a una red que es externa a AS para ser el mismo orden de magnitud como el costo de los enlaces internos.

• **type2 -** Métricas externas son un orden de magnitud más grande; cualquier métrica de tipo2 se considera mayor que el costo de cualquier ruta interna a la AS. El uso de métricas tipo2 asume que el router entre e AS es el mayor costo de enrutamiento de un paquete .

redistribute-static –(Redistribuir Estáticas) si establece, el router redistribuirá la información sobre todas las rutas estáticas agregadas a su base de datos de la asignación de ruta, es decir, rutas que se han creado usando el comando del router /ip route add (como-tipo-1, como-tipo-2, ningún)

redistribute-rip – (Redistribuir Rip)si establece, el router redistribuirá la información sobre todas las rutas aprendidas por el protocolo RIP(como-tipo-1, como-tipo-2, ningún)

redistribute-bgp –(Redistribuir Bgp) si establece, el router redistribuirá la información sobre todas las rutas aprendidas por el protocolo BGP(como-tipo-1, como-tipo-2, ningún)

distribute-default – (Redistribuir Predeterminada) Controla como propagar la ruta predefinida a otros routers:

never –(Nunca)no envía su propia ruta predeterminada (default) a otros routers

if-installed (as **type 1** or **type 2**) –(Si Instalo) envía la ruta de default sólo si se ha instalado (una ruta estática predefinida, o agregó rutas por DHCP, PPP, etc.)

always (as **type 1** or **type 2**)- (Siempre)siempre envía la ruta predeterminada

metric-default – (Métrica Predeterminada)costo de la ruta predeterminada

metric-connected – (Métrica conectado) el costo de rutas conectadas

metric-static – (Métrica estático)el costo de rutas estáticas

metric-rip – (Métrica Rip)costo de rutas aprendidas por el protocolo RIP

metric-bgp - (Métrica Bgp)costo de rutas aprendidas por el protocolo BGP

Asignación del router-id a los enrutadores de la red

Para identificar las máquinas Router Mikrotik se les coloca un identificador para su comunicación.

Maquina	Router ID
R1	1.1.1.1
R2	1.1.1.2
R3	1.1.1.3
R4	1.1.1.4
R5	1.1.1.5

Tabla III.3 Tabla Identificación de los Routers con OSPF.

Asignación de Redes

Se agregó las redes que participan en OSPF, esto se hace en la ventana principal OSPF, en la pestaña *Networks* y se añade los segmentos de las interfaces correspondientes:

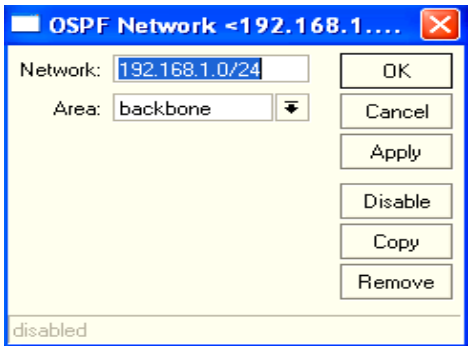


Gráfico III.34 Añadir redes para el ruteo OSPF.

Este proceso se lo debe realizar con todas las Network que se necesite que participen en el protocolo OSPF, hay que tomar en cuenta que si se agrega un segmento a OSPF Network y esta no se encuentra en alguna interfaz activa no va a ser anunciada y por tanto no va a formar parte de OSPF. Al terminar deben tener algo similar a la **Gráfica III.35**:

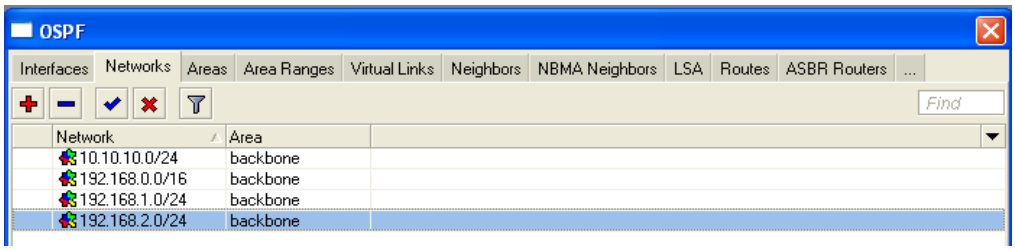


Gráfico III.35 Vista de las Redes de OSPF.

Se trabajó con una sola área y es el área 0, si se observa las redes colocadas anteriormente en la casilla Área, por default se puso Backbone; esto quiere decir que automáticamente se ha creado el área 0, si por ejemplo se usara más de un área entonces se tiene que especificar esto en la sección de Área y entonces en el combo box aparece además de backbone las otras áreas.

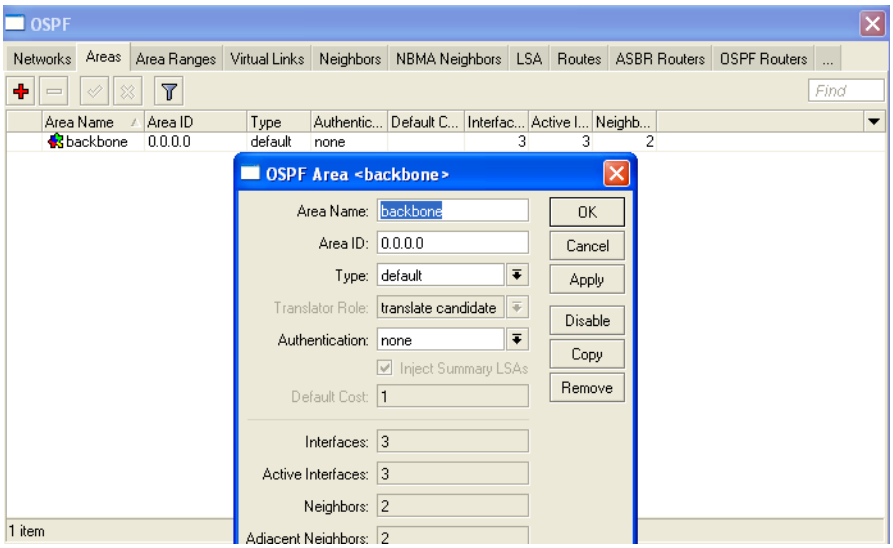


Gráfico III.36 Configuración del área backbone en OSPF.

Áreas de OSPF

Ospf permite agrupar conjuntos de routers. Tal grupo es conocido como área. En cada área corre como una copia separada del algoritmo básico de ruteo de enlace. Esto significa que cada área tiene su propia base de estado enlace y su gráfico correspondiente. El **Gráfico III.36** nos indica los parámetros que se explican a continuación:

area-name nombre del área

area-id (*IP address*; default: **0.0.0.0**) - Identificador de área OSPF. Por defecto el área-id = 0.0.0.0 es el área de red troncal. OSPF backbone siempre contiene todos los enrutadores de borde de área. El backbone es responsable de la distribución de información de enrutamiento entre aéreas no backbone.

authetication (*ninguno* | *simple* | *md5*; por defecto: **ninguno**) – Especifica los métodos de autenticación para los mensajes del protocolo OSPF.

- **none** – no usa autenticación
- **simple** - autenticación de texto plano
- **md5** - autenticación con clave de Message Digest 5

default-cost (*integer*; default: **1**) - Especifica el costo predeterminado utilizado para las áreas de rutas internas. Aplicables solamente a los enrutadores de límite de área.

Este proceso se tiene que repetir en los 4 router Mikrotik restantes: R5, R3, R2 y R4, usando sus respectivas IP para la configuración del OSPF y al final una vez configurado los 5 routers Mikrotik, en la sección de Neighbor de cada router, se puede ver a los router vecinos con los cuales ya se realizo una adyacencia como se muestra a continuación.

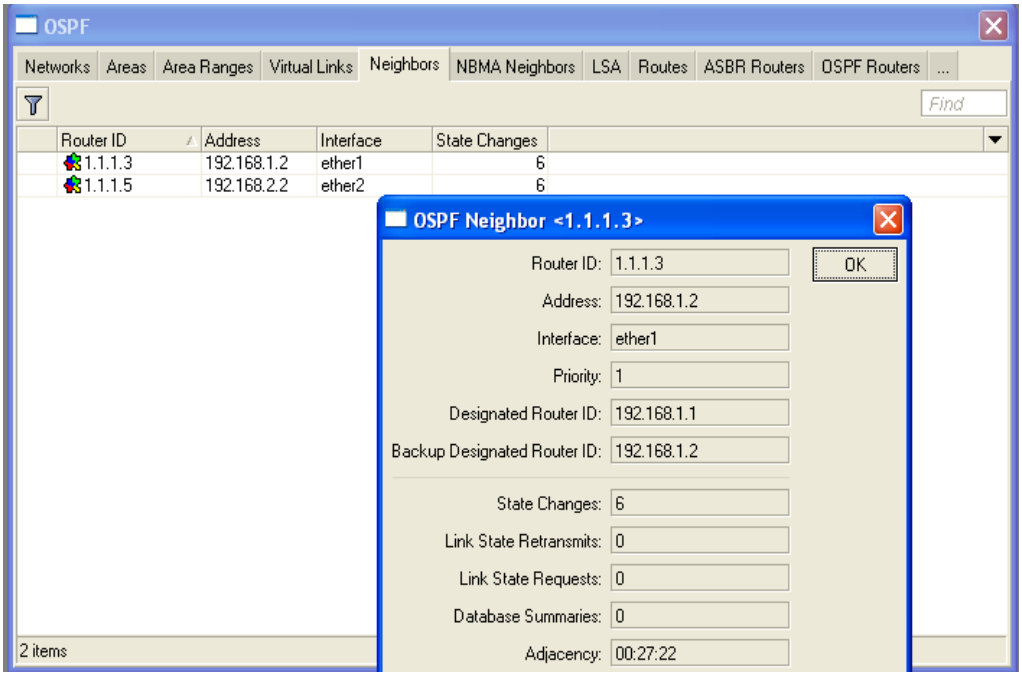


Gráfico III.37 Vista de los routers vecinos OSPF.

Ospf Neighbors

El submenú provee acceso a la lista de los routers OSPF vecinos, a continuación se detallan los parámetros de un Neighbor como muestra el **Gráfico III.37**:

router-id - parámetro ID router del vecino.

address - dirección IP del vecino OSPF.

priority - prioridad de vecino que se utiliza en las elecciones de enrutador designado en esta red.

state – estado de la conexión:

Down - la conexión está inactive

Attempt - Enviar paquete hello

Init - paquete hello recibido del vecino

2-Way - comunicación bidireccional establecida

ExStart - negociación de estado de Exchange

Exchange - intercambiando con la Base de datos de la abertura del enlace

Loading – recibiendo información del vecino

Full - los enrutadores vecinos son completamente adyacentes (las bases de datos de estado del vínculo completamente están sincronizados)

state-changes - número de cambios de estado de la conexión

ls-retransmits - número de retransmisiones de estado de vínculo

ls-requests -número de solicitudes de estado de vínculo

db-summaries - número de registros de base de datos de estado del vínculo anunciados por el vecino.

dr-id - id de la ruta del enrutador designado para este vecino.

backup-dr-id - id del router de la ruta de respaldo diseñado para este vecino.

Interfaces de OSPF

Este servicio proporciona herramientas para configuración de fondo adicional de parámetros específicos de la interfaz de OSPF. No es necesario configurar interfaces a fin de ejecutar ospf, estos campos se indican a continuación en el **Gráfico III.38**:

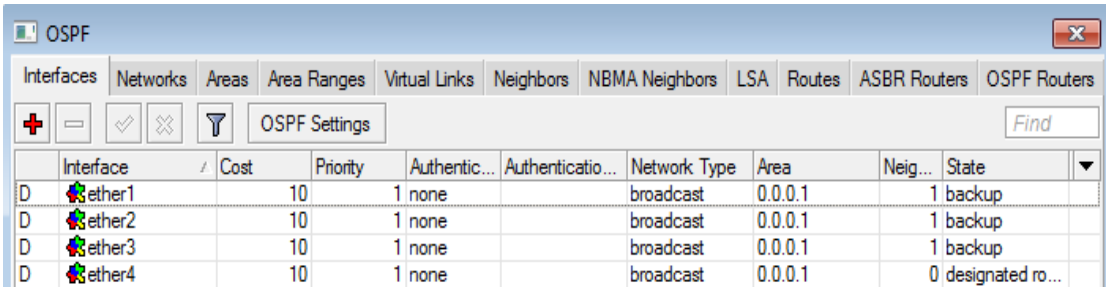


Gráfico III.38 Interfaces del Router en OSPF.

authentication-key (*text*; default: **""**) - clave de autenticación deben ser utilizados por los enrutadores vecinos que están utilizando autenticación simple de OSPF

cost (*integer*: 1..65535; default: **1**) – costo de interfaz expresado como métrica de enlaces estáticos.

dead-interval (*time*; default: **40s**) - Especifica el intervalo después de que un vecino se declara como muertos. El intervalo se anuncia en paquetes de hello del enrutador. Este valor debe ser la misma para todos los enrutadores y servidores de acceso en una red específica.

hello-interval (*time*; default: **10s**) - el intervalo entre paquetes de hello que envía el enrutador en la interfaz. Cuanto menor sea el intervalo hello, se detectará los cambios topológicos más rápidos, pero se puedan tener más tráfico de enrutamiento. Este valor debe ser el mismo en cada extremo de la adyacencia, lo contrario que no se formará la adyacencia.

interface (*name*; default: **all**) interfaz en que se ejecutará OSPF.

• **All** se utiliza para las interfaces que no posean cualquier configuración específica.

priority (*integer*: 0..255; default: **1**) - prioridad del enrutador. Ayuda a determinar el enrutador designado para la red. Cuando los dos enrutadores conectados a una red

ambos intentan convertirse en el enrutador designado, el único enrutador con mayor prioridad tendrá preferencia.

retransmit-interval (*time*; default: **5s**) - tiempo entre retransmitir anuncios de enlaces perdidos.

Cuando un enrutador envía un anuncio de estado del vínculo (LSA) a su vecino, mantiene la LSA hasta recibir de vuelta el reconocimiento. Si no recibe ninguna confirmación en el tiempo, retransmiten la LSA. Se recomiendan los siguientes valores: para la transmisión red son 5 segundos y de red de punto a punto son 10 segundos.

transmit-delay (*time*; default: **1s**) - demora de transmisión del estado del enlace es el tiempo estimado necesario para transmitir un paquete de actualización del estado del enlace en la interfaz

POR LÍNEAS DE CÓDIGO

El ID del Router debe ser único dentro del sistema autónomo (AS) y se lo debe dejar como: 1.1.1.X.

A continuación se muestra la configuración de todos los Routers Mikrotik con protocolo MPLS.

R1

[admin@R1]> routing ospf set distribute-default=as-never

set redistribute-connected=as-type-1

set redistribute-static=as-type-1

[admin@R1]> routing ospf area add name=backbone area-id=0.0.0.0

[admin@R1]> routing ospf network add network=200.10.10.0/24 area=backbone

[admin@R1]> routing ospf network add network=192.168.5.0/24 area=backbone

[admin@R1]> routing ospf network add network=192.168.0.0/16 area=backbone

R2

[admin@R2]> routing ospf set distribute-default=as-never

set redistribute-connected=as-type-1

set redistribute-static=as-type-1

[admin@R2]> routing ospf area add name=backbone area-id=0.0.0.0

[admin@R2]> routing ospf network add network=192.168.4.0/24 area=backbone

[admin@R2]> routing ospf network add network=192.168.5.0/24 area=backbone

[admin@R2]> routing ospf network add network=192.168.0.0/16 area=backbone

R3

[admin@R3]> routing ospf set distribute-default=as-never

set redistribute-connected=as-type-1

set redistribute-static=as-type-1

[admin@R3]> routing ospf area add name=backbone area-id=0.0.0.0

[admin@R3]> routing ospf network add network=192.168.1.0/24 area=backbone

[admin@R3]> routing ospf network add network=192.168.3.0/24 area=backbone

[admin@R3]> routing ospf network add network=192.168.4.0/24 area=backbone

[admin@R3]> routing ospf network add network=192.168.0.0/16 area=backbone

R4

[admin@R4]> routing ospf set distribute-default=as-never

set redistribute-connected=as-type-1

set redistribute-static=as-type-1

[admin@R4]> routing ospf area add name=backbone area-id=0.0.0.0

[admin@R4]> routing ospf network add network=10.10.10.0/8 area=backbone

[admin@R4]> routing ospf network add network=192.168.1.0/24 area=backbone

[admin@R4]> routing ospf network add network=192.168.2.0/24 area=backbone

[admin@R4]> routing ospf network add network=192.168.0.0/16 area=backbone

R5

[admin@R5]> routing ospf set distribute-default=as-never

set redistribute-connected=as-type-1

set redistribute-static=as-type-1

[admin@R5]> routing ospf area add name=backbone area-id=0.0.0.0

[admin@R5]> routing ospf network add network=192.168.2.0/24 area=backbone

[admin@R5]> routing ospf network add network=192.168.3.0/24 area=backbone

[admin@R5]> routing ospf network add network=192.168.0.0/16 area=backbone

Para ver las configuraciones de la red ospf (ver **Gráfica III.39**) lo hacemos mediante el comando:

[admin@MikroTik]> **routing ospf network print**

```
[admin@R4] > routing ospf network print
Flags: X - disabled, I - invalid
 #   NETWORK            AREA
 0   192.168.1.0/24     backbone
 1   192.168.2.0/24     backbone
 2   192.168.0.0/16     backbone
 3   10.10.10.0/24      backbone
```

Gráfico III.39 Impresión de las redes de un Router OSPF.

Como testing final conectamos el cliente y el servidor a las interfaces correspondientes en el escenario establecido (ver **Gráfico I.1**) y como resultado de la configuración de OSPF debemos tener respuesta de las IP de la red, para posteriormente acceder remotamente a cualquier máquina router Mikrotik mediante Winbox.

3.3.3.3 Configuración de MPLS

Para la configuración de éste escenario con protocolo MPLS, se debe especificar que necesita del protocolo OSPF para que exista comunicación entre las máquinas que intervienen en la nube para el ruteo de los paquetes.

POR INTERFAZ GRÁFICA

Cada enrutador está configurado con un lobridge de adaptador de bucle que contiene la dirección de bucle invertido. En la página http://wiki.mikrotik.com/wiki/MPLSVPLS podemos ver que esto sirve para dos propósitos:

Como sólo hay una sesión LDP entre 2 enrutadores cualquiera, sin importar cuántos enlaces se conectan, la dirección IP loopback asegura que el período de sesiones LDP no se ve afectado por el estado de interfaz o cambios de dirección usan la dirección loopback.

Se agrega interfaz Bridge que servirá de puente para la configuración de MPLS, como se observa en el **Gráfico III.40**:

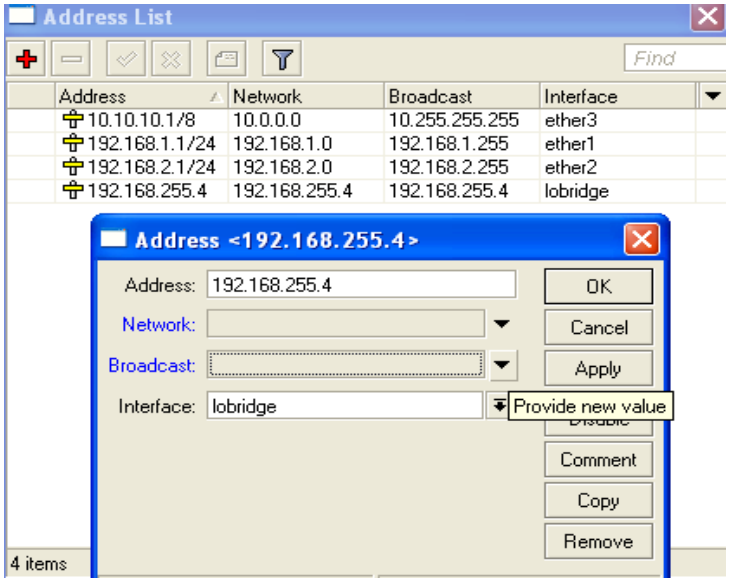


Gráfico III.40 Configuración de Interfaz bridge en MPLS.

Luego se accede a la pestaña MPLS – LDP Interface del menú principal de Winbox, se selecciona la opción Enabled y se coloca el identificador el LSR y la dirección de transporte de dicho router (ver **Gráfico III.41**).

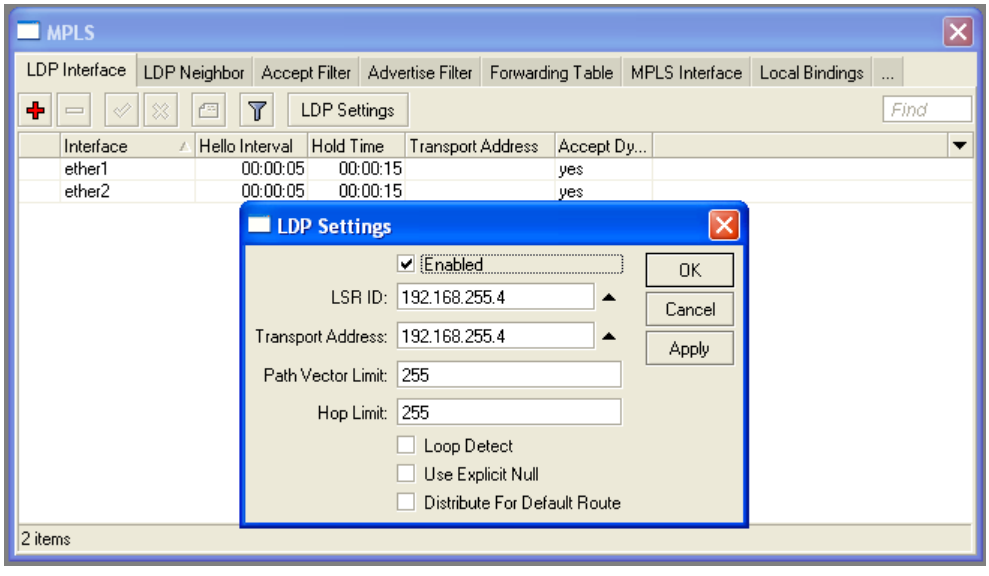


Gráfico III.41 Configuración de valores de LDP en MPLS.

Se añade las interfaces del router que intervienen en la nube MPLS, haciendo clic en  de la pestaña LDP Interface, como nuestra el **Gráfico III.42** a continuación:

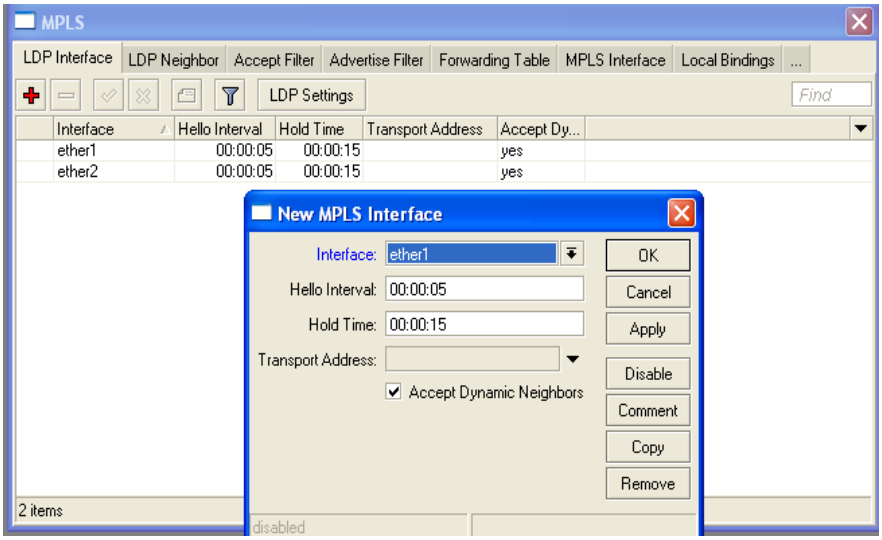


Gráfico III.42 Añadir Interfaces a la nube MPLS.

POR LÍNEAS DE CÓDIGO

A continuación se muestra la configuración de todos los Routers Mikrotik con protocolo MPLS.

R1

[admin@R1]> interface bridge add name=lobridge

[admin@R1]> ip address add address=192.168.255.1/32 interface=lobridge

[admin@R1]> mpls ldp set enabled=yes lsr-id=192.168.255.1 transport-address= 192.168.255.1

[admin@R1]> mpls ldp interface add interface=ether1

R2

[admin@R2]> interface bridge add name=lobridge

[admin@R2]> ip address add address=192.168.255.2/32 interface=lobridge

[admin@R2]> mpls ldp set enabled=yes lsr-id=192.168.255.2 transport-address=192.168.255.2

[admin@R2]> mpls ldp interface add interface=ether1

[admin@R2]> mpls ldp interface add interface=ether2

R3

[admin@R3]> interface bridge add name=lobridge

[admin@R3]> ip address add address=192.168.255.3/32 interface=lobridge

[admin@R3]> mpls ldp set enabled=yes lsr-id=192.168.255.3 transport-address=192.168.255.3

[admin@R3]> mpls ldp interface add interface=ether1

[admin@R3]> mpls ldp interface add interface=ether2

[admin@R3]> mpls ldp interface add interface=ether3

R4

[admin@R4]> interface bridge add name=lobridge

[admin@R4]> ip address add address=192.168.255.4/32 interface=lobridge

[admin@R4]> mpls ldp set enabled=yes lsr-id=192.168.255.4 transport-address=192.168.255.4

[admin@R4]> mpls ldp interface add interface=ether1

[admin@R4]> mpls ldp interface add interface=ether2

R5

[admin@R3]> interface bridge add name=lobridge

[admin@R3]> ip address add address=192.168.255.5/32 interface=lobridge

[admin@R3]> mpls ldp set enabled=yes lsr-id=192.168.255.5 transport-address=192.168.255.5

[admin@R3]> mpls ldp interface add interface=ether1

[admin@R3]> mpls ldp interface add interface=ether2

3.3.3.4 Configuración de QoS

En este apartado se implementa el marcado y clasificación de paquetes que se dan prioridad para el manejo del tráfico, de éste modo se aplica Calidad de Servicio (QoS) en los Routers Mikrotik.

- ***Manipulación y Clasificación de Tráfico***

Para manipular los tráficos y otorgarles QoS, se utilizan los procedimientos básicos de clasificación y asignación de prioridad.

Llega el momento de priorizar paquetes en nuestras redes con Mikrotik. Este proceso recibe el nombre de Calidad de Servicio QoS.

Cuando se implementa QoS, se dice que los paquetes de nuestra red son marcados. Esta marca se realiza en el campo TOS del paquete IP y es gracias a esta marca que podemos indicar a nuestro router que paquetes tienen más o menos prioridad.

Un ejemplo típico que hace referencia a cuando es conveniente implementar QoS, es cuando en nuestra red existe algún servicio de voz (VoIP o telefonía IP) y video. Esto se debe a que los paquetes de este tipo de servicio necesitan ser ¨despachados¨ de forma inmediata por nuestro router para lograr así la mejor calidad posible.

Aquí se presenta los comandos necesarios para dar solución a esta problemática. Las configuraciones necesarias a nuestro router son las siguientes:

Se ha diseñado un conjunto de políticas con el objetivo de evaluar la pérdida de paquetes y la variación del retardo para tráficos de alta prioridad (por ejemplo video) al momento de existir congestión en una de las interfaces un enrutador particular, debido a la utilización intensa del ancho de banda por tráficos no prioritarios (Ftp y Http).

Luego se configuró las reglas que limitan la tasa de transferencia de los tráficos de Video, y asigna los valores DSCP respectivos a los tráficos Web y Ftp que seleccionan implícitamente una de las cuatro colas de egreso en las interfaces del router.

- ***Configuración de reglas Mangle***

Se realizaron marcas en los paquetes para su proceso. Muchos otros medios en RouterOS hacen uso de estas marcas, por ejemplo los árboles de cola (queue trees), NAT, routing.

Marcar es la única manera de identificar paquetes dentro de los queues de árbol y puede ser usado como un clasificador para diferentes políticas de ruteo. Las marcas mangle sólo existen dentro del router, ellos no se transmiten por la red.

Adicionalmente, mangle facilita la modificación de algunos campos de la cabecera IP, como TOS (DSCP) y campo TTL.

- Se puede realizar el marcado de los paquetes basándose en:
- Dirección IP Origen y Destino

- Puerto Origen y Destino T
- Protocolo de transporte (TCP o UDP)
- Cabecera TOS / DS (ver **Gráfico III.43**)

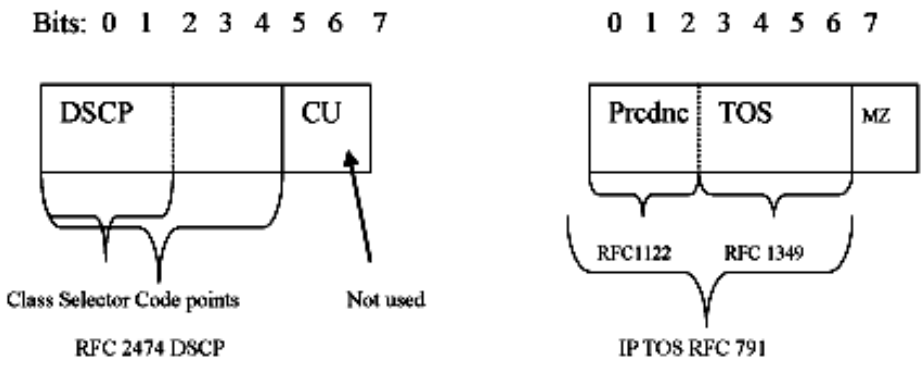


Gráfico III.43 Marcado de paquetes en los campos DSCP y TOS

Se accede a la herramienta Winbox para conectarse a máquina RouterOS, se hace clic en IP – Firewall del menú principal, se selecciona la pestaña MANGLE y añadimos una regla a la vez, con el botón  :

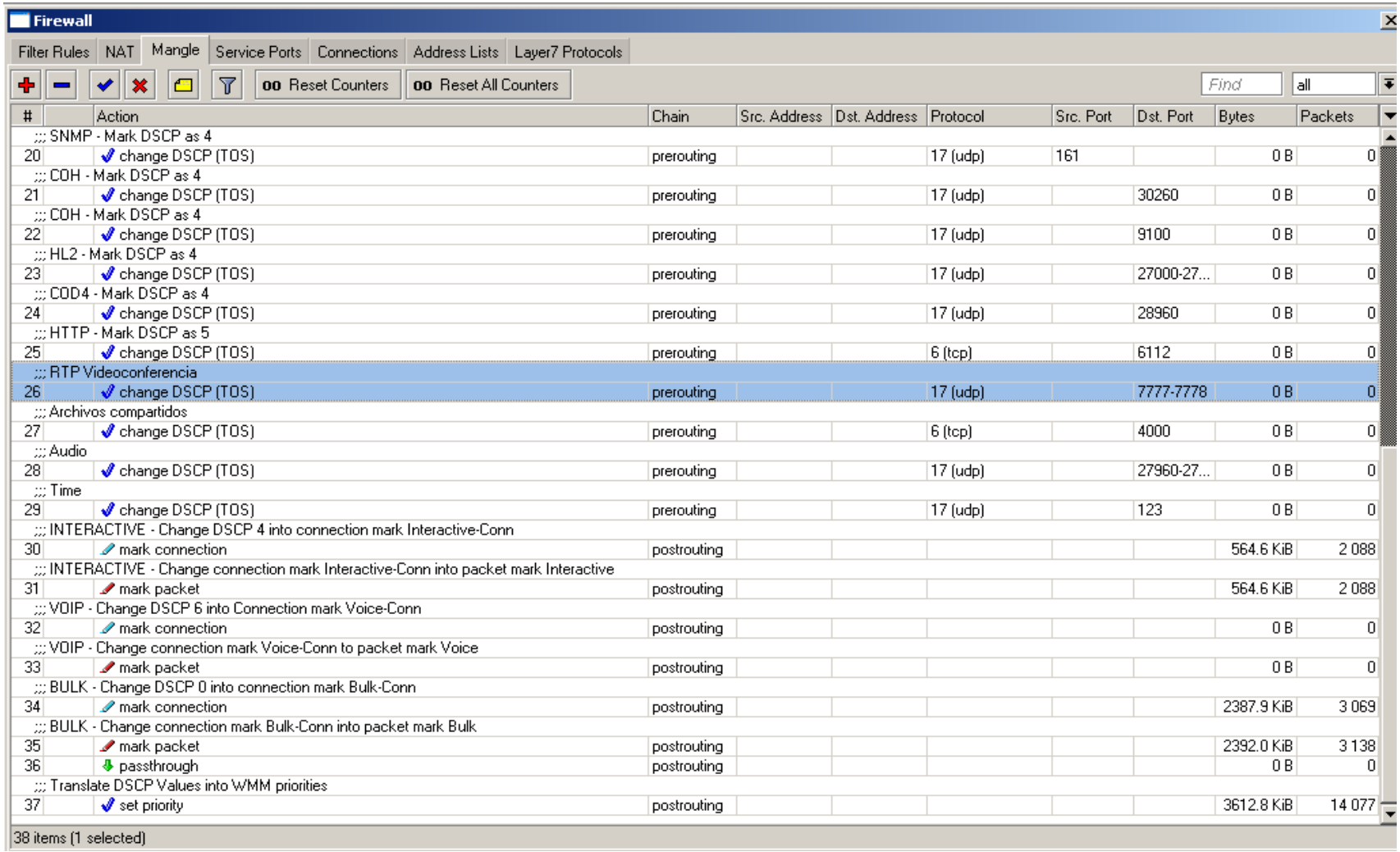


Gráfico III.44 Pantalla reglas Mangle para el marcado de paquetes

Para mayor entendimiento indicamos la configuración de las reglas mangle mediante líneas de código que pueden ser ejecutadas desde el terminal de Mikrotik:

En el **Gráfico III.44** nos muestra las configuraciones realizadas con Winbox, que se detalla a continuación por líneas de código:

/ip firewall mangle

```
 add action=change-dscp chain=prerouting comment="" disabled=no new-dscp=0

 add action=change-dscp chain=prerouting comment="ssh" disabled=no dst-port=22 new-dscp=4
protocol=tcp

 add action=change-dscp chain=prerouting comment="telnet" disabled=no dst-port=23 new-dscp=4
protocol=tcp

add action=change-dscp chain=prerouting comment="" disabled=no dst-port=5060 new-dscp=6
protocol=udp

 add action=change-dscp chain=prerouting comment="" disabled=no dst-port=4569 new-dscp=6
protocol=udp

 add action=change-dscp chain=prerouting comment="" disabled=no dst-port=53 new-dscp=4 protocol=udp

 add action=change-dscp chain=prerouting comment="" disabled=no dst-port=4569 new-dscp=6
protocol=tcp

 add action=change-dscp chain=prerouting comment="ospf" disabled=no new-dscp=4 protocol=ospf

 add action=change-dscp chain=prerouting comment="icmp" disabled=no new-dscp=4 protocol=icmp

add action=change-dscp chain=prerouting comment="" disabled=no dst-port=6668 new-dscp=4
protocol=tcp

 add action=change-dscp chain=prerouting comment="" disabled=no dst-port=6697 new-dscp=4
protocol=tcp

 add action=change-dscp chain=prerouting comment="" disabled=no dst-port=7324 new-dscp=4
protocol=tcp

 add action=change-dscp chain=prerouting comment="" disabled=no dst-port=7325 new-dscp=4
protocol=tcp

 add action=change-dscp chain=prerouting comment="" disabled=no dst-port=64738 new-dscp=6
protocol=tcp

 add action=change-dscp chain=prerouting comment="" disabled=no dst-address=10.10.10.1 dst-port=80
new-dscp=4 protocol=tcp
```

add action=change-dscp chain=prerouting comment="WINBOX - Mark DSCP as 4" disabled=no dst-port=8291 new-dscp=4 protocol=tcp

add action=change-dscp chain=prerouting comment="WINBOX - Mark DSCP as 4" disabled=no src-port=8291 new-dscp=4 protocol=tcp

add action=change-dscp chain=prerouting comment="SNMP - Mark DSCP as 4" disabled=no dst-port=161 new-dscp=4 protocol=udp

add action=change-dscp chain=prerouting comment="HTTP - Mark DSCP as 5" disabled=no src-port=161 new-dscp=2 protocol=udp

add action=change-dscp chain=prerouting comment="RTP - Videoconferencia as 5" disabled=no dst-port=27000-27065 new-dscp=1 protocol=udp

add action=change-dscp chain=prerouting comment=Quake3 disabled=no dst-port=27960-27965 new-dscp=4 protocol=udp

add action=mark-connection chain=postrouting comment="INTERACTIVE - Change DSCP 4 into connection mark Interactive-Conn" disabled=no\

dscp=4 new-connection-mark=Interactive-Conn passthrough=yes

add action=mark-packet chain=postrouting comment="INTERACTIVE - Change connection mark Interactive-Conn into packet mark Interactive"\

connection-mark=Interactive-Conn disabled=no new-packet-mark=Interactive passthrough=yes

add action=mark-connection chain=postrouting comment="VOIP - Change DSCP 6 into Connection mark Voice-Conn" disabled=no \

dscp=6 new-connection-mark=Voice-Conn passthrough=yes

add action=mark-packet chain=postrouting comment="VOIP - Change connection mark Voice-Conn to packet mark Voice"\

connection-mark=Voice-Conn disabled=no new-packet-mark=Voice passthrough=yes

add action=mark-connection chain=postrouting comment="BULK - Change DSCP 0 into connection mark Bulk-Conn" disabled=no\

dscp=0 new-connection-mark=Bulk-Conn passthrough=yes

add action=mark-packet chain=postrouting comment="BULK - Change connection mark Bulk-Conn into packet mark Bulk" \

connection-mark=Bulk-Conn disabled=no new-packet-mark=Bulk passthrough=yes

add action=passthrough chain=postrouting comment="" disabled=no dscp=4 ipv4-options=any

add action=set-priority chain=postrouting comment="Translate DSCP Values into WMM priorities" disabled=no new-priority=from-dscp passthrough=yes

- ***Configuración de Encolamiento***

QoS es implementado por un mecanismo de encolamiento. El Queuing maneja la manera en que los paquetes están esperando por su turno para salir de la interface.

Disciplinas de queueing controlan el orden y velocidad de los paquetes saliendo a través de la interface, adicionalmente define cuales paquetes deben esperar por su turno para ser enviados fuera y cuáles deben ser descargados.

- ***Queue Types***

Es la forma de hacer queues, pueden ser de 2 tipos:

- Tipo Scheduler: reordena el flujo de paquetes. Este tipo de disciplinas limitan el numero de paquetes esperando, no la velocidad
    - FIFO
    - RED
    - SFQ
- Tipo Shaper: controlan la velocidad del flujo de datos. Adicionalmente pueden hacer un trabajo programado
    - PCQ
    - HTB

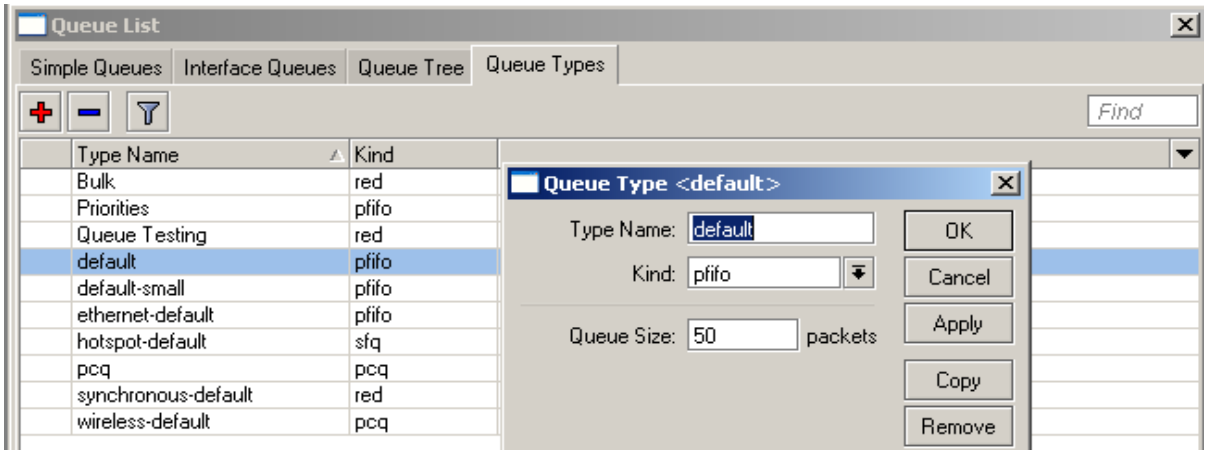


Gráfico III.45 Ventana configuración del Queue Type

En el **Gráfico III.45** se indica los parámetros de configuración de un queue type.

Puedes configurar las propiedades de queue con la línea de comando:

/queue type

set default kind=pfifo name=default pfifo-limit=50

set ethernet-default kind=pfifo name=ethernet-default pfifo-limit=50

set wireless-default kind=pcq name=wireless-default pcq-classifier=src-address,dst-address pcq-limit=50 pcq-rate=0 pcq-total-limit=2000

set synchronous-default kind=red name=synchronous-default red-avg-packet=1000 red-burst=20 red-limit=60 red-max-threshold=50 red-min-threshold=10

set hotspot-default kind=sfq name=hotspot-default sfq-allot=1514 sfq-perturb=5

add kind=pfifo name=Priorities pfifo-limit=10

add kind=red name="Queue Testing" red-avg-packet=1000 red-burst=20 red-limit=60 red-max-threshold=50 red-min-threshold=10

add kind=pcq name=pcq pcq-classifier="" pcq-limit=50 pcq-rate=0 pcq-total-limit=2000

add kind=red name=Bulk red-avg-packet=1000 red-burst=20 red-limit=60 red-max-threshold=50 red-min-threshold=10

set default-small kind=pfifo name=default-small pfifo-limit=10

- ***Queue Tree***

Queues de Árbol son más sofisticadas maneras de manejar el tráfico. Ellas permiten construir “hierarchy de clases” a la medida.

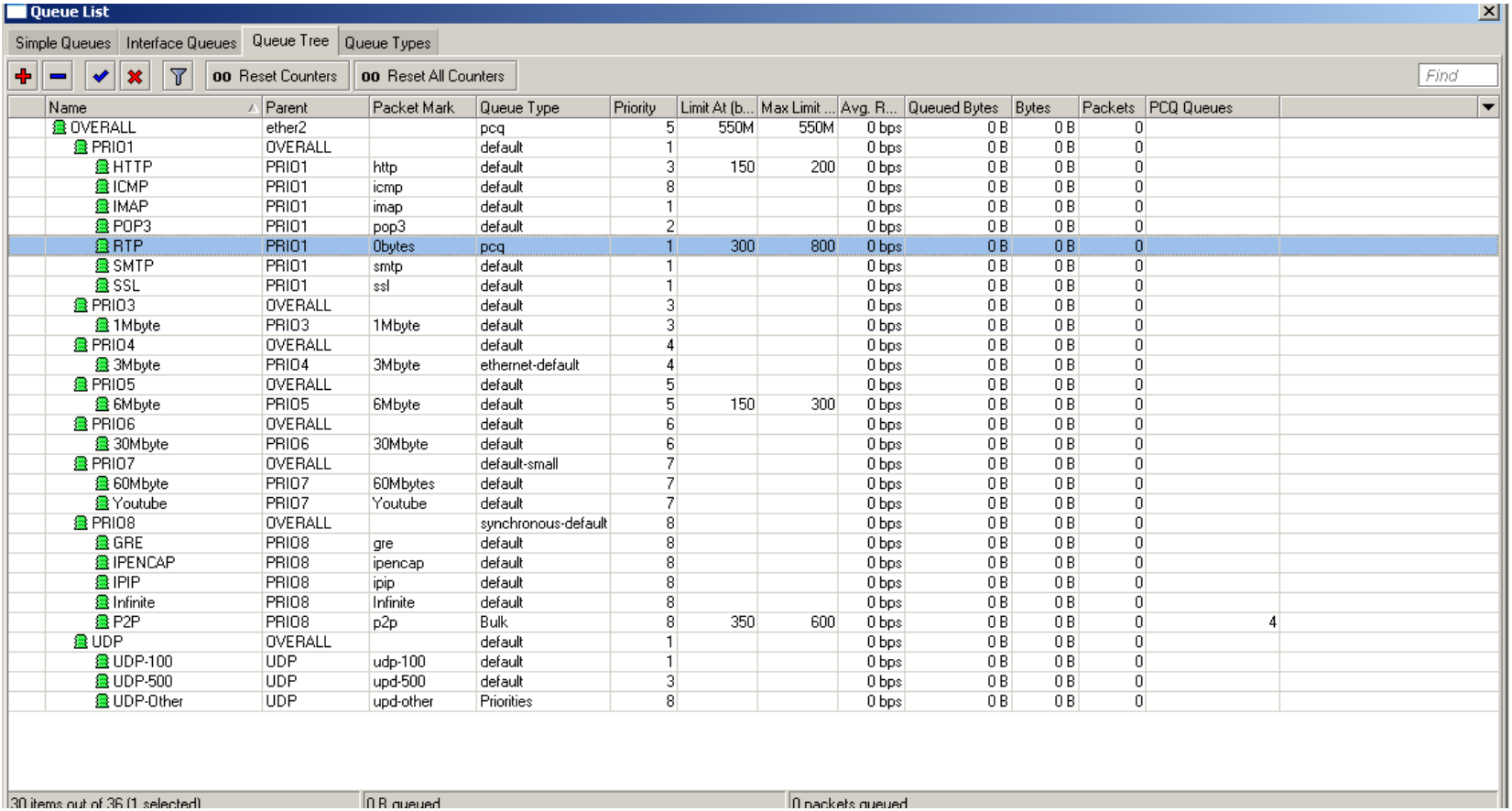
Filtros de queues de árbol son aplicados en la interface especificada (ver **Gráfico III.46**). Los filtros son solamente marcas que el firewall hace a los flujos de paquetes en la opción “mangle”, los filtros “ven” las direcciones de los paquetes como si arribaran al router

Los filtros en las interfaces “global-in” and “global-out” son ejecutadas antes que los filtros simples. Se hace notar que los queues simples están separados en 2 partes – 'direct' (en “global-out”) y 'reverse' (en “global-in”).

Queues simples son la manera más fácil de controlar las velocidades de los clientes. Ellas permiten manejar rx, tx y velocidades agregadas justo solo con una entrada.

Vamos a generar varios niveles de Prioridades para los flujos:

- ICMP
- Tráfico Interactivo RTP (Videoconferencia)
- Aplicaciones especiales (Escritorio Remoto / VNC / etc)
- HTTP
- SMB/ CIFS



Name	Parent	Packet Mark	Queue Type	Priority	Limit At (b...	Max Limit ...	Avg. R...	Queued Bytes	Bytes	Packets	PCQ Queues
OVERALL	ether2		pcq	5	550M	550M	0 bps	0 B	0 B	0	
PRIO1	OVERALL		default	1			0 bps	0 B	0 B	0	
HTTP	PRIO1	http	default	3	150	200	0 bps	0 B	0 B	0	
ICMP	PRIO1	icmp	default	8			0 bps	0 B	0 B	0	
IMAP	PRIO1	imap	default	1			0 bps	0 B	0 B	0	
POP3	PRIO1	pop3	default	2			0 bps	0 B	0 B	0	
RTP	PRIO1	0bytes	pcq	1	300	800	0 bps	0 B	0 B	0	
SMTP	PRIO1	smtp	default	1			0 bps	0 B	0 B	0	
SSL	PRIO1	ssl	default	1			0 bps	0 B	0 B	0	
PRIO3	OVERALL		default	3			0 bps	0 B	0 B	0	
1Mbyte	PRIO3	1Mbyte	default	3			0 bps	0 B	0 B	0	
PRIO4	OVERALL		default	4			0 bps	0 B	0 B	0	
3Mbyte	PRIO4	3Mbyte	ethernet-default	4			0 bps	0 B	0 B	0	
PRIO5	OVERALL		default	5			0 bps	0 B	0 B	0	
6Mbyte	PRIO5	6Mbyte	default	5	150	300	0 bps	0 B	0 B	0	
PRIO6	OVERALL		default	6			0 bps	0 B	0 B	0	
30Mbyte	PRIO6	30Mbyte	default	6			0 bps	0 B	0 B	0	
PRIO7	OVERALL		default-small	7			0 bps	0 B	0 B	0	
60Mbyte	PRIO7	60Mbytes	default	7			0 bps	0 B	0 B	0	
Youtube	PRIO7	Youtube	default	7			0 bps	0 B	0 B	0	
PRIO8	OVERALL		synchronous-default	8			0 bps	0 B	0 B	0	
GRE	PRIO8	gre	default	8			0 bps	0 B	0 B	0	
IPENCAP	PRIO8	ipencap	default	8			0 bps	0 B	0 B	0	
IPIP	PRIO8	ipip	default	8			0 bps	0 B	0 B	0	
Infinite	PRIO8	Infinite	default	8			0 bps	0 B	0 B	0	
P2P	PRIO8	p2p	Bulk	8	350	600	0 bps	0 B	0 B	0	4
UDP	OVERALL		default	1			0 bps	0 B	0 B	0	
UDP-100	UDP	udp-100	default	1			0 bps	0 B	0 B	0	
UDP-500	UDP	upd-500	default	3			0 bps	0 B	0 B	0	
UDP-Other	UDP	upd-other	Priorities	8			0 bps	0 B	0 B	0	

Gráfico III.46 Pantalla reglas Queue Tree para priorización del tráfico

También pueden ser configuradas por medio de líneas de comando y ser ejecutadas desde el terminal de Winbox, que de detalla a continuación:

/queue tree

```
add limit-at=550000000 max-limit=550000000 name=OVERALL parent=ether2 priority=5
        add name=PRIO1 parent=OVERALL priority=1
                add name=0-512 packet-mark=0bytes parent=PRIO1 priority=1
                add name=ICMP packet-mark=icmp parent=PRIO1 priority=8
                add name=POP3 packet-mark=pop3 parent=PRIO1 priority=1
                add name=RTP packet-mark=smtp parent=PRIO1 priority=2
                add name=IMAP packet-mark=imap parent=PRIO1 priority=1
                add name=HTTP packet-mark=http parent=PRIO1 priority=1
                add name=SSL packet-mark=ssl parent=PRIO1 priority=1
                add name=MSN-MESSENGER packet-mark=msn-messenger parent=PRIO1 priority=1
        add name=PRIO3 parent=OVERALL priority=3
                add name=1Mbyte packet-mark=1Mbyte parent=PRIO3 priority=3
        add name=PRIO4 parent=OVERALL priority=4
                add name=3Mbyte packet-mark=3Mbyte parent=PRIO4 priority=4
        add name=PRIO5 parent=OVERALL priority=5
                add name=6Mbyte packet-mark=6Mbyte parent=PRIO5 priority=5
        add name=PRIO6 parent=OVERALL priority=6
                add name=30Mbyte packet-mark=30Mbyte parent=PRIO6 priority=6
        add name=PRIO7 parent=OVERALL priority=7
                add name=Youtube packet-mark=Youtube parent=PRIO7 priority=7
                queue=Youtube_down
                add name=60Mbyte packet-mark=60Mbytes parent=PRIO7 priority=7
        add name=PRIO8 parent=OVERALL priority=8
```

```
                add name=Infinite packet-mark=Infinite parent=PRIO8 priority=8
                add name=GRE packet-mark=gre parent=PRIO8 priority=8
                add name=P2P packet-mark=p2p parent=PRIO8 priority=8
                add name=IPENCAP packet-mark=ipencap parent=PRIO8 priority=8
                add name=IPIP packet-mark=ipip parent=PRIO8 priority=8
        add name=UDP parent=OVERALL priority=1
                add name=UDP-100 packet-mark=udp-100 parent=UDP priority=1
                add name=UDP-500 packet-mark=upd-500 parent=UDP priority=3
                add name=UDP-Other packet-mark=upd-other parent=UDP priority=8
add disabled=yes limit-at=22000000 max-limit=22000000 name=PRIO8-19h parent=INTERNAL priority=3
        add name=Infinite-19h packet-mark=Infinite parent=PRIO8-19h priority=8
        add name=P2P-19h packet-mark=p2p parent=PRIO8-19h priority=8
        add name=GRE-19h packet-mark=gre parent=PRIO8-19h priority=8
        add name=IPENCAP-19h packet-mark=ipencap parent=PRIO8-19h priority=8
        add name=IPIP-19h packet-mark=ipip parent=PRIO8-19h priority=8
        add name=IPSEC-AH-19h packet-mark=ipsec-ah parent=PRIO8-19h priority=8
        add name=IPSEC-ESP-19h packet-mark=ipsec-esp parent=PRIO8-19h priority=8
```

CAPÍTULO IV

ANÁLISIS DE RESULTADOS

4.1 Introducción

En este capítulo se pone a consideración el análisis de los resultados obtenidos a través del desarrollo del proyecto de tesis, los mismos que sirven también para la comprobación de la hipótesis. Para esto se ha trabajado sobre los 2 escenarios desarrollados el primero la construcción de la red con el protocolo OSPF, y el segundo la red OSPF con MPLS los resultados se obtuvieron a partir del uso de tres herramientas de medición de tráfico y análisis de paquetes: Whireshark 1.2.6, Colasoft 6.9 Enterprise Edition y Observer Suite 10.0.

4.2 Captura de Tráfico y Análisis de Paquetes

Se transmitió durante 5 minutos tráfico sobre los dos escenarios planteados el primero OSPF sin MPLS, y el otro sobre el escenario OSPF con MPLS obteniéndose la captura de los siguientes paquetes en los sniffer whireshark y colasoft, clasificados según el tipo de tráfico enviado. Se muestra las diferentes capturas de los paquetes generados por los diversos tipos de tráfico en el escenario planteado (ver **Gráfico I.1**).

4.2.1 Aplicaciones Real Time

Se realizó transmisiones de video en tiempo real bajo el esquema cliente/servidor para evaluar el desempeño de la red en los dos escenarios planteados, para este tipo de aplicación utilizamos la herramienta netmeeting 3.01 para el establecimiento de la video conferencia

Se analiza la cabecera del campo IP al enviar una Videoconferencia implementando MPLS en la red, basándonos en la especificación del formato de la cabecera ip que se lo puede encontrar en el **RFC 0791,** vemos que el campo de Differentiated Services Codepoint tiene el siguiente valor:

Ocho bits: 0110 0000

Bits 0-2: Prioridad.

Bit 3: 0 = Demora Normal, 1 = Baja Demora.

Bit 4: 0 = Rendimiento Normal, 1 = Alto rendimiento.

Bit 5: 0 = Fiabilidad Normal, 1 = Alta fiabilidad.

Bits 6-7: Reservado para uso futuro.

0	1	1	0	0	0	0	0
Prioridad	Prioridad	Baja Demora					

Tabla III.4 Tabla análisis cabecera ip de un paquete RTP.

Se puede observar que al clasificar y priorizar el tráfico (ver **Gráfico IV.46**), en éste caso para el tráfico RTP tenemos una alta prioridad y una baja demora, garantizando así la QoS.

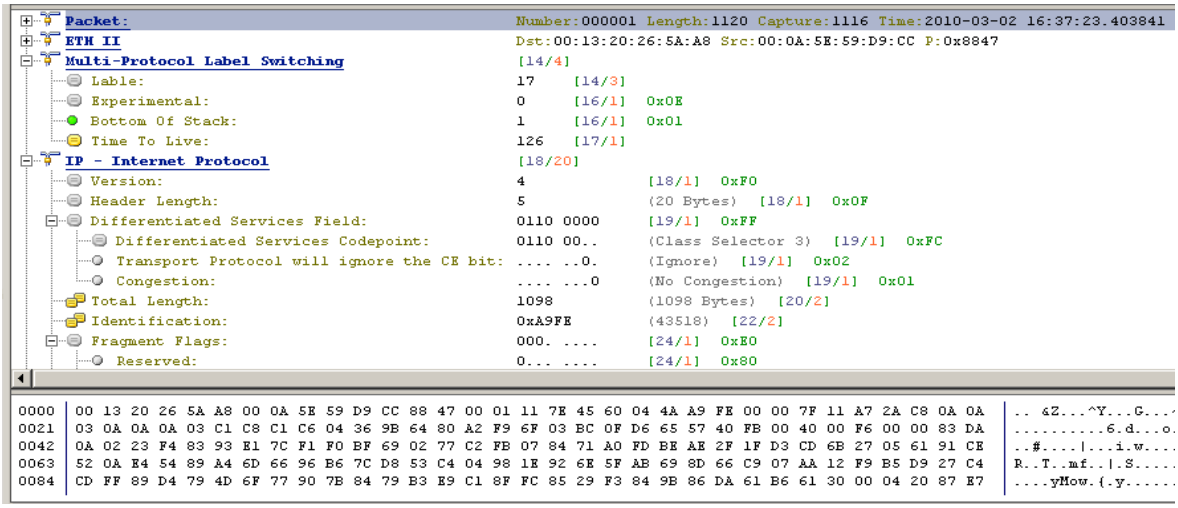


Gráfico IV.47 Captura de paquetes RTP aplicando MPLS, en sniffer Colasoft

4.2.2 Página Web

Se alojo una página web en el servidor Apache para realizar las pruebas de transmisión de los paquetes de tipo HTTP, para el evaluar el desempeño de la red con la implementación del escenario planteado.

Ocho bits: 0000 0000

Bits 0-2: Prioridad.

Bit 3: 0 = Demora Normal, 1 = Baja Demora.

Bit 4: 0 = Rendimiento Normal, 1 = Alto rendimiento.

Bit 5: 0 = Fiabilidad Normal, 1 = Alta fiabilidad.

Bits 6-7: Reservado para uso futuro.

0	0	0	0	0	0	0	0
Prioridad	Prioridad	Baja Demora					

Tabla III.5 Tabla análisis cabecera ip de un paquete Http.

Para el tráfico generado por peticiones http (ver **Gráfico IV. 48**), se observa que no posee prioridad y tiene una demora normal, según se comprueba con la configuración realizada al dar privilegio al tráfico generado por Videoconferencia.

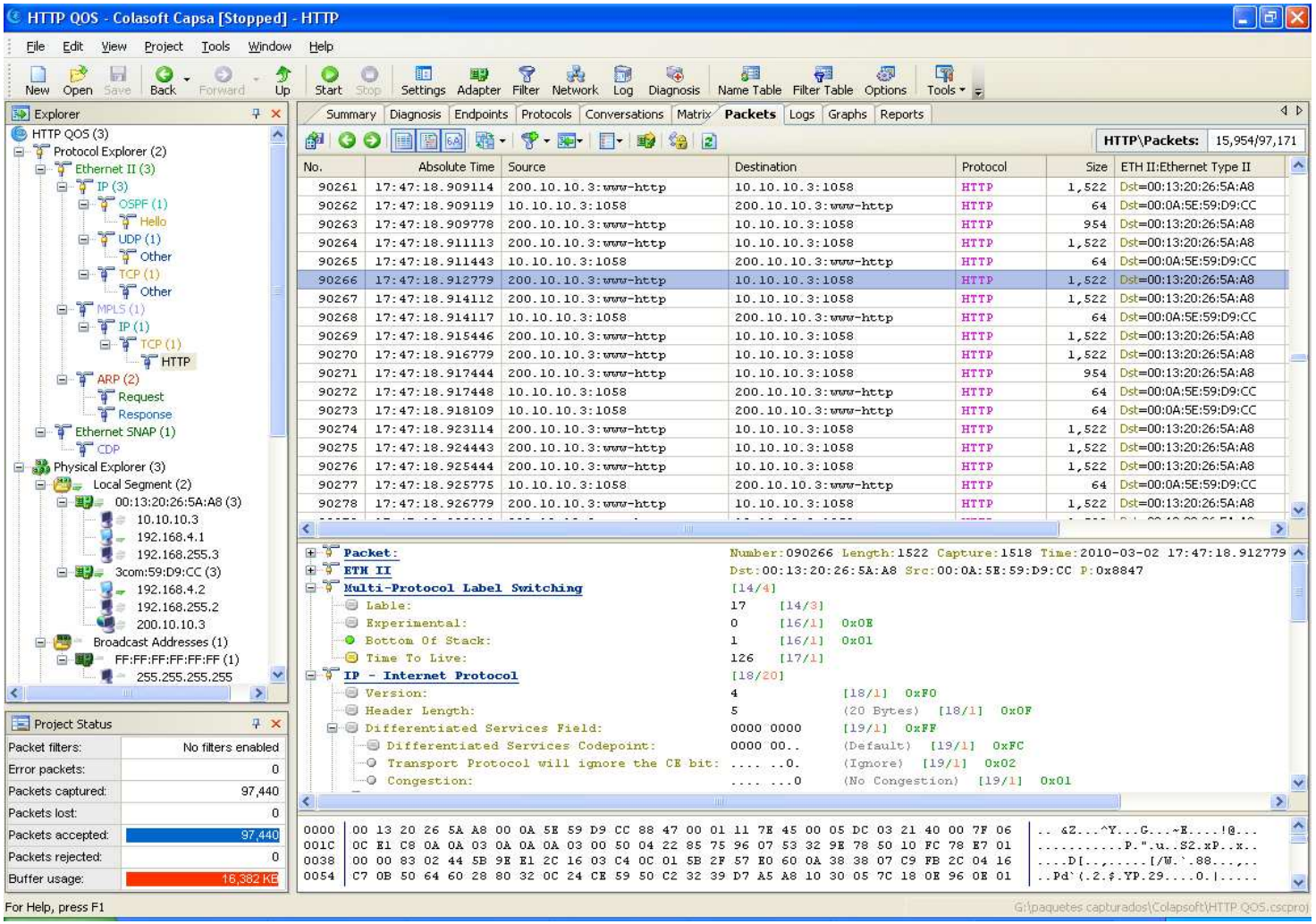


Gráfico IV.48 Captura de paquetes Http aplicando MPLS, en sniffer Colasoft

4.2.3 Protocolo ICMP

Para el análisis de este protocolo se genero tráfico a través de un ping (ver **Gráfico IV. 49**) desde la maquina cliente 10.10.10.3 hacia el servidor 200.10.10.3.

Ocho bits: 0000 0000

Bits 0-2: Prioridad.

Bit 3: 0 = Demora Normal, 1 = Baja Demora.

Bit 4: 0 = Rendimiento Normal, 1 = Alto rendimiento.

Bit 5: 0 = Fiabilidad Normal, 1 = Alta fiabilidad.

Bits 6-7: Reservado para uso futuro.

0	0	0	0	0	0	0	0
Prioridad	Prioridad	Baja Demora					

Tabla III.6 Tabla análisis cabecera ip de un paquete Icmp.

No se le dio prioridad a éste tipo de tráfico, por tal razón sus valores permanecen en 0, tal como muestra la **Tabla III.6.**

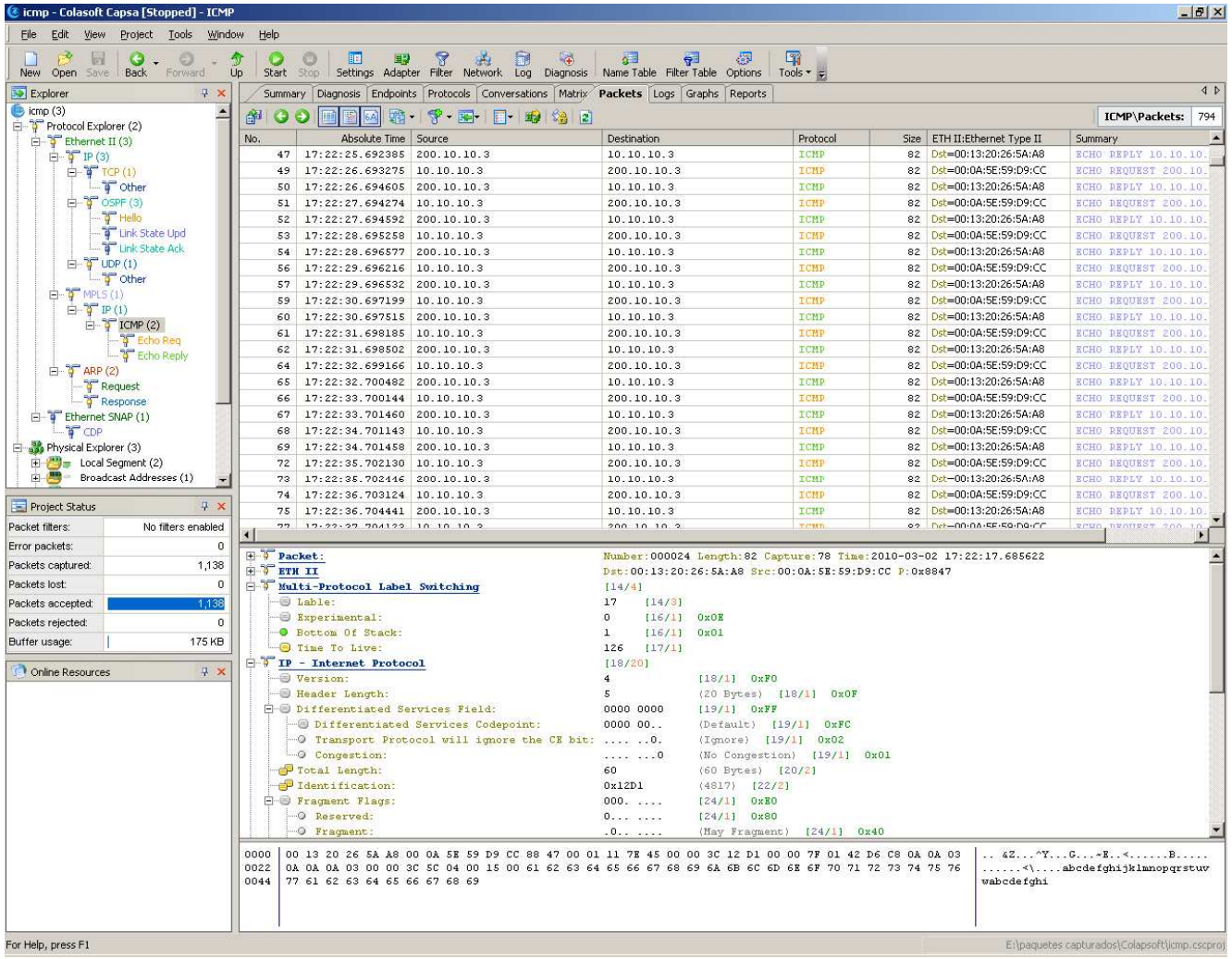


Gráfico IV.49 Captura de paquetes ICMP aplicando MPLS, en sniffer Colasoft

4.2.4 Protocolo CIFS (Common Internet File System)

CIFS es el nombre que adoptó Microsoft en 1998 para el protocolo SMB.

(Server Message Block). Protocolo de red (que pertenece a la capa de aplicación en el modelo OSI, ver **Gráfico II.2**) que permite compartir archivos, impresoras, y demás recursos entre nodos de una red. Se usa principalmente en computadoras con Windows y nos permitirá el análisis de los paquetes generados (ver **Gráfico IV. 50**) a través de la compartición de archivos en el escenario planteado.

Ocho bits: 0000 0000

Bits 0-2: Prioridad.

Bit 3: 0 = Demora Normal, 1 = Baja Demora.

Bit 4: 0 = Rendimiento Normal, 1 = Alto rendimiento.

Bit 5: 0 = Fiabilidad Normal, 1 = Alta fiabilidad.

Bits 6-7: Reservado para uso futuro.

0	0	0	0	0	0	0	0
Prioridad	Prioridad	Baja Demora					

Tabla III.7 Tabla análisis cabecera ip de un paquete Icmp.

De igual forma observamos que al no dar prioridad a este tipo de tráfico los valores permanecen en 0, como indica la **Tabla III.7.**

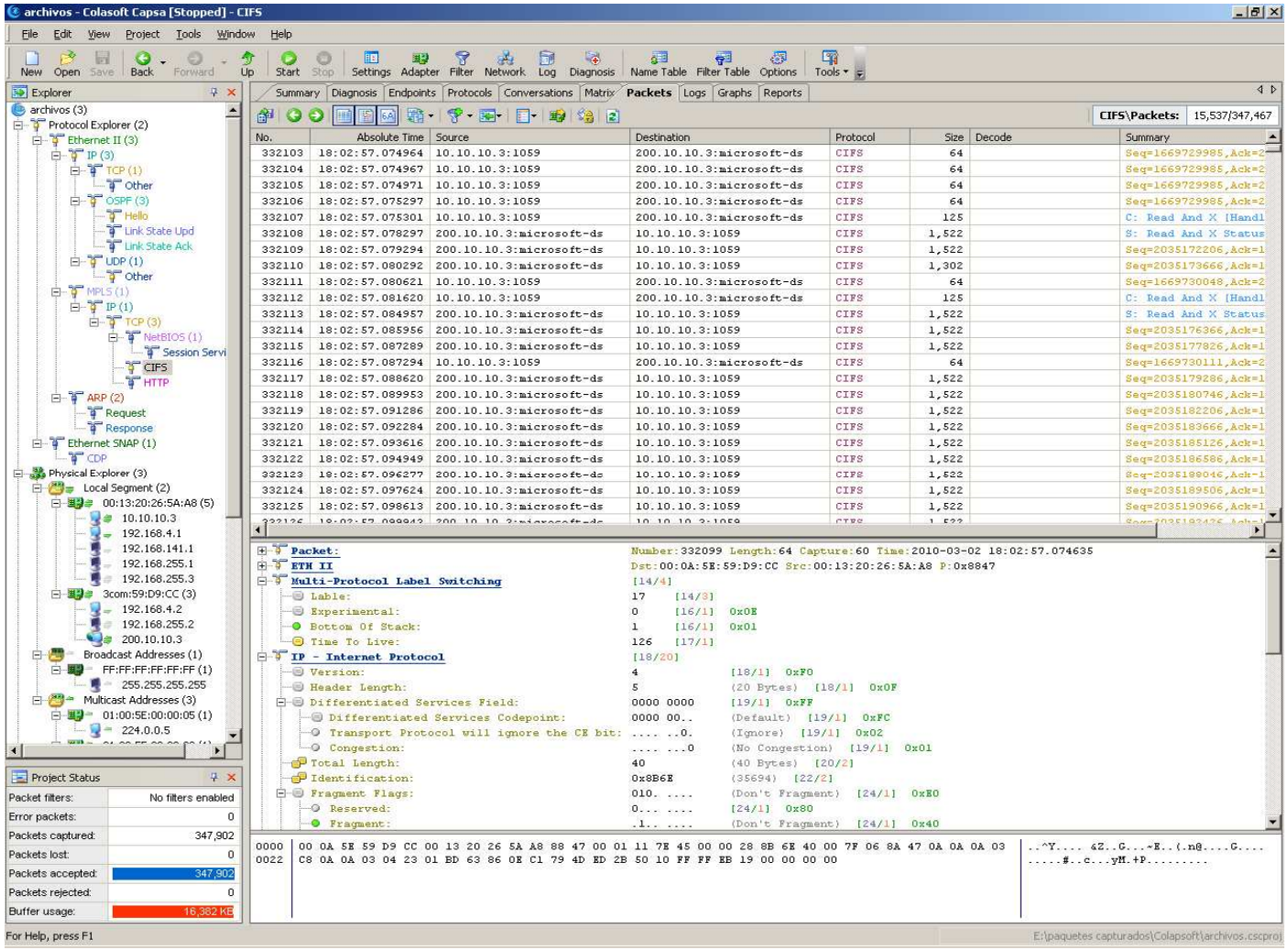


Gráfico IV.50 Captura de paquetes CIFS aplicando MPLS, en sniffer Colasoft

4.3 Metodología y Parámetros de Medición

El tipo de medición realizado para la evaluación del escenario y análisis de los protocolos es el tipo activo, intrusivo y extremo a extremo.

Es decir, se inyecta un tráfico generado a partir de aplicaciones en tiempo real, utilizando herramientas como: netmeeting 3.01 para el establecimiento de una Videoconferencia, un servidor apache para alojar páginas web, de esta manera se inserta tráfico artificial a la red para la generación de protocolos y estudio de cabeceras.

Para la medición del tráfico y los paquetes se utilizaron dos herramientas: el sniffer Wireshark 1.2.6 que es un analizador de tráfico de red, el sniffer Colasoft Capsa 6.9 Enterprise Edition que es un monitor de tráfico de red en tiempo real.

4.3.1 Determinación y Descripción de los Parámetros de Medición

En este apartado se analizan los parámetros que determinan la QoS en una red, y que será un factor muy importante para el desarrollo de la tesis.

4.3.1.1 Parámetro 1: Ancho de Banda

El ancho de banda es la media del número de bits por segundo que pueden ser transmitidos correctamente a través de la red. El caudal de medida suele encontrarse desde Kbps ó Mbps hasta Gbps2.

4.3.1.2 Parámetro 2: Retardo Punto a Punto

Es el tiempo medio acumulado durante el trayecto de un paquete para atravesar la red de un punto a otro. Para medir con exactitud el retardo, se deben tener en cuenta los puntos donde éste se produce:

Retardo de propagación. Es el retardo que se obtiene del tiempo que tarda la luz en recorrer la fibra óptica por la que se transmite. El retardo medio suele ser del orden de 5m/s por cada 10.000Km aunque puede variar en función de los eventos que se sucedan sobre el medio de transmisión.

Retardo de conmutación. Se produce por el tiempo consumido en el procesado realizado para cambiar el enlace por el que un paquete ha entrado al router.

Retardo de clasificación (scheduling). El retardo de scheduling o queueing se debe a la acción de clasificar el tráfico en las diferentes colas de los equipos de red. Desde el momento en el que un paquete llega a una cola, se decide cual es su clase correspondiente, se añade a esa cola y luego, se vuelve a transmitir a la salida de la cola se sucede un retardo en la transmisión. Según el tipo de algoritmo utilizado para la clasificación del tráfico este tiempo pude sufrir variaciones.

Retardo de serialización. El retardo de serialización aparece cuando un paquete es adaptado a un medio por el cual se va a transmitir. La velocidad de ese mismo medio y el tamaño del paquete son determinantes para este retardo.

4.3.1.3 Parámetro 3: Pérdida de Paquetes

La pérdida de paquetes es medida como un porcentaje de los paquetes transmitidos. Son los paquetes que siendo enviados nunca llegan a su destino. Los motivos que provocan una pérdida de paquetes son múltiples siendo la congestión el primer causante de ello. Concretamente, el límite de capacidad de los buffers de los dispositivos de red es el punto donde se registra el problema. A esto se añade, la retransmisión realizada por las aplicaciones cuando detectan que los paquetes no llegan.

Una alternativa para evitar esta pérdida de paquetes es disponer de una velocidad de salida de datos mayor que la de entrada. Esta opción es en la mayoría de los casos inviable por el coste que supone. Siendo así, las medidas a tomar son más propias de la naturaleza de las comunicaciones, proponiendo utilizar UDP en vez de TCP, o incluso observando que algunas aplicaciones son tolerantes con un cierto porcentaje de pérdida de paquetes.

4.3.1.4 Parámetro 4: Jitter

Variación del retardo punto a punto de los paquetes causada por la clasificación y los retardos de acceso en el nodo fuente, y por el retardo de los nodos de tránsito y el buffer del nodo de recepción. Las variaciones que suceden durante estos procesos, por no tener comportamientos fijos, son los causantes de la aparición del jitter.

Para muchas aplicaciones multimedia el jitter puede tener un efecto más dañino que un alto retardo de transmisión.

4.3.2 Determinación de los indicadores de los parámetros de medición

A continuación se muestra algunos de los indicadores que determinan los parámetros que garantizan la QoS.

4.3.2.1 Parámetro 1: Ancho de Banda

Bits transmitidos

Paquetes Recibidos

Paquetes Transmitidos

Tráfico Generado

4.3.2.2 Parámetro 2: Retardo Punto a Punto

Búsqueda en las tablas de ruteo

Calidad de Imagen

Aplicaciones Multimedia

4.3.2.3 Parámetro 3: Pérdida de Paquetes

Paquetes Perdidos

Paquetes Aceptados

Paquetes Filtrados

4.3.2.4 Parámetro 4: Jitter

Uso del buffer

Retardo

Velocidad de Transmisión

4.4 Criterios de evaluación de QoS

El objetivo fue comprobar la distribución de ancho de banda en caso de congestión, así como observar la variación del retardo o jitter, el retraso punto a punto y la pérdida de paquetes.

Se utilizaron cuatro flujos de tráfico, que reflejan los que comúnmente circulan por la red: Video, Http, Smb /Cifs e Icmp. Durante 5 minutos se transmitió tráfico de Video, seguidamente se transmitió tráfico Http por 3 minutos, en el minuto 8 y por 2 minutos se transmitió tráfico Smb/Cifs y por último en el minuto 10 y por 1 minuto, se transmitió tráfico Icmp; para los escenarios configurados sólo con ruteo OSPF y otro aplicando MPLS corriendo con OSPF.

4.4.1 ESCENARIO OSPF

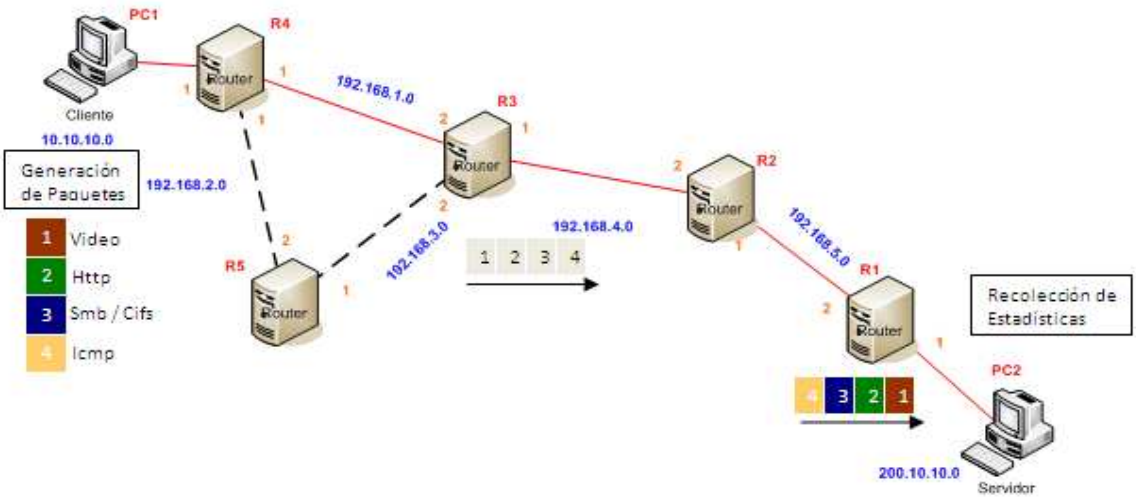


Gráfico IV.51 Evaluación del tráfico OSPF

En el **Gráfico IV. 51** se observa el escenario formada por los 5 PC Router Mikrotik y las máquinas cliente y servidor, al generar tráfico por la red, se observa que al utilizar OSPF toma el camino o la ruta más corta, pasando por las máquinas Router: R4, R3, R2 y R1 hasta llegar al servidor donde se gestionan las peticiones del cliente.

4.4.1.1 Ancho de Banda

En el enrutamiento de tráfico proposionado por OSPF, observamos como se distribuye el ancho de banda para el consumo del tráfico en la red, siendo los picos más altos a partir del minuto 5 con, donde se empezó a generar peticiones al servidor Web y en la compartición de archivos. El uso de éste protocolo no reserva ancho de banda ni asigna prioridad al tráfico de datos, el **Gráfico IV.52** nos lo indica a continuación:

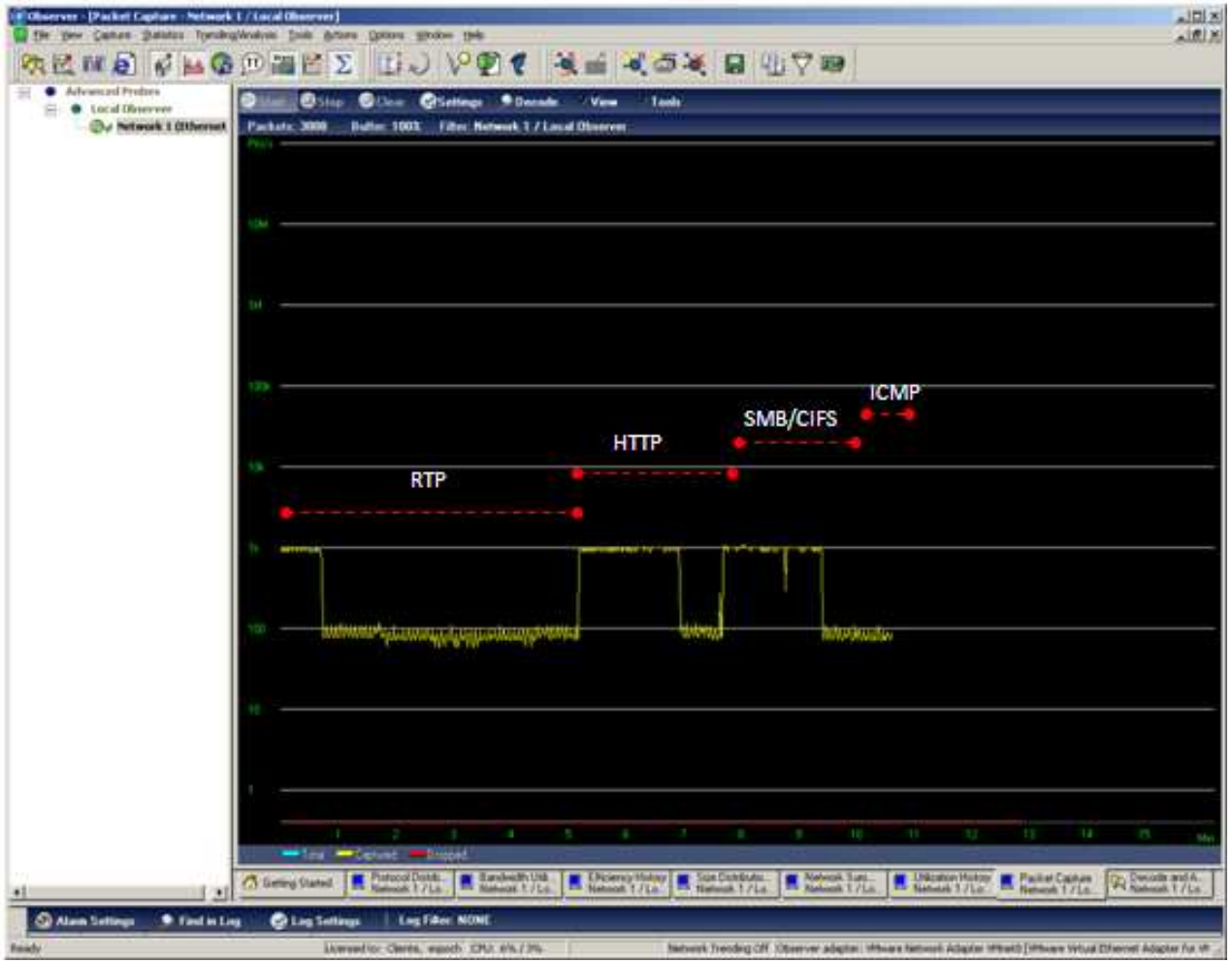


Gráfico IV.52 Ventana distribución de Ancho de Banda en la captura de tráfico con OSPF

4.4.1.2 Retardo Punto a Punto

Se observa los resultados obtenidos de las pruebas realizadas, en el cual indica la agrupación de los datos es en función de su tiempo de respuesta, indicando el retardo o delay descrito en milisegundos.

Se analizan los saltos por los que tienen que pasar los paquetes hasta llegar a su destino, mediante el comando *tracer* en símbolo del sistema (ver **Gráfico IV.53)**:

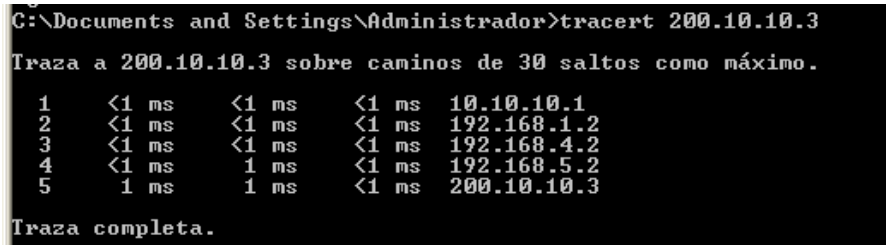


Gráfico IV.53 Comando tracer en simbolo del sistema

Para los distintos tráficos se puede observar que existe altos tiempos de respuesta para el tráfico TCP(Http y Smb/Cifs), mientras que el tráfico UDP (Rtp) son casi imperceptibles los tiempos de respuesta, pues existe una agrupación de los datos con un porcentaje aproximadamente alto, el **Gráfico IV.54** lo indica a continuación:

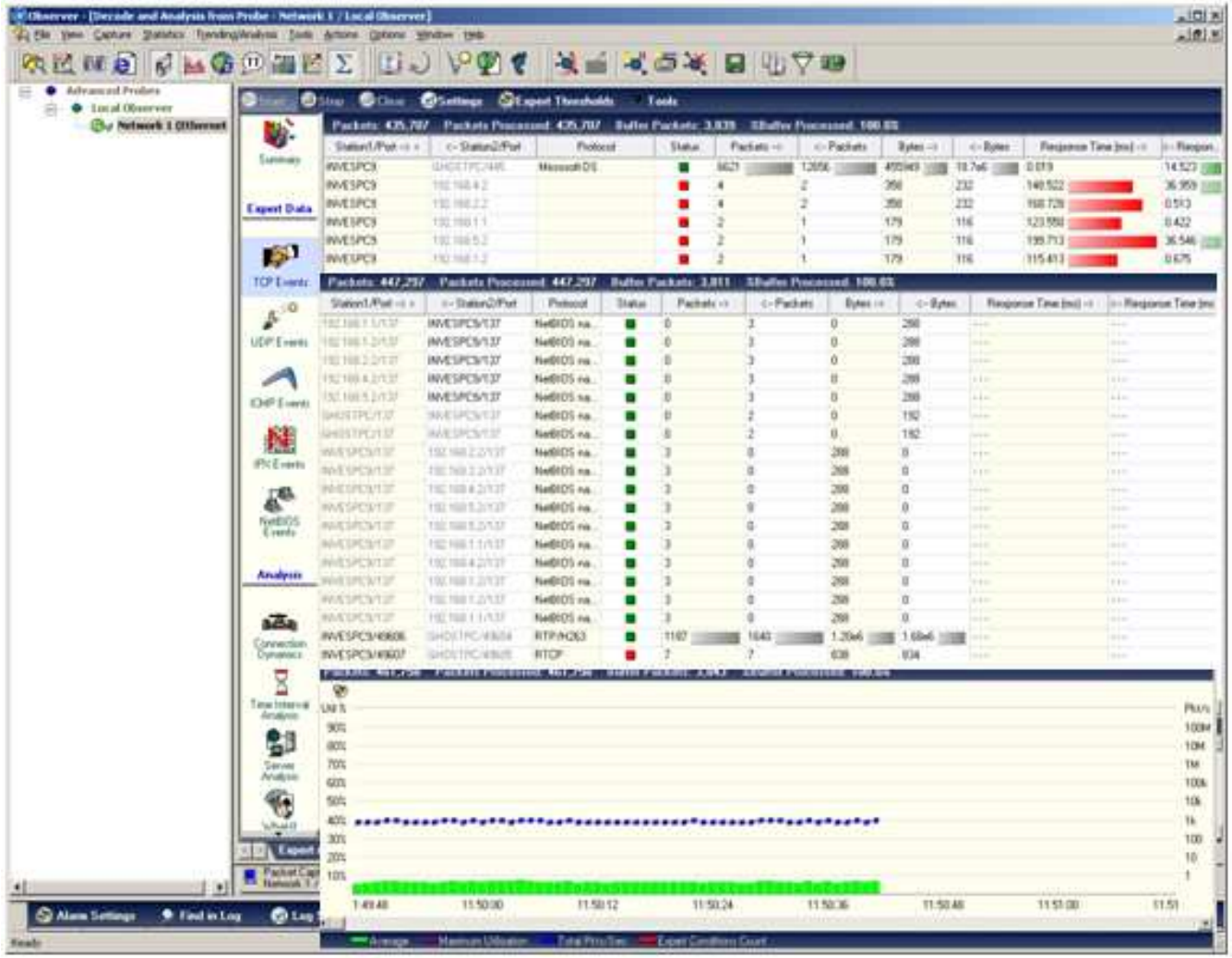


Gráfico IV.54 Ventana captura de tazas de tráfico en la captura de tráfico con OSPF

4.4.1.3 Jitter

Para el anális del jitter se lo hará con el tráfico generado por el Protocolo RTP (Videoconferencia), de un tiempo total de 5min. En la transmisión de retorno los picos máximos son aproximadamente de 56,53ms en un 45% del jitter total, el 25% del jitter está sobre los 25 ms y el 30% se encuentra bajo los 40 ms. Mientras que en la transmisión de ida los picos máximos son de 48,71ms, el 85% del jitter se encuentra por sobre los 25 ms y el 15% se encuentra sobre los 40 ms.

En este perfil se puede determinar que en la transmisión de retorno existe una perdida mayor con respecto a la transmisión de ida en un tiempo aproximado de 5,2min, lo que se puede observar en el **Gráfico IV. 55,** donde el pico más alto se alcanza en el segundo 312 que se muestra a continuación:

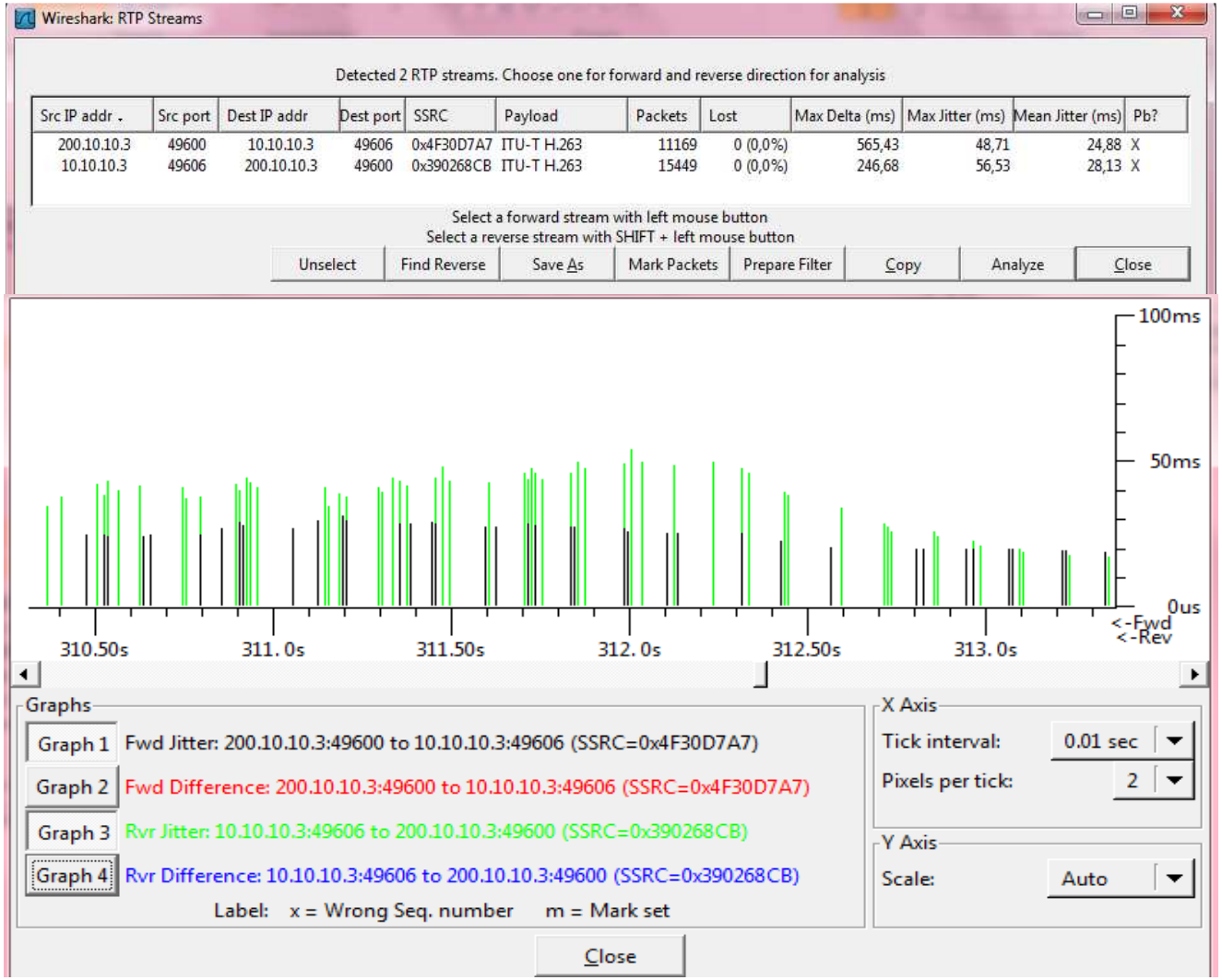


Gráfico IV.55 Ventana Jitter de RTP en la captura de tráfico con OSPF

4.4.1.4 Pérdida de Paquetes

En la transmisión de tráfico de la red con protocolo OSPF se puede observar los valores y tazas de utilización de bytes, bits, paquetes, bits por segundo, paquetes por segundo, promedios de utilización de bytes y bits; siendo mayor la utilización a partir de un tamaño 1518 paquetes ocupando un 65,1%. El 4,9% usado por paquetes de tamaño 512-1023, seguido del 4,3% usado lo ocupa paquetes de tamaño entre 1024-1517, el resto oscilan entre tamaño de 64-511.

En la tabla inferior vemos que se generó una pérdida total de 33,621 paquetes además del uso del buffer 16,382 KB, a continuación de detalla en el **Gráfico IV. 56**:

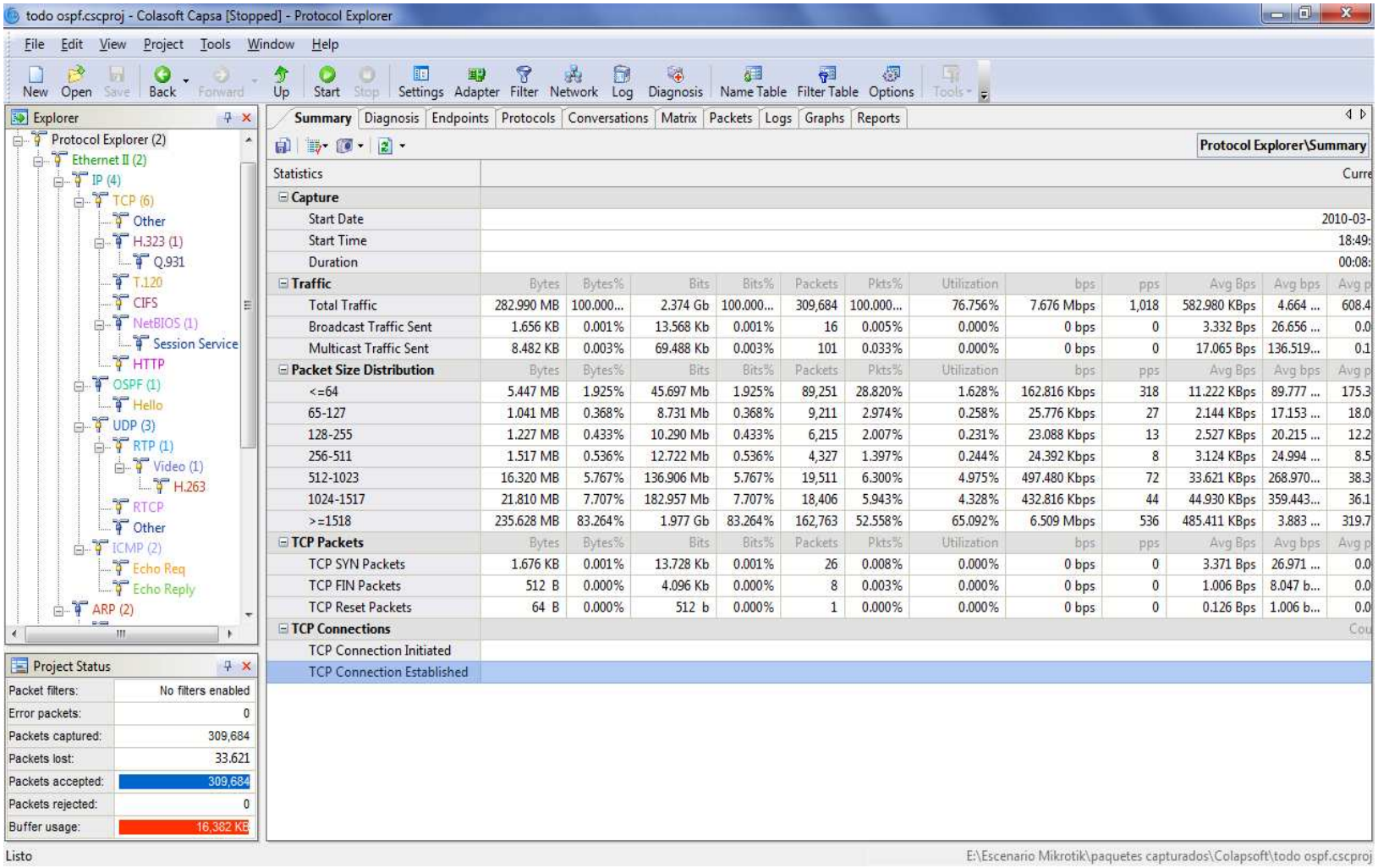


Gráfico IV.56 Ventana resumen del tráfico generado con OSPF

4.4.2 ESCENARIO MPLS

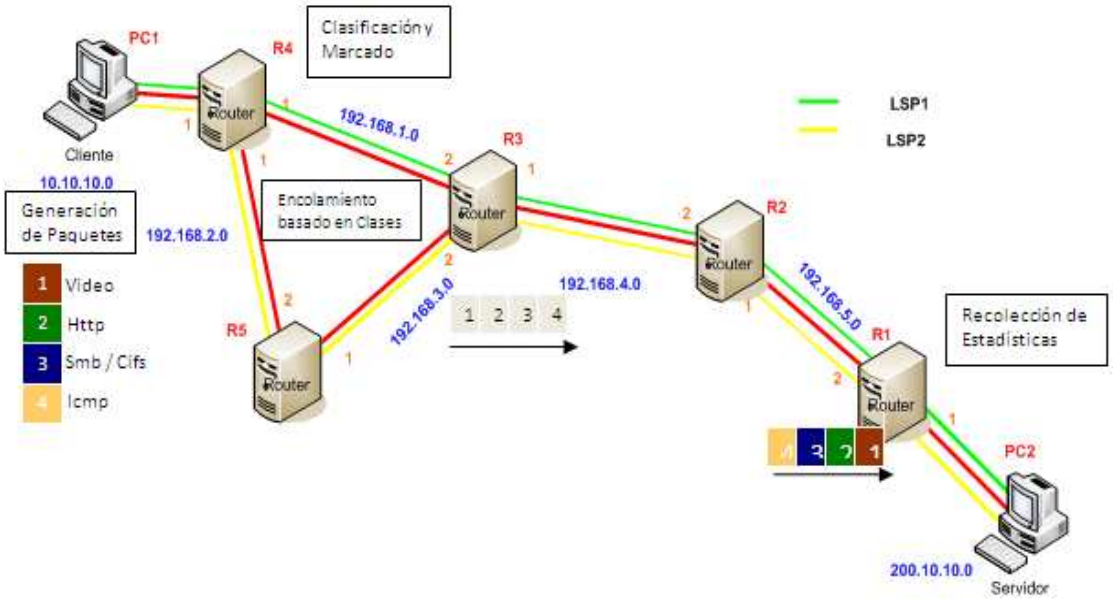


Gráfico IV.57 Evaluación del tráfico MPLS

En el **Gráfico IV. 57** Se observa el escenario que conforma la nube MPLS y las máquinas cliente y servidor, al generar tráfico por la red, se observa que al utilizar éste protocolo, se produjo la clasificación y marcado de los paquetes a través de las reglas mangle anteriormente configuradas (ver **Gráfico III.44**) y generar encolamiento basándose en prioridades de paquetes (ver **Gráfico III.46**), puede tomar 2 caminos posibles LSP1 y LSP2, pero el más óptimo es el LSP1 que luego se lo analiza en el **Gráfico IV. 59**.

4.4.2.1 Ancho de Banda

El tráfico generado al usar MPLS bajo OSPF, observamos como se distribuye objetivamente más altos el ancho de banda para el consumo del tráfico en la red, la transmición de videoconferencia ocupa mayor ancho de banda, ya que asi en la configuración de la CoS se le dio prioridad 1 a éste tipo de tráfico, los protocolos Http, Smb/ Cif e Icmp son balanceados para una equitativa ocupación del ancho de banda para la red montada. En el **Gráfico IV. 58** se lo puede apreciar:

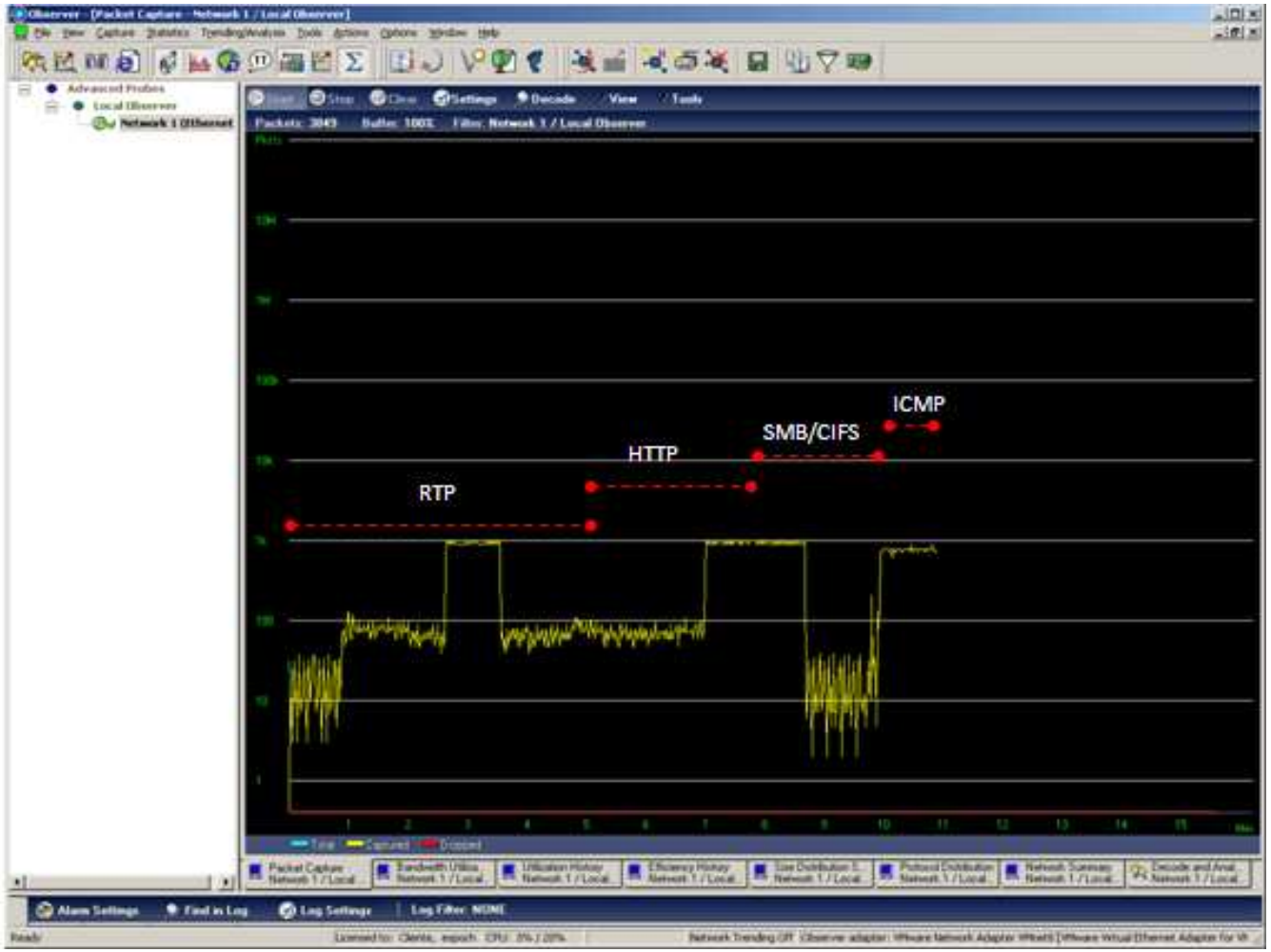


Gráfico IV.58 Ventana distribución de Ancho de Banda en la captura de tráfico con MPLS

4.4.2.2 Retardo Punto a Punto

Se analizan los saltos por los que tienen que pasar los paquetes hasta llegar a su destino, mediante el comando traceroute en símbolo del sistema:

Y en mikrotik con la línea de comando (ver el **Gráfico IV.59**), que se indica continuación:

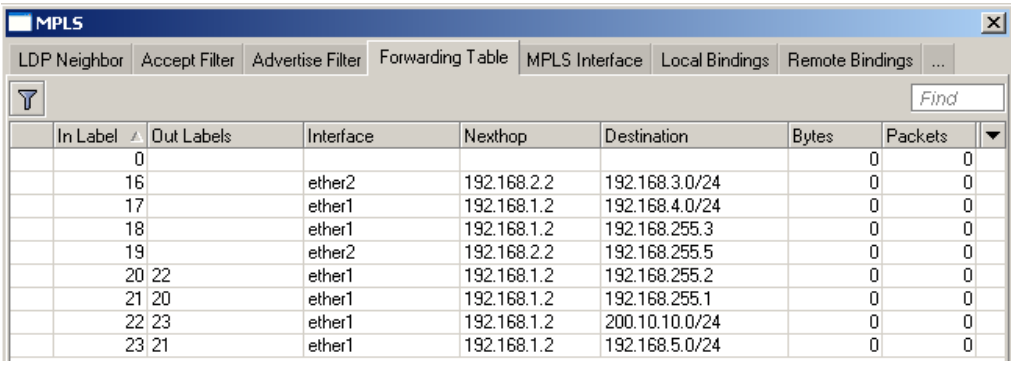
[admin@Mikrotik]> **tool traceroute** *{hacia donde}* **src-address=***{desde donde}*

```
[admin@R4] > tool traceroute 192.168.255.1 src-address=192.168.255.4
     ADDRESS                                          STATUS
   1     192.168.1.2 2ms 1ms 2ms
                       mpls-label=21
   2     192.168.4.2 1ms 2ms 1ms
                       mpls-label=18
   3   192.168.255.1 1ms 1ms 1ms
```

Gráfico IV.59 Impresión de los saltos por los routers MPLS

Análisis de las etiquetas de MPLS en cada router

R4



In Label	Out Labels	Interface	Nexthop	Destination	Bytes	Packets
0					0	0
16		ether2	192.168.2.2	192.168.3.0/24	0	0
17		ether1	192.168.1.2	192.168.4.0/24	0	0
18		ether1	192.168.1.2	192.168.255.3	0	0
19		ether2	192.168.2.2	192.168.255.5	0	0
20	22	ether1	192.168.1.2	192.168.255.2	0	0
21	20	ether1	192.168.1.2	192.168.255.1	0	0
22	23	ether1	192.168.1.2	200.10.10.0/24	0	0
23	21	ether1	192.168.1.2	192.168.5.0/24	0	0

Gráfico IV.60 Tabla Forwarding de router R4

R5

MPLS

LDP Neighbor | Accept Filter | Advertise Filter | Forwarding Table | MPLS Interface | Local Bindings | Remote Bindings | ...

Find

In Label	Out Labels	Interface	Nexthop	Destination	Bytes	Packets
0					0	0
16		ether2	192.168.3.2	192.168.4.0/24	0	0
17		ether2	192.168.3.2	192.168.255.3	0	0
18		ether1	192.168.2.1	10.0.0.0/8	0	0
19		ether1	192.168.2.1	192.168.255.4	0	0
20		ether1	192.168.2.1	192.168.1.0/24	0	0
21	22	ether2	192.168.3.2	192.168.255.2	0	0
22	23	ether2	192.168.3.2	200.10.10.0/24	0	0
23	20	ether2	192.168.3.2	192.168.255.1	0	0
24	21	ether2	192.168.3.2	192.168.5.0/24	0	0

Gráfico IV.61 Tabla recepción/envío de etiquetas del router R5

R3

MPLS

LDP Neighbor | Accept Filter | Advertise Filter | Forwarding Table | MPLS Interface | Local Bindings | Remote Bindings | ...

Find

In Label	Out Labels	Interface	Nexthop	Destination	Bytes	Packets
0					0	0
16		ether1	192.168.1.1	192.168.2.0/24	0	0
17		ether1	192.168.1.1	10.0.0.0/8	66001	89
18		ether1	192.168.1.1	192.168.255.4	0	0
19		ether2	192.168.3.1	192.168.255.5	0	0
20	18	ether3	192.168.4.2	192.168.255.1	0	0
21		ether3	192.168.4.2	192.168.5.0/24	8614	54
22		ether3	192.168.4.2	192.168.255.2	0	0
23	21	ether3	192.168.4.2	200.10.10.0/24	0	0

Gráfico IV.62 recepción/envío de etiquetas del router R3

R2

MPLS

LDP Neighbor | Accept Filter | Advertise Filter | Forwarding Table | MPLS Interface | Local Bindings | Remote Bindings | ...

Find

In Label	Out Labels	Interface	Nexthop	Destination	Bytes	Packets
0					0	0
16		ether1	192.168.4.1	192.168.3.0/24	0	0
17		ether1	192.168.4.1	192.168.1.0/24	0	0
18		ether2	192.168.5.2	192.168.255.1	0	0
19	16	ether1	192.168.4.1	192.168.2.0/24	0	0
20		ether1	192.168.4.1	192.168.255.3	0	0
21		ether2	192.168.5.2	200.10.10.0/24	0	0
22	18	ether1	192.168.4.1	192.168.255.4	0	0
23	19	ether1	192.168.4.1	192.168.255.5	0	0
24	17	ether1	192.168.4.1	10.0.0.0/8	34950	45

Gráfico IV.63 recepción/envío de etiquetas del router R2

R1

MPLS

LDP Neighbor | Accept Filter | Advertise Filter | Forwarding Table | MPLS Interface | Local Bindings | Remote Bindings | ...

Find

In Label	Out Labels	Interface	Nexthop	Destination	Bytes	Packets
0					0	0
16	16	ether1	192.168.5.1	192.168.3.0/24	0	0
17		ether1	192.168.5.1	192.168.4.0/24	0	0
18	17	ether1	192.168.5.1	192.168.1.0/24	0	0
19	19	ether1	192.168.5.1	192.168.2.0/24	0	0
20	20	ether1	192.168.5.1	192.168.255.3	0	0
21	24	ether1	192.168.5.1	10.0.0.0/8	0	0
22	22	ether1	192.168.5.1	192.168.255.4	0	0
23	23	ether1	192.168.5.1	192.168.255.5	0	0
24		ether1	192.168.5.1	192.168.255.2	0	0

Gráfico IV.64 recepción/envío de etiquetas del router R1

El **Gráfico IV.65** muestra el flujo de las etiquetas en cada una de las PC Routers Mikrotik, se puede ver en el R4 la etiqueta de entrada 22 y como etiqueta de salida la 23, la misma que es pasada el R3 como etiqueta de entrada y sale con la etiqueta 21, luego el R2 toma la etiqueta 21 en su entrada y sale con la etiqueta 18 al R1, R1 toma esta etiqueta como su etiqueta de entrada y finalmente sale con la etiqueta 17 hasta llegar a la máquina servidor donde se extrae la cabecera MPLS y se trata al paquete como IP.

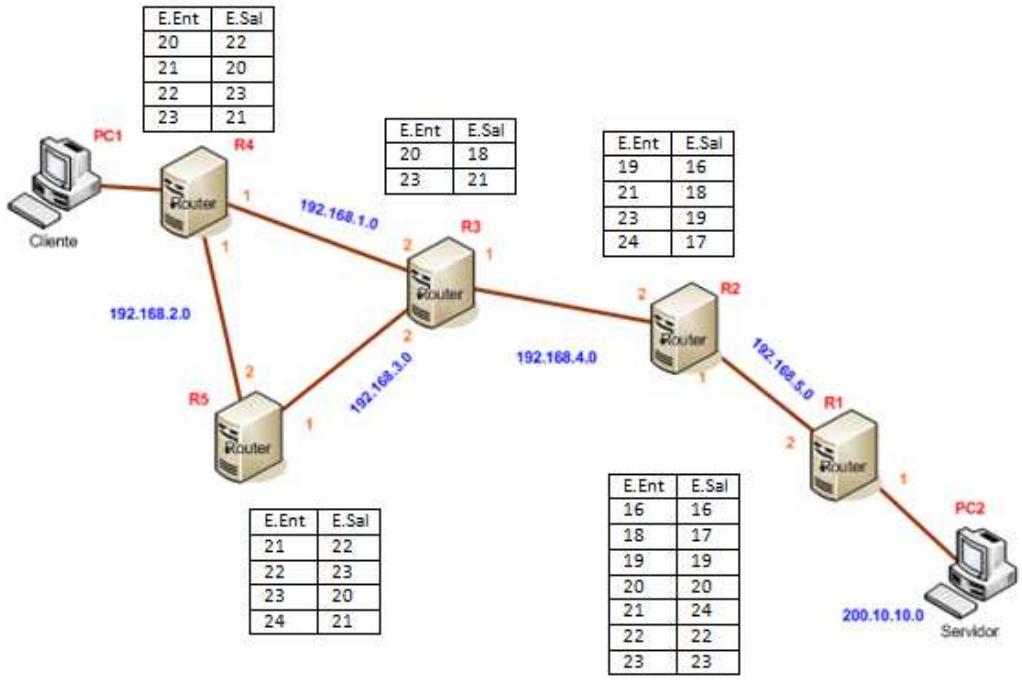


Gráfico IV.65 Generación de etiquetas para la comunicación del protocolo MPLS

En el **Gráfico IV. 66** observamos los resultados obtenidos de las pruebas realizadas con protocolo MPLS, el cual indica el retardo o delay descrito en milisegundos, podemos ver que existe bajos tiempos de respuesta para el tráfico TCP(Http - Smb/Cifs) y UDP (Rtp), son casi imperceptibles los tiempos de respuesta, pues existe una agrupación de los datos con un porcentaje estimadamente bajo.

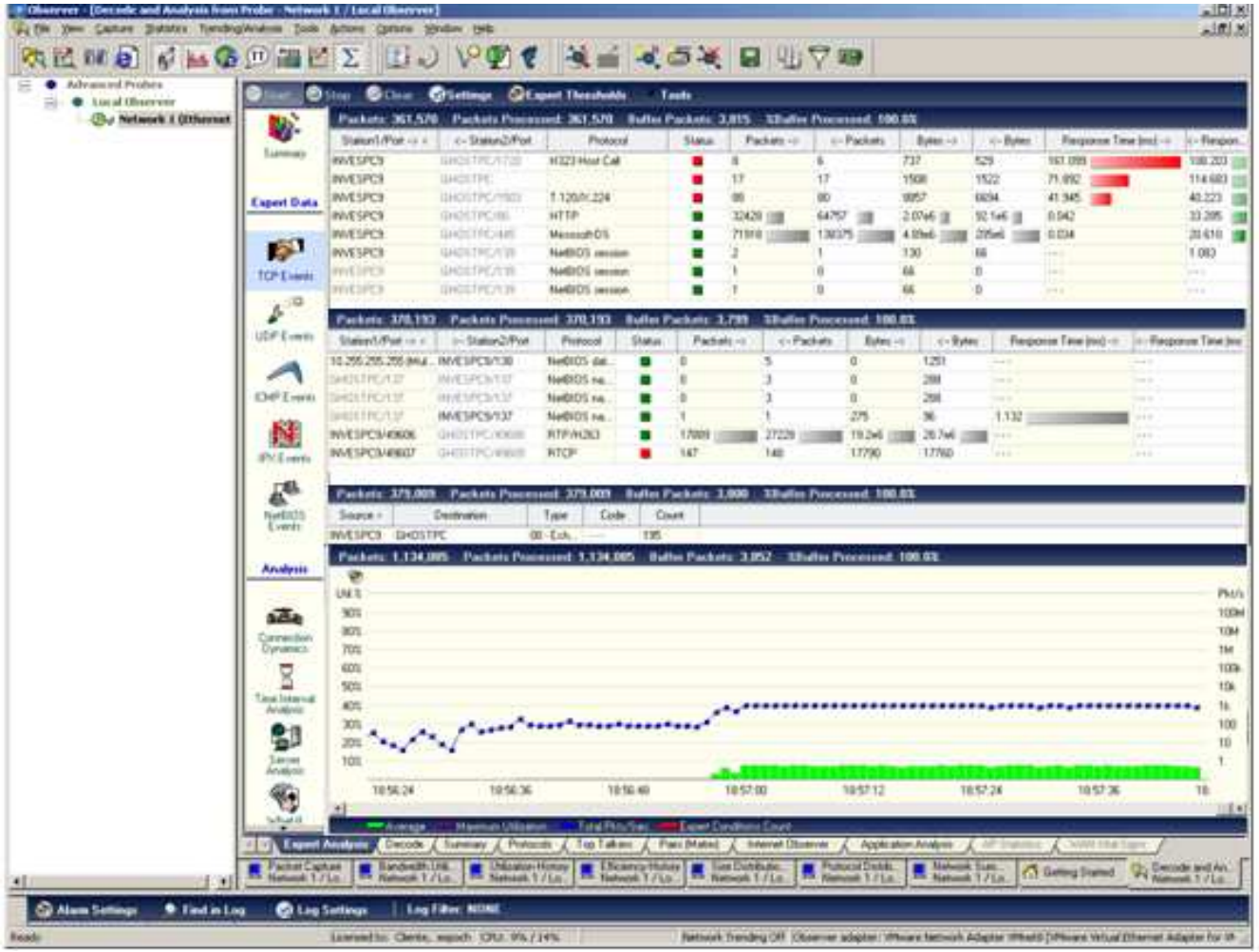


Gráfico IV.66 Ventana captura de tazas de tráfico en la captura de tráfico con MPLS

4.4.2.3 Jitter

Durante la transmición de tráfico generado en la red, podemos ver que la transmisión de retorno los picos máximos son aproximadamente de 51,85ms en un 30% del jitter, el 70% del jitter está bajo los 20 ms. Mientras que en la transmisión de ida los picos máximos son de 45,46ms, el 80% del jitter se encuentra por sobre los 30 ms y el 20% se encuentra bajo los 25 ms.

En este perfil se puede determinar que en la transmisión de ida existe una perdida menor con respecto a la transmisión de retorno en un tiempo aproximado de 6,8min, lo que se puede observar en el **Gráfico IV. 67,** donde el pico más alto se alcanza en el segundo 409,5s que se muestra a continuación:

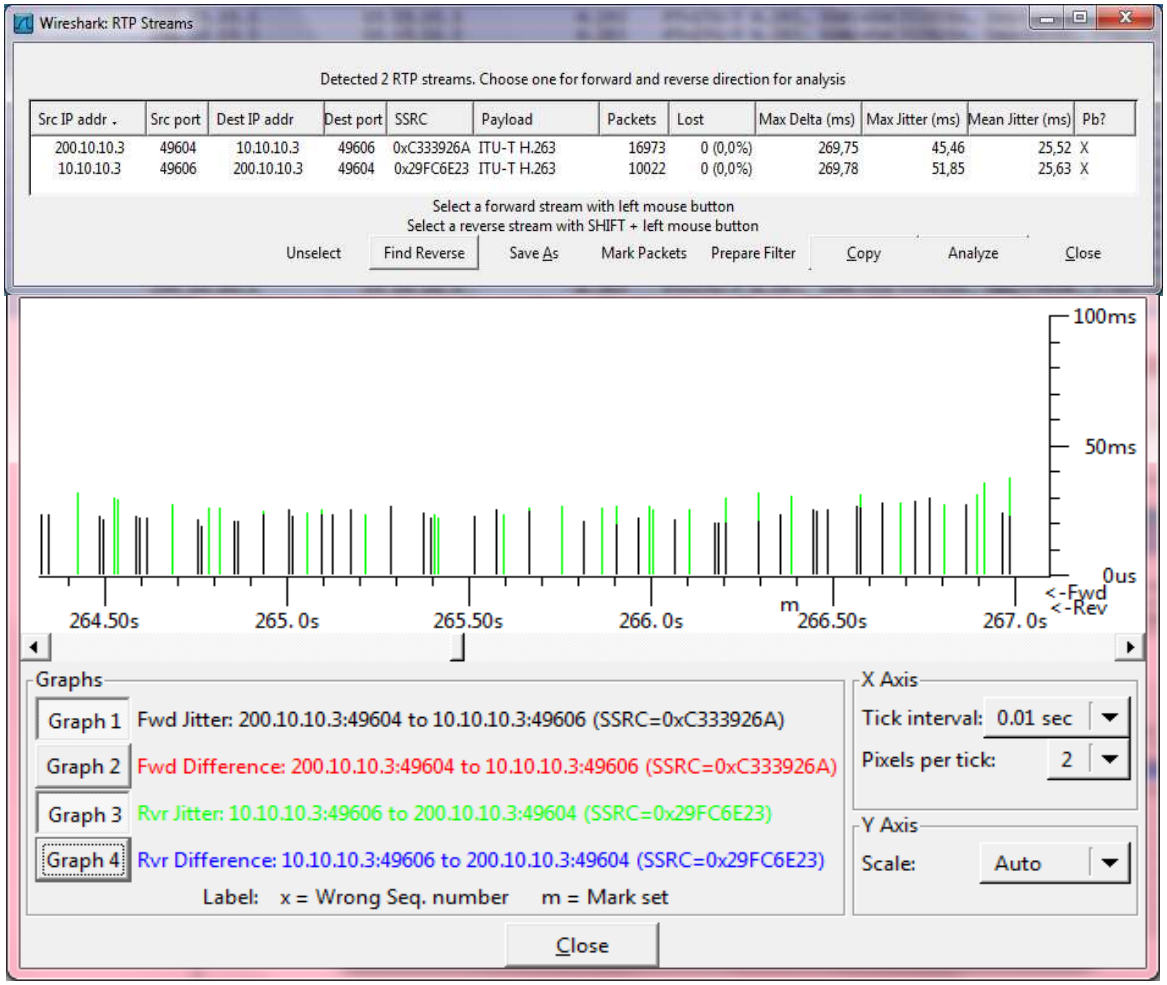


Gráfico IV.67 Ventana Jitter de RTP en la captura de tráfico con MPLS

4.4.2.4 Pérdida de paquetes

En la transmisión de tráfico de la red con protocolo MPLS se puede observar los valores y tazas de utilización de bytes, bits, paquetes, bits por segundo, paquetes por segundo, promedios de utilización de bytes y bits; siendo mayor la utilización a partir de un tamaño 1518 paquetes ocupando un 61,8%. El 1,39% usado por paquetes de tamaño 512-1023 y menores de 64, el resto oscilan entre tamaño de 654-1023.

En la tabla inferior vemos que no se generó pérdida de paquetes y el uso del buffer ocupado fue de 16,382 KB (Ver **Gráfico IV.68**).

La pérdida de paquetes es la principal causa de degradación de la calidad, es decir es un factor preponderante en lo que se refiere a servicios en tiempo real. Dado que el tráfico de Videoconferencia (RTP) se implementa sobre UDP el único control que se puede realizar sobre la pérdida de paquetes se da en las puntas de la transmisión. Los codecs implementan técnicas de corrección de errores para hacerlos transparentes al usuario, utilizando algoritmos de interpolación sobre los datos recibidos para generar la información perdida.

Sin embargo, cuando las pérdidas superan cierto umbral o cuando se dan en ráfagas ya dejan de ser útiles las técnicas mencionadas.

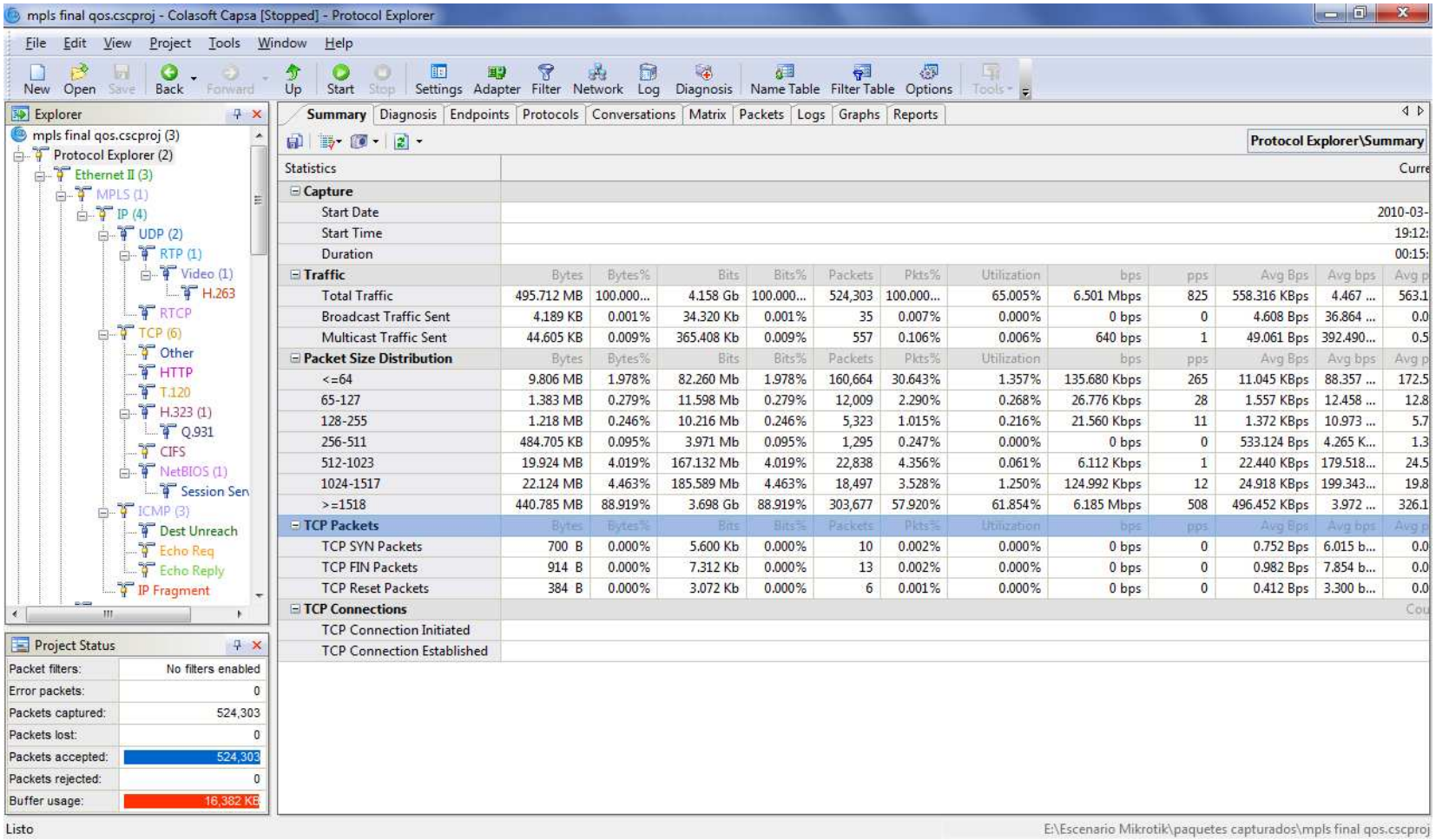


Gráfico IV.68 Ventana resumen del tráfico generado con MPLS

4.5 Hipótesis

"El manejo de la calidad de servicio en redes basadas en MPLS bajo plataforma Linux, permitirá la administración de manera más eficiente de las redes WAN".

4.5.1 Verificación de la Hipótesis

Para verificar si la hipótesis se acepta o se niega, se debe separar en 2 variables, dependiente e independiente, como se indica a continuación:

Variable Independiente: El manejo de la Calidad de Servicio en redes basadas en MPSL bajo plataforma Linux

Variable Dependiente: Administración eficiente de las redes WAN

4.5.2 Valorización

Se evaluó los indicadores definidos para cada parámetro de medición, se empleará la siguiente matriz de valorización con los valores cuantitativos y cualitativos, como muestra en la **Tabla IV.8:**

Valor cualitativo	Valor cuantitativo
Muy Bajo	1
Bajo	2
Medio	3
Alto	4
Muy Alto	5
NA	Sin valor cuantitativo

Tabla IV.8 Tabla de Valorización

4.5.2.1 Muy Bajo

Esta calificación se asigna cuando el protocolo no cumpla con el objetivo del indicador. Dicho de otra manera cuando el protocolo no contenga la característica del indicador. El equivalente en valor cuantitativo será igual a 1.

4.5.2.2 Bajo

Este valor cualitativo se asigna al protocolo que cumplan de forma deficiente con el objetivo del indicador correspondiente. Su valor cuantitativo será igual a 2.

4.5.2.3 Medio

La presente calificación se le asigna al protocolo que cumplan parcialmente con el objetivo del indicador. El equivalente cuantitativo será igual a 3.

4.5.2.4 Alto

El valor cualitativo Muy bueno se asignará al protocolo que cumpla con casi todos los requerimientos del indicador. El valor cuantitativo será igual a 4.

4.5.2.5 Muy Alto

Esta calificación se asigna al protocolo que cumplan a cabalidad con el objetivo del indicador. Su valor cuantitativo será igual a 5.

4.5.2.6 NA

Se determina NA cuando el indicador no es aplicable asignar una calificación.

4.5.3 Evaluación de los Indicadores de los Parámetros de Medición de los Escenarios Planteados

En este apartado se analiza los indicadores estimados para cada parámetro que determina la QoS en la red, se le coloca una puntuación basada en la **Tabla IV.8.**

4.5.3.1 Evaluación de los Indicadores del Parámetro 1: Ancho de Banda

En la **Tabla IV.9** se muestra la calificación que se asignó a los indicadores del Parámetro 1: Ancho de Banda, se ve como MPLS es más eficiente en la transmisión de bits, y su agilidad al recibir y transmitir paquetes, por lo que genera poco tráfico a comparación de OSPF.

Herramientas / Indicadores	OSPF	MPLS
Bits transmitidos	2	5
Paquetes Recibidos	3	4
Paquetes Transmitidos	4	4
Tráfico Generado	4	2

Tabla IV.9 Análisis Cualitativo Parámetro 1

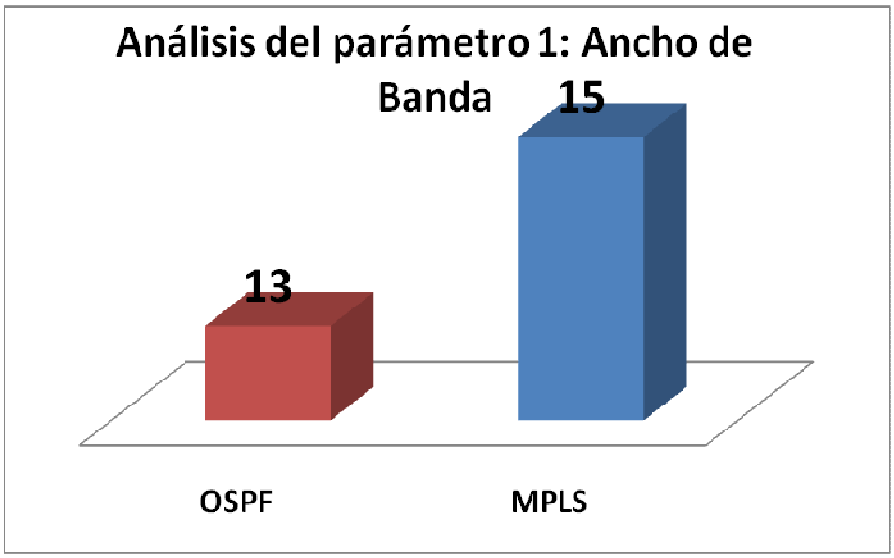


Gráfico IV.69 Gráfico Estadístico Análisis Cualitativo Parámetro 1

El **Gráfico IV.69** muestra como MPLS es superior en el manejo del ancho de banda obteniendo un total de 15 puntos de los valores cuantitativos dados para su estimación, comparación de OSPF que obtiene 13.

4.5.3.2 Evaluación de los Indicadores del Parámetro 2: Retardo Punto a Punto

En la siguiente tabla se muestra la calificación que se asignó a los indicadores del Parámetro 2: Retardo Punto a Punto.

Herramientas / Indicadores	OSPF	MPLS
Búsqueda en las tablas de ruteo	4	2
Calidad de Imagen	3	2
Aplicaciones Multimedia	5	2

Tabla IV.10 Análisis Cualitativo Parámetro 2

En la **Tabla IV.10** se muestra la calificación que se asignó a los indicadores del Parámetro 2: Retardo Punto a Punto, se ve que OSPF obtiene mayor valoración en el factor Búsqueda en las tablas de ruteo ya que éste toma mayor tiempo en designar cual será el siguiente salto en el ruteo, al producir demora también se degenera la calidad en imágenes y en imágenes multimedia, mientras que MPLS se mantiene constante, al encontrar la mejor ruta, despacha el tráfico siempre por esa vía.

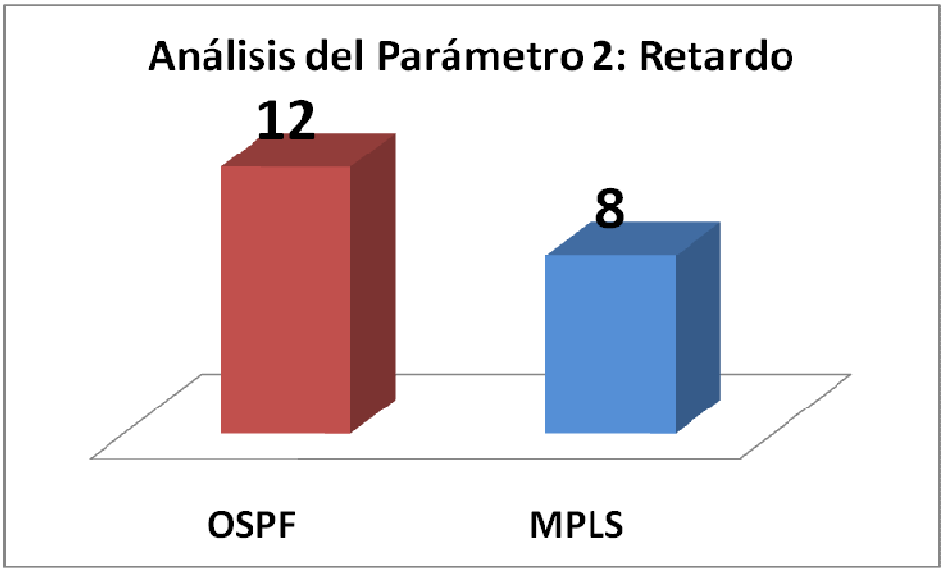


Gráfico IV.70: Gráfico Estadístico Análisis Cualitativo Parámetro 2

El **Gráfico IV.70** muestra como OSPF obtiene mayor puntuación al analizar el Retardo Punto a Punto, y se aprecia una notoria diferencia con MPLS, siendo esta mejor al tratar este factor que influye en la QoS de la red.

4.5.3.3 Evaluación de los Indicadores del Parámetro 3: Pérdida de Paquetes

En la **Tabla IV.11** se muestra la calificación que se asignó a los indicadores del Parámetro 3: Pérdida de Paquetes, se observa que OSPF tiene altos valores en el factor pérdida de paquetes, además de bajos valores en los paquetes recibidos y filtrados, por ende MPLS obtiene mejor puntuación al controlar estos factores garantizando la QoS.

Herramientas / Indicadores	OSPF	MPLS
Paquetes Perdidos	5	1
Paquetes Aceptados	3	4
Paquetes Filtrados	3	4

Tabla IV.11 Análisis Cualitativo Parámetro 3

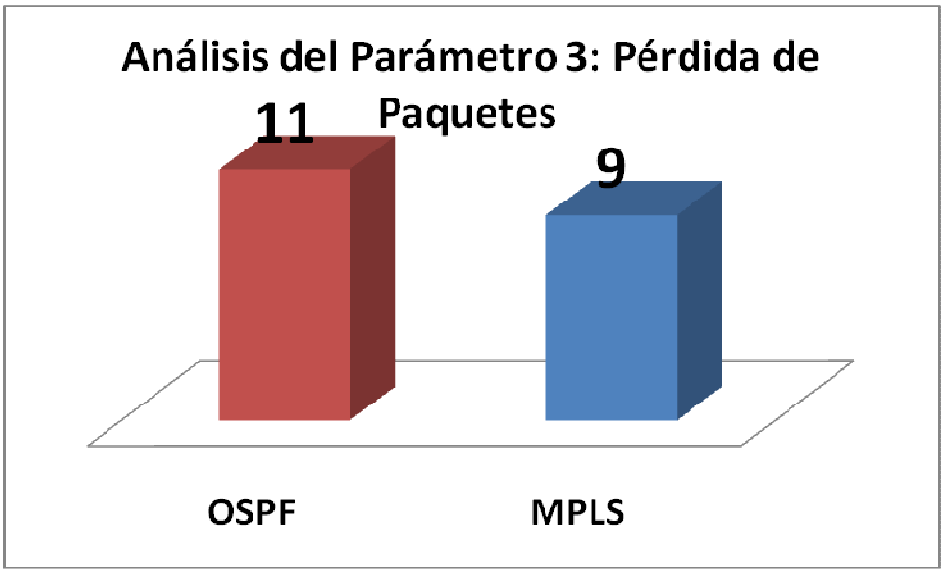


Gráfico IV.71 Gráfico Estadístico Análisis Cualitativo Parámetro 3

El **Gráfico IV.71** muestra los altos valores obtenidos por OSPF obtiene al momento de producir Pérdida de Paquetes, mientras que MPLS sabe controlar los factores que impiden la entrega de paquetes.

4.5.3.4 Evaluación de los Indicadores del Parámetro 4: Jitter

En la **Tabla IV.12** se muestra la calificación que se asignó a los indicadores del Parámetro 4: Jitter, se observa que OSPF hace consumos mayores del buffer, por tanto produciendo más retardo y con poca velocidad de transmisión y MPLS administra estos factores de forma contraria.

Herramientas / Indicadores	OSPF	MPLS
Uso del Buffer	5	2
Retardo	4	1
Velocidad de Transmisión	2	5

Tabla IV.12 Análisis Cualitativo Parámetro 4

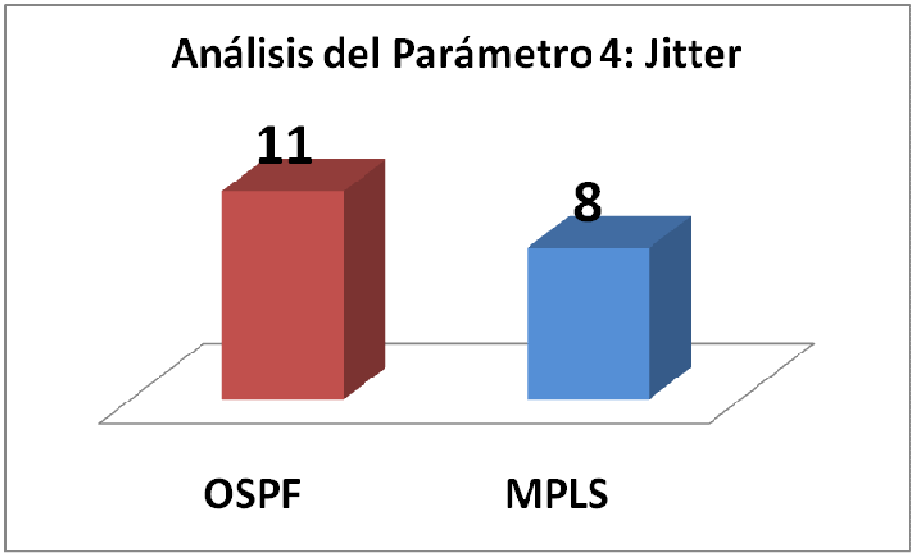


Gráfico IV.72 Gráfico Estadístico Análisis Cualitativo Parámetro 4

El **Gráfico IV.72** muestra en éste análisis como OSPF genera altos valores al momento de tratar el Jitter, mientras que MPLS sabe cuidar los factores que influyen en la producción de éste parámetro que reduce la QoS en la red.

4.5.4 Matriz de Valorización: Análisis Comparativo Cualitativo de los Indicadores de los Parámetros de los Protocolos OSPF y MPLS

Luego de haber medido el tráfico y haber realizado el análisis de las cabeceras de los protocolos OSPF con MPLS y OSPF sin MPLS, en las pruebas desarrolladas anteriormente podemos cuantificar la calificación de los indicadores de los 4 parámetros que conforman el análisis comparativo, a continuación la **Tabla IV.13** muestra la matriz de valorización:

Herramientas / **Indicadores**	**Fo (OSPF)**	**Fe (MPLS)**	$X^2 = \frac{\sum (F_0 - F_e)^2}{F_e}$
Bits Transmitidos	2	5	1,8
Paquetes Recibidos	3	4	0,25
Paquetes Transmitidos	4	4	0
Tráfico Generado	4	2	2
Búsqueda en las tablas de ruteo	4	2	2
Calidad de Imagen	3	4	0,25
Aplicaciones Multimedia	5	2	4,5
Paquetes Perdidos	5	1	16
Paquetes Aceptados	3	4	0,25
Paquetes Filtrados	3	4	0,25
Uso del buffer	5	2	4,5
Paquetes Transmitidos	4	1	9
Calidad de la Imagen	2	5	1,8
TOTAL	**47**	**40**	**42,6**

Tabla IV.13 Matriz de Valoración

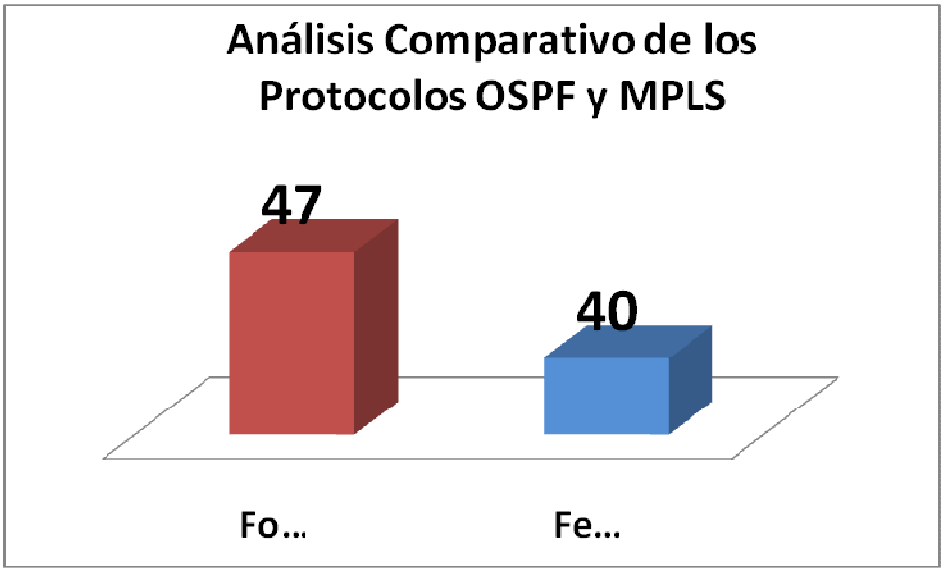


Gráfico IV.73 Gráfico Estadístico Análisis comparativo de OSPF y MPLS

El **Gráfico IV.73** muestra mediante el diagrama de barras simple de la sumatoria obtenida por tabulación de todos los indicadores de los parámetros, determinándose como protocolo más funcional y que mejora e implementa la QoS es MPLS que alcanzó un porcentaje del 40% a diferencia de OSPF que obtuvo un 47%. Lo que quieres decir que OSPF tiene un alto porcentaje de fallas a comparación de MPLS, por ende este último tiene mejor rendimiento en el manejo de la QoS de redes bajo plataforma Linux.

4.5.4.1 Comprobación de la Hipótesis y Resultados

La prueba aplicada para nuestro caso fue la χ^2 de Pearson (pronunciado como "ji-cuadrado" y a veces como "chi-cuadrado) es considerada como una prueba no paramétrica que mide la discrepancia entre una distribución observada y otra teórica

(bondad de ajuste), indicando en qué medida las diferencias existentes entre ambas, de haberlas, se deben al azar en el contraste de hipótesis.

La fórmula que da el estadístico es la siguiente:

$$X^2 = \frac{\sum \left(F_0 - F_e\right)^2}{F_e}$$

	Variable 1	**Variable 2**
Media	3,6153846	3,0769231
Varianza	1,0897436	2,0769231
Observaciones	13	13
Grados de libertad	12	12
ji cuadrado	42,6	
Valor crítico para F (una cola)	5,2260295	

Tabla IV.14 Tabla de contingencia para calcular x^2

En la **Tabla IV.14** muestra el análisis estadístico para las variables 1 y 2 de nuestra hipótesis. A la vista de este resultado, lo que tenemos que hacer ahora es plantear un contraste de hipótesis.

4.5.4.2 Planteamiento de Hipótesis para comprobar si existe diferencia significativa entre los protocolos

H0= El manejo de la calidad de servicio en redes basadas en MPLS bajo plataforma Linux, no permitirá la administración de manera más eficiente de las redes WAN.

H1= El manejo de la calidad de servicio en redes basadas en MPLS bajo plataforma Linux, permitirá la administración de manera más eficiente de las redes WAN.

Bajo la hipótesis nula de independencia, se sabe que los valores del estadístico χ^2 se distribuyen según una distribución conocida denominada ji-cuadrado, que depende de un parámetro llamado "grados de libertad" (g.l.). Para el caso de una tabla de contingencia de r filas y k columnas, los g.l. son igual al producto del número de filas menos 1 (r-1) por el número de columnas menos 1 (k-1) (Valores obtenidos de la Tabla de Valoración)

Para nuestro caso el valor del Grado de Libertad es 12

De ser cierta la hipótesis nula, el valor obtenido debería estar dentro del rango de mayor probabilidad según la distribución ji-cuadrado correspondiente. El valor-p que usualmente reportan la mayoría de paquetes estadísticos no es más que la probabilidad de obtener, según esa distribución, un dato más extremo que el que proporciona el test o, equivalentemente, la probabilidad de obtener los datos observados si fuese cierta la hipótesis de independencia. Si el valor-p es muy pequeño (usualmente se considera $p<0.05$) es poco probable que se cumpla la hipótesis nula y se debería de rechazar.

De este modo, si el estadístico χ^2 calculado del experimento toma un valor de 42.6, y el valor crítico estandarizado de χ^2 es 5.22 (ver **Gráfico IV.74**).

Siendo que el valor Chi cuadrada (c 2) obtenido es mayor que el valor crítico, se desacredita la hipótesis nula que afirma que "El manejo de la calidad de servicio en redes basadas en MPLS bajo plataforma Linux, no permitirá la administración de manera más eficiente de las redes WAN" y se concluye que "El manejo de la calidad de servicio en redes basadas en MPLS bajo plataforma Linux, permitirá la administración de manera más eficiente de las redes WAN"

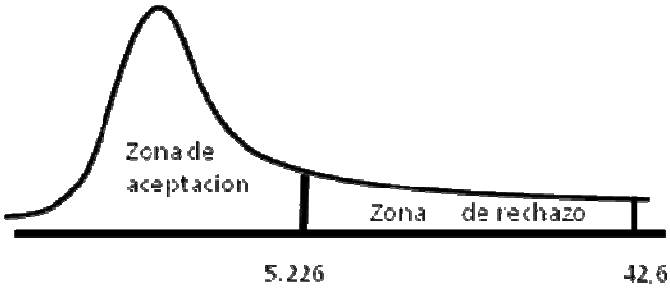


Gráfico IV.74 Gráfico Explicativo de Aceptación de la hipótesis

CONCLUSIONES

- La aplicación de mecanismos de ingeniería de tráfico y de diferenciación de servicios no resulta suficiente para la provisión de garantías QoS si no se evita que la red llegue a una situación de sobreutilización de sus recursos, inevitablemente provocando congestión. Por ello, es necesario aplicar mecanismos de control de admisión, que también han sido objeto de un gran esfuerzo de investigación sobre la utilización de Mikrotik para la configuración de los routers.

- Las Políticas de calidad de servicio se realizan a través del campo Tipo de Servicio (ToS) del paquete IP en IPv4. Para la priorización de tráfico se realizó configuraciones en dicho campo y así se pudo comprobar la aplicación de QoS para este tipo de redes, que no solamente limitación, es un intento de usar los recursos existentes racionalmente (no es necesario utilizar todo el ancho de banda disponible). QoS balancea y prioriza el flujo de datos, asegurando la mejor velocidad posible y previniendo el "monopolio" del canal de datos. Esta es la razón del porque se llama "Quality of Service".

- El sistema operativo Mikrotik RouterOS, nos permitió el desarrollo y culminación del trabajo de Tesis, pese a ser una herramienta con valor de licenciamiento moderado frente a otros equipos propietarios, existen en la red alternativas para su crakeo, y en casos educativos como el nuestro resultó sencillo su instalación,

administración, y uso en las pc habituales, por lo que se comprobó que se puede simular escenarios prácticos y funcionales sin la necesidad de grandes costos de valor.

- Con la implantación de calidad de servicio (QoS), es posible ofrecer mayor garantía y seguridad para las aplicaciones avanzadas, una vez que el tráfico de estas aplicaciones pasa a tener prioridad en relación con aplicaciones tradicionales.

- La descripción de estos dos protocolos de QoS podría hacer pensar que son excluyentes, pero no es así, de hecho se complementan. En la práctica, es muy frecuente encontrar muchas posibles combinaciones entre estas dos arquitecturas y más aún, pueden combinarse con otras tecnologías para dar soporte a la QoS extremo a extremo.

- Al analizar los parámetros que aseguran la QoS como: Ancho de Banda, Pérdida de Paquetes, Retardo Punto a Punto y Jitter, comprobamos que MPLS ofrece mejoras evidentes, al realizar diferenciación y priorización del tráfico evita la congestión y optimiza el manejo y el control de uso de los recursos de la red. MPLS por sí solo no proporciona diferenciación del tráfico, siendo este requisito imprescindible para la provisión de garantías de QoS, por ello se puede complementar con DiffServ para aplicar esta diferenciación.

RECOMENDACIONES

- Mikrotik es una útil alternativa para la simulación de Routers, ya que nos permite la fácil configuración y administración de los recursos de la red, comparado con Sistemas Operativos como Fedora, cuya configuración resulta complicada, RouterOS es una solución práctica y económica, a diferencia del manejo de equipos propietarios que poseen altos costos, por eso es recomendable su uso para el campo educativo y empresarial.

- Al trabajar con software libre es importante conocer cuáles son los módulos y componentes con los que trabaja y la versión del kernel y módulos con los que es compatible, para evitar problemas posteriores en su utilización.

- Para la captura de tráfico de la red, es necesario ubicar una máquina que contenga los sniffers, en el centro de la nube, debido a que ahí se hará una captura real del tráfico que se está generando en la red.

- El escenario planteado debe tener varias alternativas para la realización de los saltos, de otra forma la comprobación de las rutas que tomen los paquetes puede ser siempre la misma y la verificación de los caminos inexistente.

RESUMEN

Se busca mejorar la Calidad de Servicio de redes utilizando el protocolo MPLS, bajo plataforma Linux, proporcionando una guía metodológica como ayuda didáctica en el proceso enseñanza aprendizaje para el laboratorio de redes de la Escuela de Ingeniería en Sistemas de la ESPOCH.

Las herramientas utilizadas para la configuración de la red fueron: Mikrotik RouterOS v3.22, Winbox v2.2.15, se revisó la guía de los RFC 1349 2328 3032 donde especifican y estandarizan los protocolos relacionados con redes. Escogiéndose el protocolo OSPF para realizar su enrutamiento debido a que es avanzado y escalable. Verificándose que los mecanismos MPLS facilitan el etiquetado de paquetes e impactan positivamente a los servicios sensibles al tiempo de transmisión

El comportamiento de la red fue evaluado con parámetros como: Ancho de banda, Retardo, Jitter y Pérdida de paquetes, analizados con sniffers wireshark y colasoft. Mediante estadística descriptiva se realizó la representación en un diagrama de barras simple de la sumatoria obtenida por tabulación de todos los parámetros, determinándose que el protocolo más funcional y que mejora la calidad de servicio es MPLS que alcanzó un porcentaje de 47% cumpliendo con total funcionalidad el aseguramiento de entrega de paquetes en la red, a diferencia de OSPF que obtuvo un 40%.

Se elaboró una guía metodológica en base al proceso de simulación con equipos de escritorio, cuyos contenidos son: instalación, licenciamiento, software empleado, configuración de los protocolos OSPF y MPLS, con su aplicación el estudiante podría instalar utilizar y armar una red, sirviendo para su capacitación práctica.

SUMMARY

Seeks to improve the quality of service network using the MPLS Protocol under Linux platform, providing a methodological guide as a teaching aid in the learning process education to network laboratory of the engineering school in the ESPOCH.

The tools used for configuration of the network were: Mikrotik RouterOS v3.22, Winbox v2.2.15, revised guide to the RFC 1349 2328 3032 where specified and standardize network protocols. The OSPF protocol had been choosen to made routing because it is advanced and scalable. Verifying the MPLS mechanisms to facilitate the labeling of packages and impact positivity to sensitive services at the time of transmission.

The behavior of the network was evaluated with parameters such as: wide bandwidth, delay, Jitter and loss of packets, analyzed with wireshark and colasoft sniffers. Using descriptive statistics was rendering a simple bar chart of the sum obtained by all the parameters tab by determining the most functional Protocol and improves the quality of service is MPLS reached 47% to meet the delivery of packets on the network, OSPF obtained 40% unlike assurance with full functionality.

It developed a methodological guide on the process simulation with desktops, whose contents are: installation, licensing, software used, and the protocol settings OSPF and MPLS, with your application, the student could install, use and build a network serving for their practical training.

GLOSARIO

RTP (Real Time Protocol - Protocolo de Tiempo Real). Protocolo empleado para transmitir información en tiempo real como audio y video para una videoconferencia.

HTTP (HyperText Transfer Protocol). Protocolo usado para acceder a la Web (WWW). Se encarga de procesar y dar respuestas a las peticiones para visualizar una página web.

SMB (Server Message Block). Protocolo de red (que pertenece a la capa de aplicación en el modelo OSI) que permite compartir archivos, impresoras, y demás recursos entre nodos de una red. Se usa principalmente en computadoras con Windows y DOS.

ICMP (Internet Control Message Protocol - Protocolo de Control de Mensajes de Internet). Subprotocolo de diagnóstico y notificación de errores del Protocolo de Internet (IP).

Es utilizado para enviar mensajes de errores cuando un servicio no está disponible o cuando un host no puede ser encontrado, etc.

SSH Al igual que el telnet (que dejó de usarse), se emplea para acceder a máquinas a través de una red. La principal ventaja con respecto a telnet, es que la información viaja cifrada y no es posible descubrir el nombre de usuario ni contraseña. Permite conectarse tipo terminal al otro ordenador.

LDP LDP posibilita a los nodos MPLS descubrirse y establecer comunicación entre sí con el propósito de informarse del valor y significado de las etiquetas que serán utilizadas en sus enlaces contiguos.

LSA Publicidad de estado-enlace. Paquete de broadcast utilizado por los protocolos estado-enlace contiene información acerca de vecinos y costos de ruta. Son utilizados por los routers receptores para mantener sus tablas de enrutamiento. Se le denomina paquete de estado de enlace (LSP).

LSP Label Switched Path. Camino Conmutado de Etiquetas: el camino compuesto por uno o más LSRs dentro de un nivel jerárquico por el que un paquete perteneciente a un determinado FEC circula. Todos los paquetes pertenecientes a un mismo FEC circularán siempre por el mismo camino LSP.

LER Layer Edge Router. Router Frontera entre Capas: Es el dispositivo LSR Frontera entre IP y MPLS. Los LER deben poseer todas las funcionalidades de un LSR y además capacidad para asociar FECs y nuevas Etiquetas con los datagramas IP que entren en la red. O para asignar direcciones IP a los FEC de los paquetes etiquetados que salen de la red.

FEC Forwarding Equivalence Class. Clase de Envío Equivalente: Es un subconjunto de paquetes IP que son tratados de la misma manera por un router. Podemos decir que en el routing convencional, cada paquete está asociado a un nuevo FEC en cada salto. En MPLS esta operación sólo se realiza la primera vez que el paquete entra en la red.

Etiqueta Un identificador de longitud corta y constante que se emplea para identificar una Clase de Envío Equivalente (FEC), normalmente con carácter local. En el caso de ATM, las etiquetas se codificarán dentro de los campos vpi - vci de los paquetes ATM.

Pila de Etiquetas	Un conjunto apilado de etiquetas que pueden circular con el paquete. Componente de Control de Conmutación de etiquetas en ATM Para soportar conmutación de etiquetas, un switch ATM debe implementar la componente de control de conmutación de etiquetas.
Calidad de Servicio	Son tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (*throughput*). Es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de video o voz.
IETF	Es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad. Fue creada en EE. UU. En 1986. La IETF es mundialmente conocida por ser la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC.
Protocolo	Los protocolos son reglas y procedimientos para la comunicación. Cuando dos equipos están conectados en red, las reglas y procedimientos técnicos que dictan su comunicación e interacción se denominan protocolos.
Licencia	Es una especie de contrato, en donde se especifican todas las normas y clausulas que rigen el uso d terminado programa, principalmente se estipulan los alcances de uso, instalación, reproducción y copia de estos productos

BIBLIOGRAFÍA

CALIDAD DE SERVICIO

- **QoS**

  <http://es.wikipedia.org/wiki/Calidad_de_Servicio>

  20090817

- **Marcado de Paquetes**

  <http://qos.iespana.es/capitulo3.htm>

  20090820

- **Ancho de Banda**

  <http://www.alfredcertain.com/?p=9>

  20090821

- **Retardo**

  <http://proyectovoip.com/voip.htm>

  20090821

- **Jitter**

  <http://wiki.it46.se/doku.php/voip4d/capitulo_3/calidad_servicio>

  20090821

- **Pérdida de Paquetes**

  <http://www.venta-visual.com/productos/prod-3-com/com_pdf/3.6.Tecnicos_com/videoconferencia_QoS_vve.pdf>

  20090821

ARQUITECTURAS DE QOS

- **Mejor Esfuerzo**

  <http://www.microsoft.com/spain/technet/recursos/articulos/cg0306.mspx>

  20091021

- **IntServ**

  <http://jpadilla.docentes.upbbga.edu.co/QoS/IntServ1%20conceptos%20basicos.pdf>

  20091023

- **Diffserv**

  <http://gitaca.es/javiercg/uploads/ES/jimenez05jitel.pdf>

  20091024

TÉCNICAS DE ENCOLAMIENTO

- **Fifo**

  <http://www.gesein.com/docs/QoSE.pdf>

  20091101

- **Encolamiento de Prioridad**

  <http://www.scielo.cl/pdf/rfacing/v13n3/art15.pdf>

  20091102

- **Encolamiento Ponderado**

  <http://www.tdx.cesca.es/TESIS_UPC/AVAILABLE/TDX-1204101-085733/07capitol4.pdf>

  20091103

MIKROTIK

- **Instalación**

  <http://wiki.mikrotik.com/wiki/RouterOS_features>

  20091205

- **Licenciamiento**

  <http://wiki.mikrotik.com/wiki/All_about_licenses>

  20091207

- **Interfaces**

  <http://wiki.mikrotik.com/wiki/Interface/General>

  20091208

- **QoS**

  <http://mum.mikrotik.com/presentations/CZ09/QoS_Megis.pdf>

  20091208

- **Configuración OSPF**

  <http://wiki.mikrotik.com/wiki/OSPF-examples>

  20091214

- **Configuración MPLS**

  <http://wiki.mikrotik.com/wiki/MPLS>

  20091215

- **Queue**

  <http://wiki.mikrotik.com/wiki/Queue>

  20100105

- **IP**

  <http://wiki.mikrotik.com/wiki/IP/Address>

  20100110

MULTIPROTOCOL LABEL SWITCHING

- **Conmutación**

  <http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml>

  20091222

- **Routing**

  <http://www.juniper.net/techpubs/software/junos/junos53/swconfig53-mpls- apps/html/mpls-overview32.html>

  20100114