ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

"ANÁLISIS DEL RENDIMIENTO DE FRAME RELAY VS ETHERNET SOBRE UNA ARQUITECTURA MPLS"

TESIS DE GRADO

Previa a la obtención del título de

INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

Presentado por:

EDISON XAVIER BAYAS MOPOSITA

MÓNICA JEANETH CUNALATA PILLA

RIOBAMBA – ECUADOR
2013

AGRADECIMIENTO

A Dios por haberme permitido llegar hasta este punto y haberme dado salud y fuerza para lograr mis objetivos.

A mi familia por todo el cariño y la paciencia durante éste difícil camino.

A los docentes de la Escuela de Ingeniería Electrónica por sus valiosas enseñanzas y por permitirme robar parte de su tiempo y realizar este proyecto.

A las personas que me han acompañado en mis múltiples travesías Sofía, Cristian y Liliana. Gracias por su amistad y cariño, ustedes son parte fundamental de este ciclo de mi vida.

Mónica.

Al cuerpo docente de la ESPOCH que acertadamente transmite su sabiduría a la juventud soñadora del país.

A mis amigas y amigos que hicieron de mi estadía algo única e inolvidable.

A aquel Poder Divino que influyó en la consecución de tan ansiado objetivo, y a toda aquella persona con la cual tuve el inmenso honor de compartir, les expreso mi más profunda gratitud plasmada aquí en estas hojas, pero sobre todo, en mi corazón.

Edison.

DEDICATORIA

A las personas más importantes de mi vida mis padres Luis y María, por haberme apoyado en todo momento, por sus consejos, sus valores, por la confianza por la preocupación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.

A mis hermanos por haber siempre estado junto a mí en cada momento brindándome su cariño y constante motivación.

Mónica.

Por la profunda confianza y la paciencia hacia mi persona, este trabajo está dedicado a mi familia, en cuyo calor he podido conocer el verdadero sentido de la vida, a pesar de altibajos que la vida tiene; han sido ellos, la razón para imponerme nuevos y ambiciosos retos pero, sobre todo, han sido y serán la fuente del valor para alcanzarlos.

Edison.

FIRMAS RESPONSABLES Y NOTA

NOMBRE	FIRMA	FECHA
Ing. Iván Menes **DECANO FACULTAD INFORMÁTICA Y ELECTRÓNICA**	……..	……..
Ing. Wilson Baldeón **DIRECTOR DE LA ESCUELA ING. EN ELECTRÓNICA, TELECOMUNICACIONES Y REDES**	……..	……..
Ing. Marcelo Donoso **DIRECTOR DE TESIS**	……..	……..
Ing. Franklin Moreno **MIEMBRO DEL TRIBUNAL**	……..	……..
Tlgo. Carlos Rodríguez **DIRECTOR CENTRO DE DOCUMENTACIÓN**	……..	……..

NOTA DE LA TESIS: ……

RESPONSABILIDAD DEL AUTOR

"Yo, Edison Xavier Bayas Moposita junto con Mónica Jeaneth Cunalata Pilla, 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".

Edison Xavier Bayas Moposita

Mónica Jeaneth Cunalata Pilla

ÍNDICE DE ABREVIATURAS

ANSI	American National Standardization Institute
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
AToM	Any Transport Over MPLS
BECN	Backward Error Congestion Notification
BGP	Border Gateway Protocol
BW	Bandwidth
CEF	Cisco Express Forwarding
CIR	Committed Information Rate
CME	Call Manager Express
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSU	Channel Service Unit
DCE	Data Circuit-Terminating Equipment
DIFFSERV	Differenced Serviced
DLCI	Data Link Connection Identifier
DS	Differentiated Services
DSCP	Differentiated Services Code Point
DSU	Data Service Unit
DTE	Data Terminal Equipment
ETH	Ethernet
EXP	Experimental
FCS	Frame Check Sequence
FEC	Forwarding Equivalence Class
FECN	Forward Explicit Congestion Notification
FIFO	First In, First Out
FLIB	Forward Label Information Base
FR	Frame Relay
GMPLS	Generalized Multi-Protocol Label Switching

GNS3	Graphical Network Simulator
HDLC	High-Level Data Link Control
IAB	Internet Architecture Board
IARP	Inverse ARP
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
INTSERV	Integrated services
IOS	Internetworking Operating System
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
ISO	International Standardization Organization
ISOC	Internet Society
ITU-T	International Telecommunications Union- Telecommunications
LAN	Local Area Network
LAPD	Link Access Protocol for D-Channel
LDP	Label Distribution Protocol
LER	Label Edge Router
LIF	Label Information Base
LMI	Local Management Interface
LSP	Label Switched Path
LSR	Label Switch Router
MAC	Media Access Control
MPLS	Multi-Protocol Label Switching
NSP	Service Network Provider
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PE	Provider Edge
PPP	Point-to-Point Protocol

PVC	Private Virtual Circuit
RT	Real Time
NRT	Non Real Time
PW	Pseudo wire
QoS	Quality of Service
RFC	Request for Comments
RSVP	Resource Reservation Protocol
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SNMP	Simple Network management Protocol
SVC	Switched Virtual Circuit
TCP/IP	Transmission Control Protocol/Internet Protocol
TE	Traffic Engineering
ToS	Type of Service
TTL	Time to Live
VLAN	Virtual Local Area Network
VPN	Virtual private network
VPWS	Private Wire Service
VRF	Virtual Routing and Forwarding
W3C	World Wide Web Consortium

INDICE GENERAL

INDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En el presente trabajo denominado “ANÁLISIS DEL RENDIMIENTO DE FRAME RELAY vs ETHERNET SOBRE UNA ARQUITECTURA MPLS”, se pretende identificar la tecnología que ofrece el mejor rendimiento y acople a la moderna tecnología MPLS la mismo que es el estándar de facto para actuales y futuras redes de Telecomunicaciones.

Se ha considerado a Ethernet dentro de este análisis debido a su rápida evolución tecnológica y su masiva presencia en las redes LAN, mientras que Frame Relay esta implementada en la mayoría de redes de transporte de alta velocidad, MPLS en cambio permite la integración de tecnologías de capa 2 y una elevada tasa de transmisión.

Es por ello que se hace indispensable conocer el comportamiento de las tecnologías Ethernet y Frame Relay mientras cruzan a través de un dominio MPLS, integrando servicios con alto grado de confiabilidad y rapidez. Este análisis permitirá, de acuerdo al entorno, elegir la combinación tecnológica adecuada.

Para alcanzar los objetivos propuestos se realizaran mediciones para cinco indicadores considerados como críticos en el rendimiento de una red, los cuales son: latencia, jitter, velocidad de transmisión, retardo, pérdida de paquetes. Estas mediciones serán realizadas en diferentes escenarios que contienen las siguientes combinaciones de tecnologías: ETHERNET+LDP, ETHERNET+RSVP, FRAME RELAY+LDP Y FRAME RELAY+RSVP, siendo LDP y RSVP protocolos de señalización de soporte de MPLS los cuales también serán evaluados.

Este documento consta de cuatro capítulos distribuidos de la siguiente manera:

En el Capítulo I tenemos el Marco Referencial donde se expone la importancia del presente trabajo y una breve reseña evolutiva de las redes de computadoras; así como también se definen los objetivos a alcanzarse junto a una propuesta hipotética inicial.

En el Capítulo II se desarrolla la conceptualización teórica necesaria para la comprensión de las distintas tecnologías a analizarse en este trabajo las mismas que servirán para realizar el posterior diseño de los escenarios e interpretación de resultados.

En el Capítulo III denominado Diseño y Simulación se proponen los distintos escenarios que serán simulados en la plataforma de GNS3, de los cuales se extraerán datos de los indicadores, con las herramientas VQManager, NetTools.

Finalmente en el Capítulo IV se realiza el análisis de los datos obtenidos en el capítulo anterior y su respectiva interpretación. A través de la comparación de estos resultados se llegara definir la tecnología que ofrezca el mejor rendimiento dentro de la arquitectura MPLS.

CAPÍTULO I

MARCO REFERENCIAL

1.1. Antecedentes

La compleja estructura de la red mundial de datos que poseemos en la actualidad es el resultado de décadas de investigación en busca de mejores algoritmos que permitan entregar los paquetes de datos eficientemente, por supuesto, este avance ha sido apoyado por la evolución tecnológica que ha permitido la construcción de potentes ordenadores especializados en el tratamiento de los flujos de información en la red.

Cuando la internet fue diseñada e implementada con el protocolo IP, durante la segunda mitad del siglo anterior, no se tomaron en consideración aspectos como el retardo, tasa de perdidas, Jitter, seguridad, volumen de tráfico entre otros parámetros que hoy en día son los factores determinantes para tener un fluido y convergente sistema de comunicaciones.

Gran parte de la infraestructura de redes de voz y datos esta soportada por una variedad de tecnologías y, muchas veces los servicios que se prestan se ven limitados debido a la rapidez con que crecen los requerimientos de los usuarios, sobre todo en lo que concierne a la transmisión de voz y video. En pro de mejorar dichos servicios el IETF, a través de su grupo de trabajo de MPLS expide un nuevo estándar resumido en el RFC 3031 conocido como MPLS, Multi Protocol Label Switching.

Esta variedad de tecnologías son el principal inconveniente para lograr la convergencia de redes y servicios.

Las empresas de Telecomunicaciones no son la excepción a esta realidad, su infraestructura ha ido evolucionando conforme el paso de los años y, por consiguiente, es una mezcla conjunta de tecnologías, protocolos y servicios.

Por consiguiente estas empresas, requieren tener un estudio acerca de las tecnologías que mejor se adapten a la infraestructura disponible y la demanda de los usuarios, incorporando indicadores que puedan ser mensurables tales como: la velocidad de transmisión, capacidad de transmisión, throughput, etc., los mismos que permiten una comparación entre tecnologías.

Debido al diseño mismo del protocolo, MPLS posibilita la asignación de recursos a través de VPN's, calidad de servicio (QoS) basada en la Clase de servicio (CoS) y, por supuesto, la realización de ingeniería de tráfico (TE).

1.2. Justificación

Gran parte de la infraestructura de redes de voz y datos está basada en Frame Relay y en los últimos años la tecnología Ethernet se ha difundido en la mayor parte de las redes de acceso convirtiéndose estas dos en las tecnologías más usadas y, que requieren su inmediata integración a una NGN con la finalidad de garantizar la óptima prestación de servicios.

Los problemas de incompatibilidad con tecnologías de capa de enlace, necesidad de ingeniería de tráfico, redefinición de algoritmos de enrutamiento, entre otros, lo cual es percibido por el cliente como un bajo rendimiento de la red dan lugar a la incertidumbre por parte de cualquier empresa de telecomunicaciones por conocer la evaluación del comportamiento de las actuales redes y la posible migración de una en común.

Es así que en el presente trabajo, a través de una adecuada herramienta de simulación, se pretende determinar la tecnología que provea el mejor rendimiento, respaldando estos conocimientos con datos obtenidos en escenario virtual que permita cuantificar la calidad de la red ante cierta topología. Se tienen como alternativas de estudio herramientas como: OPNET, NS, OMNEST, OPNET IT, OMNET, GNS3, etc.

La investigación también se enfoca en el estudio de LDP y RSVP como protocolos de creación y distribución de etiquetas con los que MPLS construye las mejores rutas, identificado las mejores características de cada uno de ellos. Estos se probaran en dos topologías MPLS de similares características donde transiten Frame Relay y Ethernet respectivamente, dando como resultado cuatro escenarios de simulación los cuales a son descritos a continuación:

- **Escenario 1:** Ethernet como tecnología de acceso y LDP como protocolo de creación y distribución de etiquetas.

- **Escenario 2:** Ethernet como tecnología de acceso y RSVP como protocolo de creación y distribución de etiquetas.

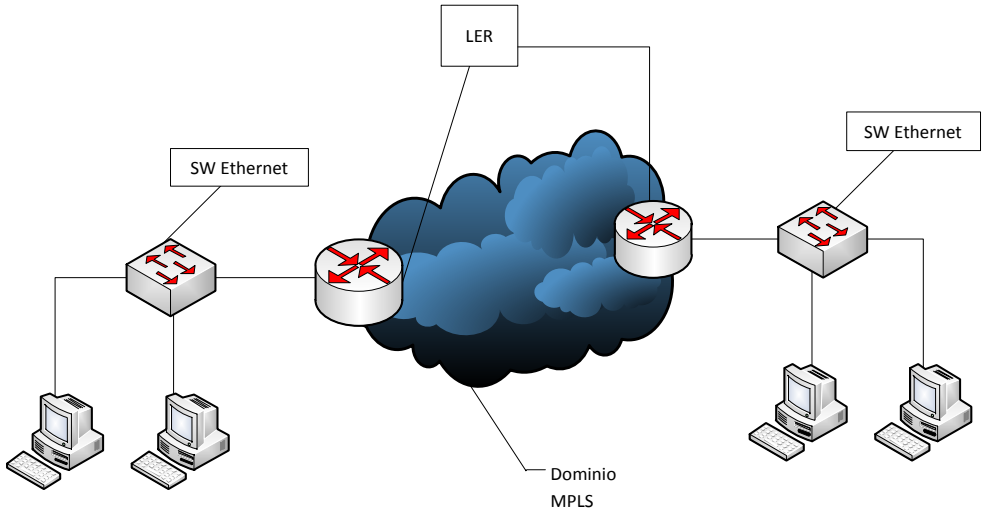


Figura I-1 Topología Ethernet sobre MPLS propuesta

- **Escenario 3:** Frame Relay como tecnología de acceso y LDP como protocolo de creación y distribución de etiquetas.
- **Escenario 4:** Frame Relay como tecnología de acceso y RSVP como protocolo de creación y distribución de etiquetas.

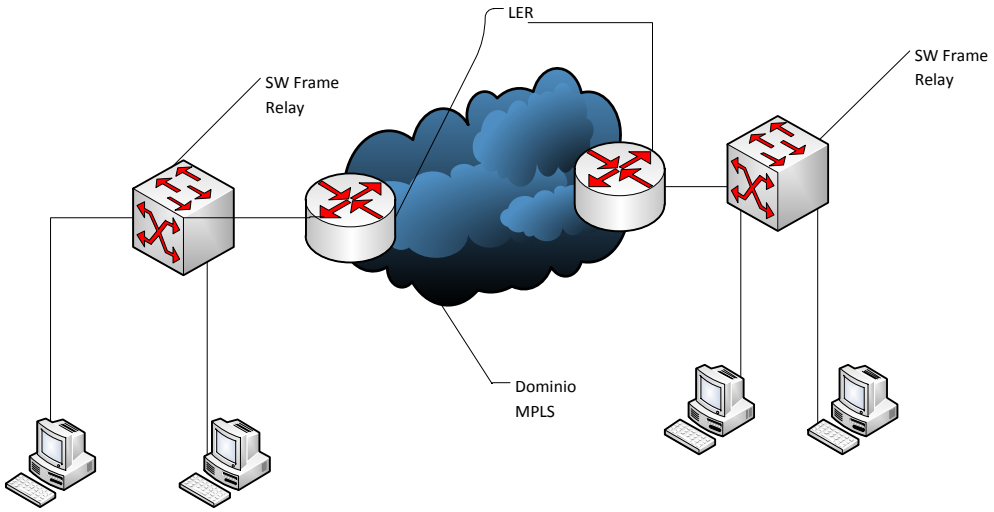


Figura I-2 Topología Frame Relay sobre MPLS propuesta.

Es así que se pretende corroborar la viabilidad de MPLS como la arquitectura de red que permite la descongestión del BackBone a través de una correcta distribución de los flujos de acuerdo a sus prioridades y, además como la plataforma ideal para la convergencia de las múltiples tecnologías de acceso existentes, lo cual, posibilita una rápida migración con un moderado nivel de complejidad.

1.3. Objetivos

1.3.1. Objetivos generales

- Analizar el rendimiento de Frame Relay vs Ethernet sobre una arquitectura MPLS, usando LDP y RSVP.

1.3.2. Objetivos específicos

- Estudiar los conceptos que caracterizan a las tecnologías MPLS, Frame Relay y Ethernet encontrado así parámetros que posibilitan la convergencia de las mismas.
- Diseñar y simular una topología que incorpore todas las tecnologías antes mencionadas.
- Medir y analizar los parámetros que definen el rendimiento en una red MPLS donde transitan Frame Relay y Ethernet.
- Elaborar una guía técnica que permita la implementación de la topología que muestre los mejores resultados de rendimiento.

1.4. Hipótesis

Las redes Ethernet sobre una arquitectura MPLS proporcionará un mejor rendimiento que una red Frame Relay bajo similares condiciones de prueba.

CAPÍTULO II

MARCO TEÓRICO

El presente capítulo se dedica al estudio teórico de la tecnología MPLS y todos aquellos protocolos involucrados en el desarrollo del presente estudio. Este capítulo es de suma importancia ya que permite conocer técnicamente la operación de las tecnologías, e inducir las consecuencias de la combinación de las mismas sin necesidad de construir un escenario real.

Se exponen las características de las tecnologías, los formatos de los paquetes o tramas, ventajas y desventajas, entre otros aspectos relacionados con el funcionamiento de las mismas**.**

Principalmente, este capítulo, se centra en el estudio de la tecnología MPLS y su tecnología AToM. Se estudia como ésta realiza el transporte de cualquier trama de capa 2, las posibilidades de ingeniería de tráfico que AToM posee, la recuperación de rutas, entre otras.

2.1. Introducción

En el presente capítulo se detalla los conceptos básicos que describen las diferentes tecnologías que intervienen en este trabajo, como son MPLS, Ethernet y Frame Relay entre otros que son fundamentales para entender como fluye la información a través de una red de datos. Principalmente se conceptualiza los aspectos generales de MPLS, sus características y funcionamiento necesarios para administrar el tráfico así como sus modos de funcionamiento Modo Cell y Modo Frame.

Se hace también una introducción al estudio a las diferentes tecnologías de las cuales se apoya MPLS para el transporte de diferentes tipos de tráfico como es AToM.

2.2. Descripción y Operación de las Tecnologías

2.2.1. Protocolo IP

Es un protocolo de comunicación de datos digitales clasificado funcionalmente en la Capa de Red según el modelo internacional OSI

Su función principal es el uso bidireccional en origen o destino de comunicación para transmitir datos mediante un protocolo no orientado a conexión que transfiere paquetes conmutados a través de distintas redes físicas previamente enlazadas según la norma OSI de enlace de datos.

El diseño del protocolo IP se realizó presuponiendo que la entrega de los paquetes de datos sería no confiable por lo cual IP tratará de realizarla del mejor modo posible, mediante técnicas de encaminamiento, sin garantías de alcanzar el destino final pero tratando de buscar la mejor ruta entre las conocidas por la máquina que esté usando IP.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o en cuyas cabeceras se encuentran las direcciones de las máquinas de origen y destino.

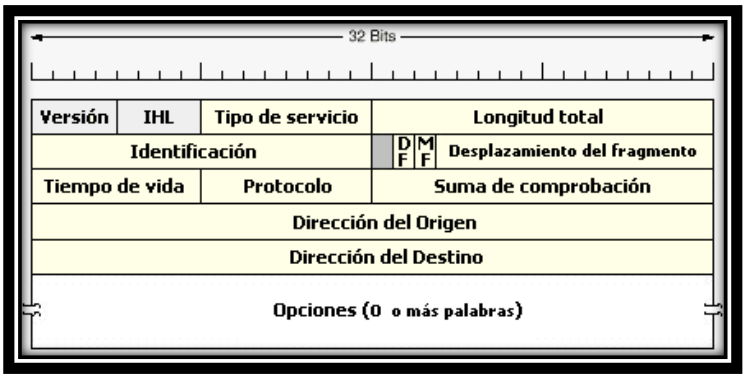


Figura II-1 Cabecer IP

Fuente: http://www.wikilearning.com/

2.2.2. Ethernet

Ethernet es una popular tecnología LAN que utiliza el acceso múltiple con portadora y detección de colisiones CSMA/CD[1] entre estaciones con diversos tipos de cables.

La red Ethernet, es una tecnología de bus de difusión, que se conoce como entrega con el mejor esfuerzo y un control de acceso distribuido. Es un bus debido a que todas las estaciones comparten un sólo canal de comunicación, es de difusión porque todos los transceptores reciben todas las transmisiones. La trama es lo que se conoce también por el nombre de "frame".

[1] **CSMA/CD**.- *Carrier Sense Multiple Access with Collision Detection*, Acceso Múltiple con Escucha de Portadora y Detección de Colisiones, es un protocolo usado en las redes multi-acceso (como Ethernet) que controla el uso de los recursos por porte de los dispositivos de red. Desarrollado por grupo de trabajo IEEE 802.3 (Ethernet).

Preambulo	Delimitador de inicio de trama	MAC de destino	MAC de origen	802.1Q Etiqueta(opcional)	Ethertype (Ethernet II) o longitud (IEEE 802.3)	Payload	Secuencia de comprobación (32-bit CRC)	Gap entre frames
7 Bytes	1 Byte	6 Byte	6 Bytes	(4 Bytes)	2 Bytes	De 46 (o 42) hasta 1500 Bytes	4 Bytes	12 Bytes
		64–1522 Bytes						
72–1530 Bytes								
84–1542 Bytes								

Figura II-2 Trama Ethernet

- **Preámbulo.-** Indica el inicio de la trama y tiene el objeto de que el dispositivo que lo recibe detecte una nueva trama y se sincronice.
- **Delimitador de inicio de trama.-** Indica que el frame empieza a partir de él.
- **Los campos de MAC (o dirección) de destino y origen.-** Indican las direcciones físicas del dispositivo al que van dirigidos los datos y del dispositivo origen de los datos, respectivamente.
- **La etiqueta 802.1Q.-** Es un campo opcional que indica la pertenencia a una VLAN o prioridad en IEEE P802.1p.
- **Ethernetype.-** Indica con que protocolo están encapsulados los datos que contiene la Payload, en caso de que se use un protocolo de capa superior.
- **Payload.-** Es donde van todos los datos y, en el caso correspondiente, cabeceras de otros protocolos de capas superiores que pudieran formatear a los datos que se tramiten (IP, TCP, etc). Tiene un mínimo de 46 Bytes (o 42 si es la versión 802.1Q) hasta un máximo de 1500 Bytes.
- **Secuencia de comprobación.-** Es un campo de 4 bytes que contiene un valor de verificación CRC[2]. El emisor calcula el CRC de toda la trama, desde el campo destino al

[2] **CRC.-** Inventado y propuesto por W. Wesley Peterson en un artículo publicado en 1961, el código de redundancia cíclica se usa para la detección de errores en redes de datos y medios de almacenamiento.

campo CRC suponiendo que vale 0. El receptor lo recalcula, si el valor calculado es 0 la trama es válida.

- **Gap.-** Final de trama. Son 12 bytes vacíos con el objetivo de espaciado entre tramas.

2.2.2.1. Principio de Transmisión

Todos los equipos de una red Ethernet están conectados a la misma línea de transmisión y la comunicación se lleva a cabo por medio de la utilización un protocolo denominado CSMA/CD (Carrier Sense Multiple Access with Collision Detect que significa que es un protocolo de acceso múltiple que monitorea la portadora: detección de portadora y detección de colisiones).

Con este protocolo cualquier equipo está autorizado a transmitir a través de la línea en cualquier momento y sin ninguna prioridad entre ellos. Esta comunicación se realiza de manera simple:

- Cada equipo verifica que no haya ninguna comunicación en la línea antes de transmitir.
- Si dos equipos transmiten simultáneamente, entonces se produce una colisión (o sea, varias tramas de datos se ubican en la línea al mismo tiempo).
- Los dos equipos interrumpen su comunicación y esperan un período de tiempo aleatorio, luego una vez que el primero ha excedido el período de tiempo, puede volver a transmitir.

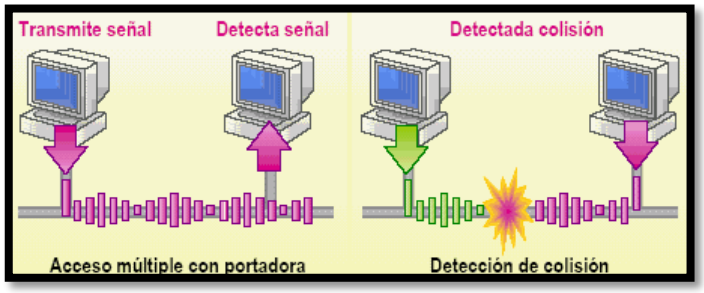


Figura II-3 Detección de colisiones

2.2.2.2. Hardware

En esencia, los elementos de una red Ethernet son: tarjetas de red, repetidores, concentradores, puentes, conmutadores, nodos de red y los medios de interconexión.

Los nodos de red pueden clasificarse en dos grandes grupos: equipo terminal de datos (DTE) y equipo de comunicación de datos (DCE).

Los DTE son dispositivos de red que generan el destino de los datos: los PC, enrutadores (router), las estaciones de trabajo, los servidores de archivos, los servidores de impresión; todos son parte del grupo de las estaciones finales.

Los DCE son los dispositivos de red intermediarios que reciben y retransmiten las tramas dentro de la red; pueden ser: conmutadores (switch), concentradores (hub), repetidores o interfaces de comunicación. Por ejemplo: un módem o una tarjeta de interfaz.

Ethernet se ha convertido en la tecnología de redes de área local más extendida en el mundo. Diseñada originalmente por una alianza entre Digital, Intel y Xerox con el nombre de Ethernet DIX, pasó a ser un estándar en 1983 cuando el IEEE recoge sus especificaciones y lo publica como Ethernet 802.3., esta ha sido la tecnología con mayor desarrollo tecnológico en el campo de las redes de datos y, en la actualidad proporciona velocidades en el orden de los Gbps y se lo aplica también a redes de área metropolitana.

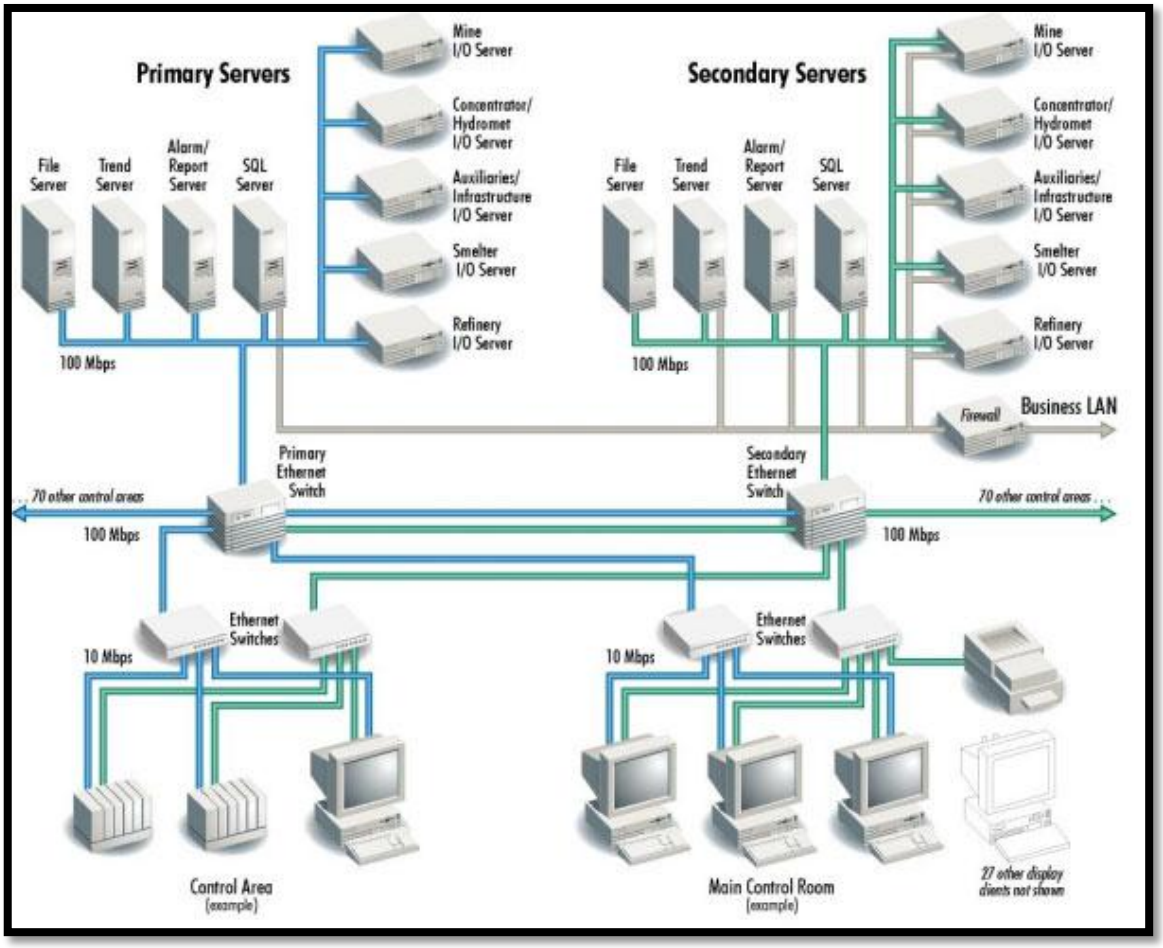


Figura II-4 Arquitectura Ethernet

2.2.3. Frame Relay

Frame Relay (FR), es una tecnología de conmutación rápida de tramas, basada en estándares internacionales, que puede utilizarse como un protocolo de transporte y como un protocolo de acceso en redes públicas o privadas proporcionando servicios de comunicaciones. Este, usa circuitos virtuales para conexión de ancho de banda por demanda.

Dichos circuitos son conocidos como identificadores de enlaces de conexión (DLCI) y proveen una ruta virtual a cada sitio remoto.

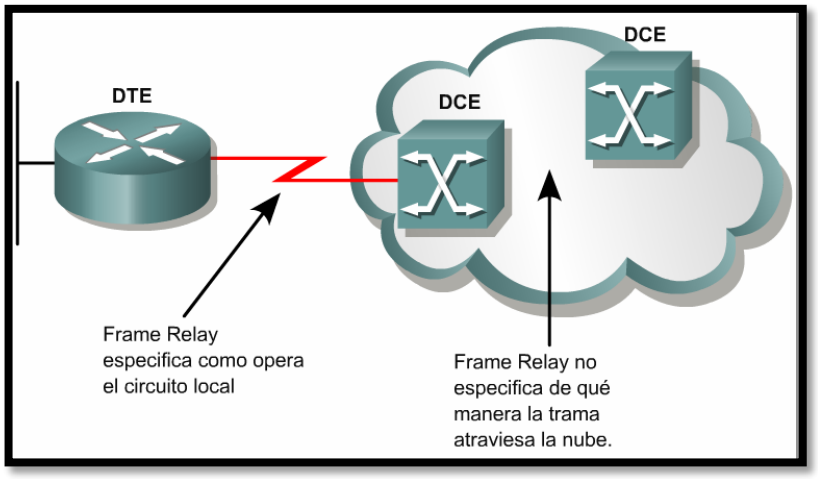


Figura II-5 Enlace FR

Frame relay es un sub conjunto del protocolo LAPD para proveer multiplexación estática a la velocidad de 50 Mbps manejando tráfico de ráfagas. El alto grado de performance de FR se debe a la calidad de las líneas, que permitieron eliminar la necesidad de recuperar errores y las funciones de control que tenían muchos protocolos anteriores.

Las redes FR se construyen partiendo de un equipamiento de usuario que se encarga de empaquetar todas las tramas de los protocolos existentes en una única trama FR.

Los dispositivos FR se dividen en dos grupos:

- **DTE**, Data Terminal Equipment.- Equipo del cliente que finaliza la conexión FR.
- **DCE**, Data Circuit-Terminating Equipment.- Son los dispositivos de red propiedad del proveedor.

Sus enlaces seriales deben ser conectados adecuadamente. Típicamente la tarea se reduce a identificar la terminal DCE que posibilita la señal de sincronización.

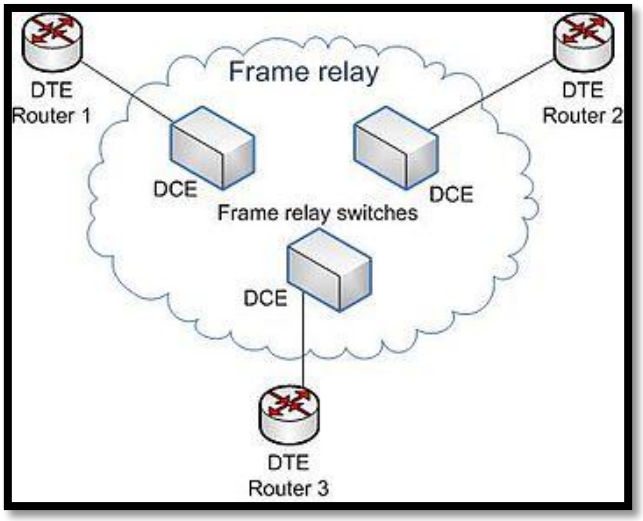


Figura II-6 Dispositivos FR

2.2.3.1. Terminología Frame Relay

Los siguientes termino son especialmente distinguibles en los sistemas FR, y pueda que tengan un significado único en estos, entonces es necesario conocer y entender su significado.

- **PVC**.- Circuito virtual permanente. Circuito virtual que se establece de forma permanente. Los PVC permiten ahorrar ancho de banda asociado con el establecimiento y corte de circuitos si determinados circuitos virtuales deben existir en todo momento.
- **SVC**.- Circuito virtual conmutado. Circuito virtual que se establece de forma dinámica por pedido y que se interrumpe cuando la transmisión se completa. Los SVC se utilizan cuando la transmisión de datos es esporádica.
- **DLCI**.- Identificador de conexión de enlace de datos. Valor que especifica un PVC o SVC en una red FR. En la especificación FR básica, los DLCI son significativos a nivel local (los dispositivos conectados pueden usar distintos valores para especificar la misma conexión). En la especificación LMI extendida, los DLCI son significativos a nivel global (los DLCI especifican dispositivos finales individuales).

- **CIR**.- Velocidad de información suscrita. Velocidad a la cual una red FR acepta transferir información en condiciones normales, con un promedio sobre un incremento de tiempo mínimo. La CIR, que se mide en bits por segundo, es una de las métricas clave del tráfico negociado.
- **IARP**.- Protocolo de resolución de direcciones inverso. Método para crear rutas dinámicas en una red. Permite que un dispositivo detecte la dirección de red de otro asociado a través de un circuito virtual.
- **LMI**.- Interfaz de administración local. Conjunto de mejoras para la especificación FR básica. La LMI[3] incluye soporte para un mecanismo de mensajes de actividad, que verifica que los datos fluyan; un mecanismo de multicast, que proporciona al servidor de red su DLCI local y el DLCI multicast; direccionamiento global, que proporciona a los DLCI significado global en lugar de simplemente significado local en la red FR.
- **FECN**.- Notificación explícita de congestión. Bit establecido por una red FR para informar al DTE que recibe la trama que se ha experimentado congestión en la ruta desde el origen hacia el destino. Los DTE que reciben tramas con el bit FECN establecido pueden solicitar que los protocolos de mayor nivel tomen las acciones de control de flujo que sean necesarias.
- **BECN**.- Notificación retrospectiva de congestión en la red. Bit establecido por una red FR en las tramas que viajan en dirección opuesta a las tramas que encuentran una ruta congestionada. Los DTE que reciben tramas con el bit BECN ya establecido pueden solicitar que los protocolos de mayor nivel tomen las acciones de control de flujo que sean necesarias.

[3] **LMI**.- Local Managnet Interface, es el estándar de señalización entre los DCE y DTE. Pueden ser 3 tipos: cisco, ansi y q933a.

2.2.3.2. Topologías FR

Una de las cuestiones más útiles que ofrece FR es la flexibilidad de conexión hacia la nube FR. El proveedor ofrece circuitos virtuales capaces de interconectar los sitios remotos con una topología particular.

- **Topología de malla completa.-** Todos los enrutadores disponen de circuitos virtuales al resto de los destinos.
- **Topología de malla parcial.-** Es un tipo de malla completa pero no todos los sitios tienen acceso a los demás.
- **Topología en estrella.-** Los sitios remotos están conectados a un punto central que por lo general ofrece un servicio o una aplicación.

2.2.3.3. Trama Frame Relay

Las tramas y cabeceras de FR pueden tener diferentes longitudes, ya que hay una gran variedad de opciones disponibles en la implementación, conocidos como anexos a las definiciones del estándar básico. La información transmitida en una trama FR puede oscilar entre 1 y 8.000 bytes, aunque por defecto es de 1.600 bytes.

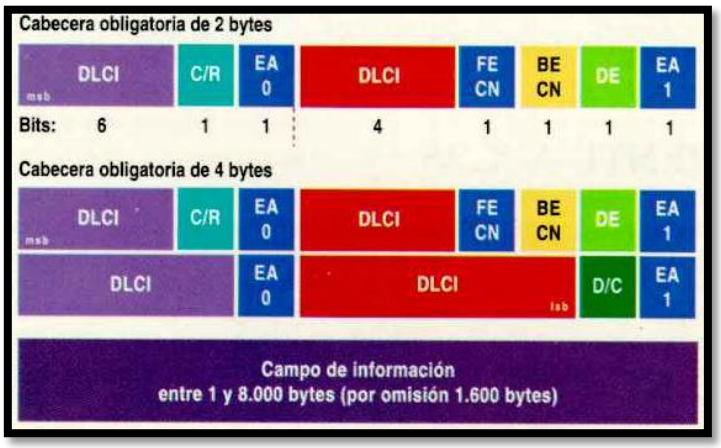


Figura II-7 Trama FR

- **Señalador.-** Indica el principio y el final de la trama FR.
- **Dirección.-** Indica la longitud del campo de dirección. La Dirección contiene la siguiente información:
    - **Valor DLCI.-** Indica el valor de DLCI. Se compone de los 10 primeros bits del campo Dirección.
    - **Control de congestión.-** Los últimos 3 bits del campo de dirección, que controlan los mecanismos de notificación de congestión FR. Estos son FECN, BECN y bits posibles para descarte (DE).
- **Datos.-** Campo de longitud variable que contiene datos de capa superior encapsulados.
- **FCS.-** Secuencia de verificación de trama (FCS), utilizada para asegurar la integridad de los datos transmitidos

2.2.3.4. Funcionamiento de Frame Relay

Cada circuito virtual está identificado de forma única por un DLCI local, lo que permite distinguir que enrutador está conectado a cada interfaz. Es posible configurar manualmente una asignación estática en la tabla de asignaciones del enrutador para poder describir la relación entre el Circuito Virtual y la dirección de capa tres del otro extremo. Las direcciones pueden asignarse también de forma dinámica mediante ARP inverso que asocia un DLCI con la dirección del siguiente salto. Las LMI son responsables de la administración y el mantenimiento del estado de enlace de los dispositivos. Los LMI son configurables, aunque las versiones actuales de IOS las detectan automáticamente.

Existen tres tipos de LMI:

- Cisco, definidas para equipos cisco.
- ANSI

- Q933a

Para iniciar el proceso de comunicación se deben producir los siguientes pasos:

- Cada enrutador es conectado al conmutador FR por medio de un CSU/DSU[4].
- El enrutador indaga el estado del circuito virtual.
- Cuando el conmutador FR recibe la petición responde informando los DLCI locales de los PVC a los enrutador remotos.
- Por cada DLCI activo los enrutadores envían un paquete ARP inverso que contiene la dirección IP correspondiente a cada Circuito Virtual.
- Los enrutadores remotos crean tablas que incluyen los DLCI locales y las direcciones IP.
- Cada 60 segundos se envían los mensajes ARP inverso.
- Cada 10 segundos se intercambia información LMI.

Dentro de la nube Frame Relay el conmutador crea tablas con la relación que tienen cada puerto/slot con los DLCI de los enrutadores remotos. FR utiliza Horizonte Dividido para evitar bucles de enrutamiento.

2.3. MPLS

En el reenvío convencional mediante IP, cada enrutador es el responsable de tomar la decisión del camino o, interfaz adecuada en función de la información de la cabecera IP. Esto requiere que el dispositivo realice un profundo análisis de cabeceras y de las tablas de encaminamiento para tomar dicha decisión, proceso que se lo hace por cada paquete que le llega una de sus

[4] **CSU/DSU**.- Channel Service Unit/Data Service Unit, dispositivo de interfaz digital que adapta las interfaces físicas en una red de portadora conmutada.

interfaces. Realizar todo este proceso requiere un elevado uso de recurso en el enrutador en cuestión.

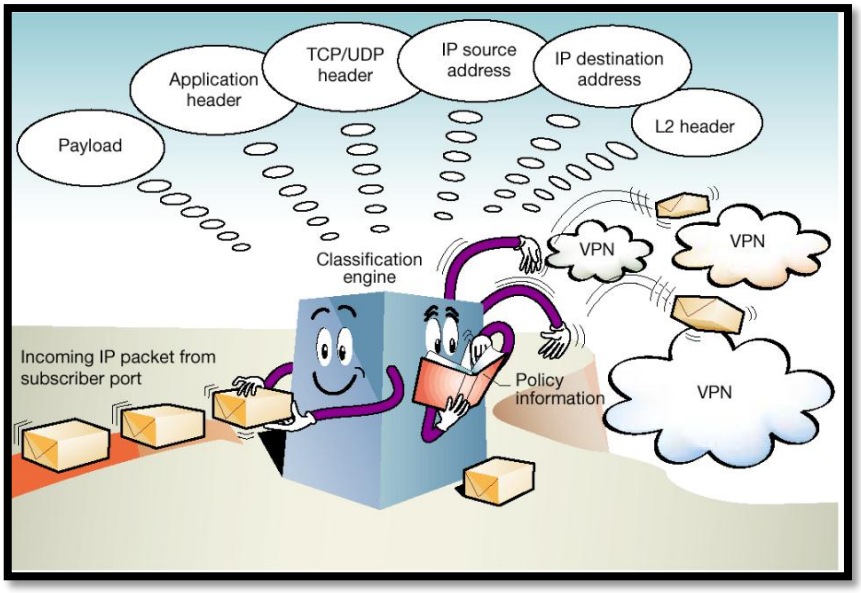


Figura II-8 Enrutamiento clásico de paquetes de datos

Fuente: (Almeida, 2012)

Los avances en hardware y software han incrementado la capacidad neta de renvió de los enrutadores. A pesar de esto, cuestiones como la flexibilidad en el reenvío, alcanzar el mínimo tiempo de procesamiento por paquete y la adaptación del mismo a las distintas tecnologías de transporte has sido el principal impedimento para mejorar la eficiencia de la red y la QoS. Así, surge le ingeniería de tráfico como principal técnica para mitigar estos defectos.

MPLS es el último avance en cuanto a tecnologías de enrutamiento/reenvió en redes IP se refiere y supone un nuevo pensamiento en el proceso de diseño. E s un estándar del IETF y está definido en la RFC 3031 (Rosen, y otros, 2001).

Entre los objetivos más sobresalientes en la elaboración del estándar se destacan los siguientes:

- Independencia de la tecnología de enlace en el modelo de referencia OSI.

- Soporte multiprotocolo.
- Posibilidad de envíos multicast.
- Compatibilidad con IntServ/DIffServ.
- Coexistencia con otras plataformas de transporte de datos.
- Posibilidad de operaciones de soporte y gestión de red, característicos en las redes IP.

2.3.1. Características

2.3.1.1. QoS (Quality of Service)

Durante los últimos años se ha trabajado por conseguir una red en la que puedan converger todos los servicios ofrecidos por los proveedores. En parte, esto ha sido posible debido a la masiva implantación del Protocolo de Internet, IP. El internet fue desarrollado con fines académicos y con el paso de los años se han encontrado en éste muchas oportunidades de negocios lo cual ha ido, hasta cierto punto, saturando la red. Por esto, muchos servicios no alcanzan el adecuado nivel de calidad.

Considerando que los usuarios principalmente consideran el factor calidad como el más importante, desarrollar técnicas que permitan sobrellevar la congestión en las redes es una prioridad.

Esta preocupación se atenúa aún más cuando consideramos tráficos de tiempo real. Supóngase un servicio telefónico en el cual no le se asegure que su interlocutor lo escuche o, por lo menos lo entienda, seguramente nadie pagaría por ese servicio (IETF, 1998).

Cuando tratamos con paquetes de dato solamente los retardos, o su variación, no son relevantes. Sin embargo un retardo superior a 150 milisegundos hace que las comunicaciones telefónicas se tornen difíciles de entender y, más allá de los 300 milisegundos, se convierten en

imposibles. Así de sensible al retardo son las transmisiones multimedia que requieren de interactividad (Cisco Systems, 2006).

La pérdida de los paquetes también es importante. Aunque en la transmisión de datos, esto se supera gracias a las retransmisiones, esta práctica no da resultados en las transmisiones multimedia interactivas.

Es necesario aclarar que las aplicaciones de streaming son aplicaciones de voz sobre IP, pero no son aplicaciones interactivas, son comunicaciones en un solo sentido. Hoy en día la radio en internet es muy popular, no dado mayores problemas en su recepción a menos que se tenga una lenta conexión de internet. Esto se debe a que en esta aplicación, el retardo es combatido con un buffer y la pérdida de paquetes con mecanismos tradiciones de recuperación y retransmisión.

La variación del retardo, técnicamente denominado Jitter, es otro parámetro a considerarse. Este influye directamente en la cadencia a la cual se reconstruye la señal. Altos valores de Jitter imposibilita sincronizar la señal recuperada a la velocidad a la que fue muestreada. Se puede absorber dichas variación agregando retardo, pero si se trata de una aplicación multimedia interactiva el margen de maniobra es muy reducido (Cisco Systems, 2006).

2.3.1.1.1. Puntos de degradación de la QoS

En una red IP convencional se aplica la política de Best Effort, es decir, se hace el mejor esfuerzo por lograr que los datos lleguen a su destino, pero no se garantiza que lo hagan. Si existe un flujo de información que supera la capacidad de un enlacen, el excedente se lo almacena en una cola de la cual saldrán paulatinamente conforme el enlace lo permita. Si además el flujo desborda la capacidad de (IETF, 1998) la cola, loa paquetes que quedaron fuera se descartan (IETF, 1998).

Este es uno de los orígenes de la perdida de paquetes. Este fenómeno también puede ser generado por el excesivo ruido en el canal de comunicaciones, o por la saturación de los buffers en los equipos y/o las aplicaciones. Ventajosamente, lo último no es significativo debido a los algoritmos de recuperación implementados.

El retardo suele añadirse durante el procesamiento de los equipos, la transmisión a través del medio y en las colas de las interfaces de red. Las dos primearas han sido ampliamente combatidas con el desarrollo tecnológico de los procesadores y la fibra óptica.

El retardo agregado por las colas se debe a que el flujo de datos sobrepasa momentáneamente la capacidad del enlace; generalmente ocurre cuando las velocidades de las interfaces de red son distintas. La solución sería obviamente tratar de mantener las colas casi vacías o, sobredimensionar, si cabe el término, los enlaces. Esta solución resultaría muy costosa.

Aquí, es necesario recordar que ciertas aplicaciones de IP transmiten la información en ráfagas y además, los protocolos convencionales de enrutamiento consideran el número de saltos. Esto hace que ciertas rutas se vean saturadas temporalmente. Entonces la solución anterior no es viable.

Se ha optado entonces, por desarrollar técnicas que permita la el tratamiento adecuado de las colas aprovechando la capacidad de marcación de los paquetes de IP de al acuerdo al tipo de tráfico, desechando la vieja técnica FIFO[5] utilizada por defecto en los equipos de red.

[5] **FIFO.-** First In First Out, es un concepto utilizado en estructuras de datos, contabilidad de costes y teoría de colas. Guarda analogía con las personas que esperan en una cola y van siendo atendidas en el orden en que llegaron, es decir, que la primera persona que entra es la primera persona que sale.

2.3.1.1.2. Soluciones de QoS

Entendiéndose por congestión al hecho de que un flujo de datos sobrepase la capacidad transmisión de un enlace, es necesario estudiar las posibles alternativas que mitiguen este hecho.

Se puede optar por una planificación de capacidades, que unifique las distintas velocidades de transmisión de una red en conjunto con sus clientes. Pero ocurre que por los enlaces circulan distintos tipos de tráfico, algunos de ellos requieren ser priorizados. Consecuentemente, se puede optar por:

- Clasificar y formar clases con requerimientos similares a partir del volumen total de tráfico.
- Controlar el volumen de tráfico que ingresa a la red.
- Aplicar políticas en función de los requerimientos de las clases formadas.

Los modelos de QoS en IP se encaminan sobre estas tres premisas. Los modelos más usados son DiffServ y RSVP.

a) 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 (RFC 2205).

b) 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 enrutadores) los tratara en base a esa marca. Define y utiliza diferentes tipos de enrutadores. Esta diferenciación depende de si se trata de un nodo interior o un nodo frontera.

El marcado del tráfico lo realizan los enrutadores 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.

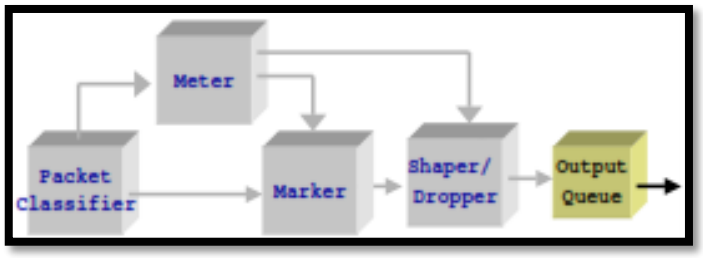


Figura II-9 Arquitectura de un nodo DiffServ

2.3.1.2. Ingeniería de Tráfico

Es la habilidad de definir rutas dinámicamente y planear la asignación de recursos en base a la demanda, así como la optimización del uso de la red. Para el balanceo de carga MPLS facilita la

asignación de recursos en las redes dependiendo de la demanda de tráfico de los usuarios, además brinda diferentes niveles de soporte. A diferencia que en OSPF, en MPLS se ven flujos de paquetes con su QoS respectivo y demanda tráfico predecible. Con MPLS es posible predecir rutas en base a flujos individuales, consiguiendo diferentes flujos entre canales similares pero dirigiéndose a diferentes enrutadores. Si llegase a amenazar congestión en la red, las rutas MPLS pueden ser re-ruteadas inteligentemente, cambiando las rutas de flujo de paquetes dinámicamente conforme a las demandas de tráfico de cada flujo. Con MPLS el flujo de paquetes viaja a través de un túnel de datos en el eje troncal creado por el Protocolo de Reserva de Recursos (RSVP), la ruta del túnel se da por los requisitos de recursos del túnel y de la red. El Protocolo de Enrutamiento Interno (IGP) encamina el tráfico a dichos túneles.

La ingeniería de tráfico, mediante el cálculo establece rutas dentro de una red de forma que se posibilite el aprovechamiento de todos los recursos por igual. Es decir, la ingeniería de tráfico permite tener el control total del flujo de la información en la red.

MPLS Traffic Engineering está definido en la RFC 2702[6] y establece que la ingeniería de trafico concierne a la optimización del performance de una red e involucra tareas como: mediciones del tráfico, modelado del tráfico y sus redes, control del tráfico de internet y la evaluación el desempeño.

Entre los principales objetivos de la TE están:

- Mover el tráfico de una ruta creada a través de un IGP hacia un camino menos congestionado.
- Compensar la subutilización de los enlaces, Load Balancing.,
- Incrementar la confiabilidad del servicio.

[6] **RFC 2702, MPLS-TE**, Multi-Protocol Label Switching Traffic Engineering

- Alcanzar retos impuestos referentes a la perdida de paquetes, retardos, etc.

Para alcanzar estos objetivos generalmente se suele:

- **Modificar los parámetros de enrutamiento.-** creando listas de prioridad en los buffers de los dispositivos de red.
- **Modificar los parámetros y atributos que asocian a los recursos.-** a través de la reserva de los recursos con el uso de ´marcas' especiales en las cabeceras de los paquetes.

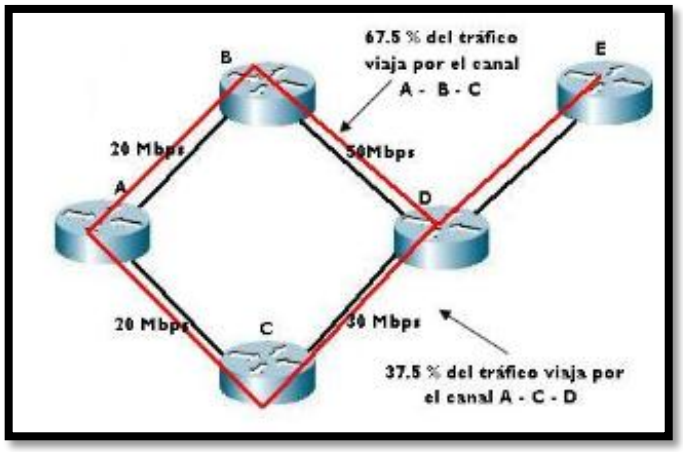


Figura II-10 Balanceo de carga MPLS-TE

MPLS-TE además permite incrementar la disponibilidad de las redes al posibilitar la creación de rutas de respaldo, las mismas que se activan rápidamente tras la interrupción de la ruta principal. Se puede crear LSP de respaldo en cualquier punto de la ruta principal.

Para esta operación, el LSR de respaldo añade una nueva etiqueta a los paquetes entrantes. Esta se mantiene a través de la ruta alternativa.

Cuando el paquete ingresa nuevamente a la ruta principal la etiqueta por el respectivo LSR y este continúa con la conmutación normal hasta completar el LSP.

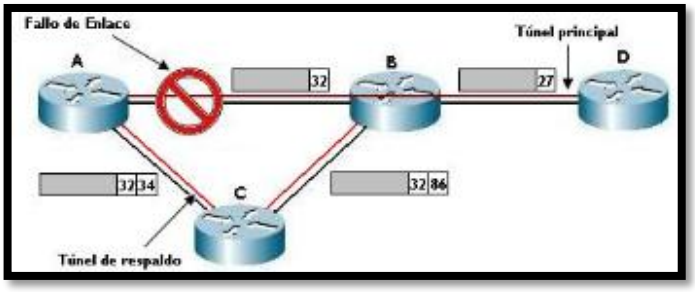


Figura II-11 Protección de enlaces MPLS-TE

2.3.1.3. Soporte Multiprotocolo

MPLS se puede usar con diversas tecnologías, por lo que por ejemplo, enrutadores y conmutadores MPLS pueden trabajar sin ningún problema con otros que sean IP. Lo que facilita la escalabilidad en la red, ya que esta tecnología está diseñada para trabajar con redes Frame Relay y ATM. Esto da la ventaja de tener redes mixtas añadiendo QoS para optimizar los recursos y expandirlos.

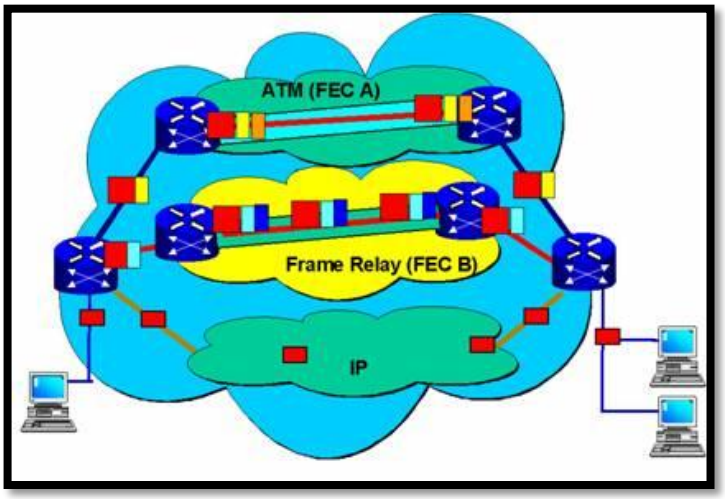


Figura II-12 Soporte multiprotocolo de MPLS

El soporte multiprotocolo de MPLS está definido por algunas técnicas de encapsulamiento de la trama original. Así por ejemplo, la tecnología AToM de Cisco Systems, la cual será estudiada más adelante.

También es posible hacer uso del modo trama o del modo celda de MPLS para acoplar las tramas de capa 2 al dominio MPLS.

La primera técnica de encapsulamiento suele ser más usada por su sencillez. Así, MPLS soporta dos modos: modo celda y el modo trama.

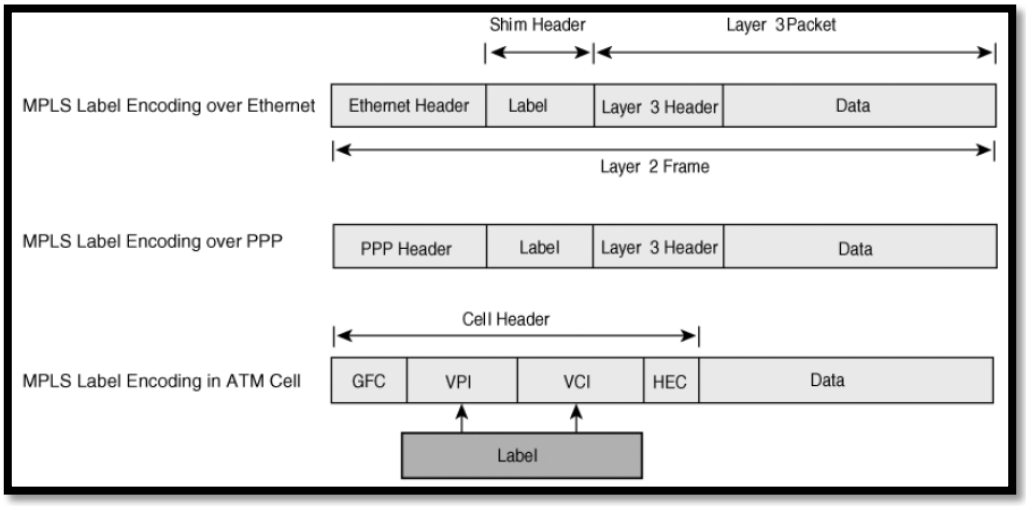


Figura II-13 Proceso de inserción de etiquetas

2.3.1.3.1. Modo Celda

Cuando se usa conectividad ATM[7] entre dispositivos, MPLS es aplicable a celdas, no a tramas, las celdas son comúnmente transportadas en el plano de información de datos. Cuando las etiquetas ATM son usadas en el núcleo MPLS, el modo operativo de MPLS es llamado *Modo Celda MPLS.*

En modo Celda MPLS, los LSRs en el núcleo de la red MPLS son conmutadores ATM que envían los datos basados en la cabecera (header) ATM. Si el LSR ATM funciona como un conmutador o switch ATM puro (plano de datos), un componente de plano de control externo también llamado

[7] **ATM.-** Asynchronous Transfer Mode, el Modo de Transferencia Asíncrona es una tecnología de telecomunicaciones desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones. Se ha caracterizado por proporcionar altas tasas de transferencia.

controlador de interruptor de etiqueta o Label Switching Controller (LSC), es requerido para la propagación de la información del plano de control. En algunos casos, sin embargo, el LSR ATM es capaz de propagar la información del plano de control además de enviar la información del plano de datos, y no requerir por lo tanto, un componente de plano de control externo.

Para ejecutar MPLS en el dominio ATM, la etiqueta superior en la pila de etiquetas que es insertada en la cabecera ATM y la cabecera IP es codificada como el VPI/VCI del circuito virtual en uso. El mecanismo permite un envío correcto de paquetes del plano de datos; los paquetes del plano de control son cambiados sobre un VC de control entre LSRs ATM directamente conectados. MPLS usa los campos VPI/VCI[8] de la cabecera ATM como etiqueta.

2.3.1.3.2. Modo Frame

En el modo frame MPLS, los enrutadores que soportan MPLS intercambian ya sea paquetes IP puros (a través de E-LSR), así como también paquetes IP etiquetados dentro del dominio MPLS. En un dominio MPLS la conmutación de etiquetas es realizada por el análisis de la cabecera y entonces se lleva a cabo las funciones que ya se han descrito en secciones anteriores, es decir remover, adherir o cambiar etiquetas, esto dependiendo de la ubicación del enrutador dentro de la red. La conectividad de enlace de datos en el modo frame MPLS es establecida empleando HDLC/PPP y Ethernet. En cuanto a ATM, ésta tecnología implica considerar otros aspectos de conectividad de capa dos, donde se emplean celdas para transportar paquetes IP, esto se analizará en el modo Celda MPLS.

[8] **VPI/VCI.-** Virtual Path Identifier/Virtual Circuit Identifier, identificadores de ruta que permiten que muchos flujos de datos diferentes puedan transitar por un canal de comunicaciones.

2.3.1.4. Soporte de Redes Virtuales Privadas (VPN)

MPLS provee un mecanismo eficiente para el manejo de redes privadas virtuales. De esta manera el tráfico de una red privada atraviesa la red pública (Internet) eficazmente y de manera transparente para el usuario, eliminando cualquier tráfico externo y protegiendo la información. Las VPN sobre MPLS son más flexibles en cualquier red, principalmente IP, además que son de mayor expansión. MPLS reenvía los paquetes a través de túneles privados usando etiquetas, las cuales actúan como códigos postales. Estas etiquetas tienen in identificador que aísla a esa VPN de las demás.

Cada VPN se asocia con una o más instancias de Ruteo/Reenvío Virtual (VRF). Una VRF determina la membrecía del cliente conectado al enrutador de frontera del proveedor del servicio (Router PE). Cada VRF se compone de una tabla de ruteo IP, una tabla de reenvío express propietaria de Cisco (CEF), un grupo de interfaces que usan dicha tabla, y un conjunto de reglas y parámetros del protocolo de ruteo que controlan la información que se incluye en la tabla de ruteo. Las VRF contienen las rutas disponibles en la VPN que pueden ser accedidas por los sitios de los clientes, cada uno de estos sitios puede estar suscritos a varias VPN, pero únicamente a un solo VRF. Cada VRF tiene almacenada información de reenvío de paquetes en las tablas IP y CEF para evitar que no salga ni que entre tráfico fuera de las VPN (Tomsu, y otros).

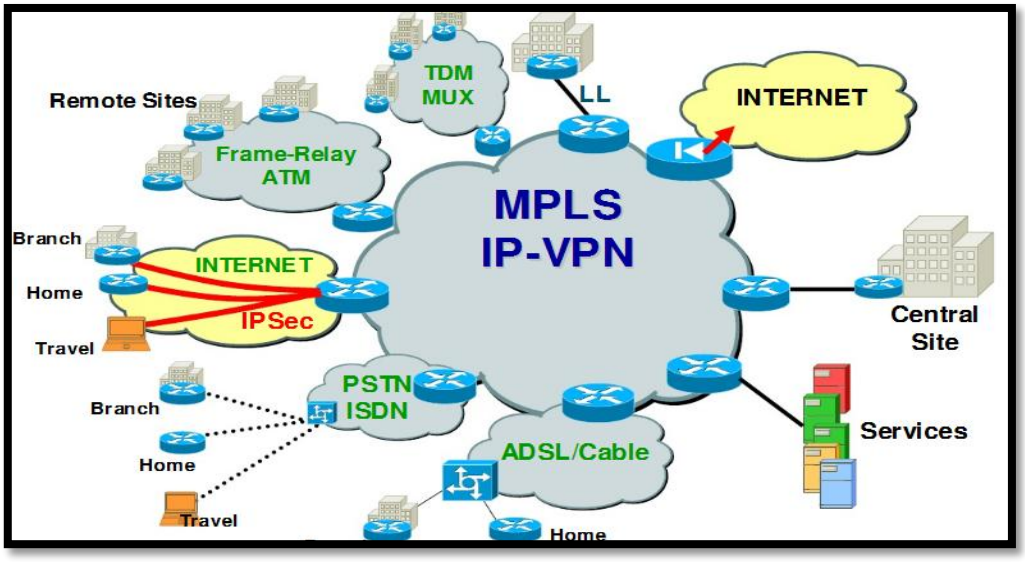


Figura II-14 Soporte de VPN's de MPLS

Fuente: (Almeida, 2012)

2.3.2. Elementos de un dominio MPLS

En un dominio MPLS intervienen algunos elementos tanto físicos como lógicos, algunos de los cuales serán explicados a continuación.

2.3.2.1. LER

Son aquellos enrutadores colocados al borde de un dominio MPLS y que permiten el intercambio de información entre la red MPLS y cualquier otra arquitectura.

En estos se insertan/extraen las etiquetas a los paquetes, según sea el caso. Además se realiza una clasificación de acuerdo a las clases de tráfico a las que pertenecen dichos paquetes para asociarlos una FEC.

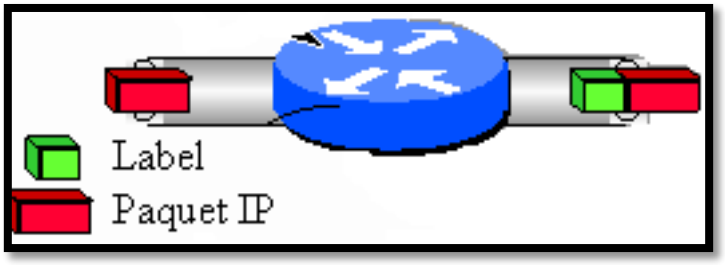


Figura II-15 Función de un LER

2.3.2.2. LSR

Son aquellos nodos internos de un dominio MPLS. Pueden ser enrutadores como tal o conmutadores ATM. Su función es realizar la conmutación en función del valor de las etiquetas.

Cabe mencionar que el valor de las etiquetas tiene significado local solamente. Un LSR está en la capacidad el cambiar valor de las etiquetas, más no de insertarlas o extraerlas.

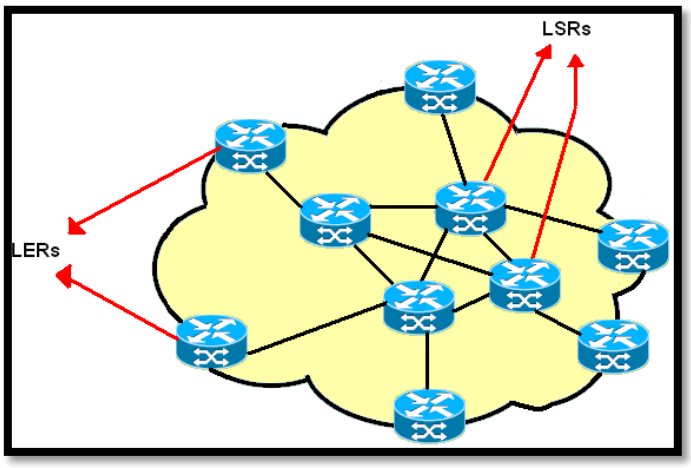


Figura II-16 Identificación de LSR's y LER's dentro de un dominio MPLS

Fuente: (Cisco Systems)

2.3.2.3. FEC

Es un grupo especial al que pertenecen paquetes con características similares, a los cuales se les asignara una etiqueta con el mismo valor y, por supuesto, compartirán la misma ruta hacia su

destino; técnicamente, compartirán un mismo LSP. Una FEC puede tener requerimientos específicos en cuanto a QoS.

Así, es posible crear una clase para cada servicio prestado por el operador de telecomunicaciones y gestionarlos por separado, asignándoles la prioridad pertinente a cada una de ellas. Las tareas de ingeniería de trafico serán también más versátiles, ya que se los flujos de datos, al transitar por el núcleo MPLS ya estarán clasificados y los LSR los identificarán a través del campo EXP de las etiquetas para asociarlas a la interfaz de salida definida.

2.3.2.4. LSP

Un LSP es una ruta unidireccional que comunica a dos LER a través del dominio MPLS. Actúan en forma de túneles y pueden incluir parámetros de QoS y TE.

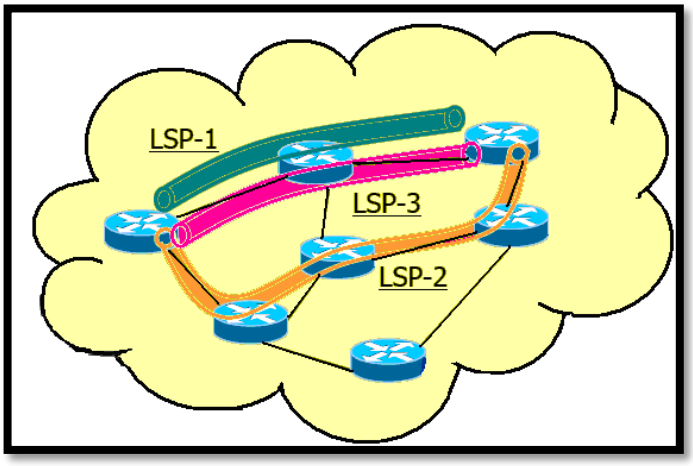


Figura II-17 LSP creado dentro del dominio MPLS

Fuente: (Alwayn, 2002)

2.3.2.5. LIF

Es aquí es donde se mantiene un registro de las etiquetas en un nodo MPLS y su correlación sus vecinos.

2.3.2.6. FLIB

En una registro de las etiquetas que solamente están siendo usadas en un momento dado.

2.3.3. Cabecera MPLS

La cabecera MPLS tiene una longitud fija 4 bytes y es insertada entre las cabeceras de capa 2 y capa 3 del modelo de referencia OSI. Comúnmente suele referirse a MPLS como un protocolo de capa 2.5.

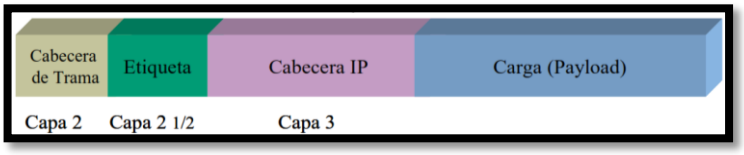


Figura II-18 Ubicación de la cabecera MPLS

Esta cabecera tiene la siguiente distribución de campos:

Figura II-19 Identificación de los campos de la cabecera MPLS

- **Label.-** ocupa 20 bits y define, junta con las etiquetas de los vecinos, los LSP dentro del dominio MPLS.
- **EXP.-** campo de 3 bits reservado para operaciones de experimentación. Suele ser usado para marcar a los paquetes de acuerdo al tráfico que transportan.
- **S.-** ocupa 1 único bit. Permite el apilamiento de las etiquetas gracias al cual es posible crear VPN's con relativa facilidad. El valor 1 indica la ausencia de más etiquetas.

- **TTL.-** campo de 8 bits que al igual que en la cabecera IP tiene como función poner un límite al recorrido de un paquete por la red y así, evitar bucles infinitos.

El campo "label" soporta 1048576 valores de etiqueta, de os cuales ciertos valores están reservados, así:

- **0**, **IPv4 Explicit NULL Label**.- indica que se retira la etiqueta y se reenvía el paquete a través del enrutamiento IPv4 convencional. Valido para etiquetas de nivel 1.
- **1, Router Alert Label.-** indica que el paquete será entregado a un módulo local para su procesado. El reenvío está determinado por la etiqueta inmediatamente inferior.
- 2**, IPv6 Explicit NULL Label.-** indica que se retira la etiqueta y se reenvía el paquete a través del enrutamiento IPv6 convencional. Válido para etiquetas de nivel 1.
- **3, Implicit NULL Label.-** únicamente asignable por un LSR.
- **4 al 15**.- etiquetas de uso especial.

2.3.3.1. Label Stacking (Apilamiento de Etiquetas)

El bit "S" permite realizar un apilamiento de las etiquetas, por lo cual, un paquete etiquetado puede contener varias etiquetas organizadas en modo LIFO.

Usualmente una sola etiqueta suele ser asignada a un paquete, pero en casos especiales suele asignarse más, como por ejemplo:

- **MPLS VPN.-** requiere de dos etiquetas. La etiqueta superior indica al enrutador siguiente que la etiqueta de primer nivel identifica a una VPN.
- **MPLS TE.-** requiere de dos o más etiquetas. Las etiquetas superiores indican el punto final de un túnel de ingeniería de tráfico y la de primer nivel indican el destino del paquete.

- **MPLS VPN y MPLS TE.-** necesita de al menos tres etiquetas.

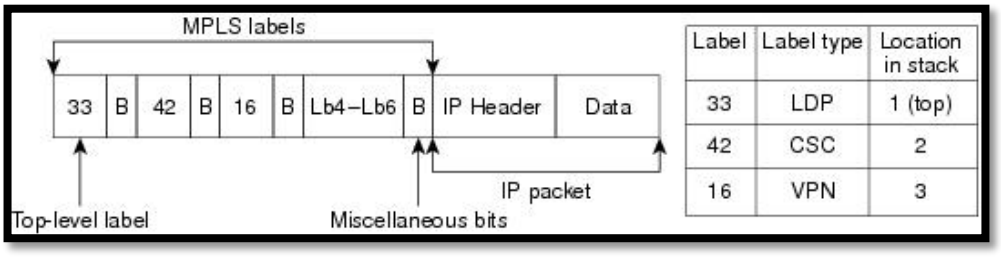


Figura II-20 Apilamiento de etiquetas MPLS

2.3.4. Funcionamiento

En MPLS la transmisión de datos sucede sobre el LSP (Label Switching Paths). Cada LSP es una cadena de etiquetas, una por cada nodo, desde el origen al destino. Hay dos formas en las que se establecen los LSP, una es antes de la transmisión y es generada manualmente o por los protocolos de control como BGP, y en la otra los LSP se crean a conforme se detectan los flujos de datos en los nodos. Estos dos procesos reciben la denominación de Control Driven y Data Driven respectivamente. La conmutación de alta velocidad de los paquetes es posible debido a que las etiquetas son de largo fijo y están insertadas en la cabecera de los paquetes, de modo que no hay que desarmarlos para acceder a ellas, esto permite la conmutación de los paquetes a nivel de hardware. Una red MPLS es de un conjunto de Enrutadores de Conmutación de Etiquetas (LSR - Label Switching Router) que tienen la capacidad de conmutar y encaminar los 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 - Forwarding Equivalence Class), 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” (Almeida, 2012).

Cada FEC aparte de la ruta de los paquetes contiene varios caracteres que definen los requerimientos de Calidad de Servicio del flujo. Los enrutadores de la red MPLS no necesitan examinar ni procesar el encabezado IP, solo se necesita reenviar cada paquete dependiendo el valor de su etiqueta. Esta es una de las ventajas que tienen los enrutadores MPLS sobre los enrutadores IP, en donde el reenvío de paquetes es más complicado. En un enrutador IP cada vez que se recibe un paquete se analiza su encabezado IP para compararlo con la tabla de enrutamiento y ver cuál es el siguiente salto o el destino más próximo. 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, lo cual hace que el tiempo de procesamiento en un enrutador MPLS sea menor.

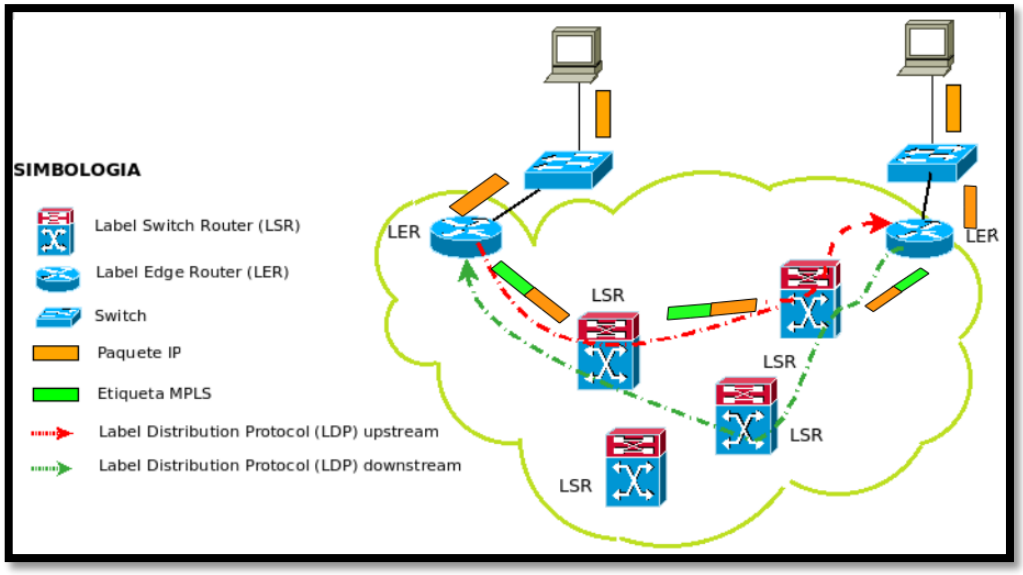


Figura II-21 Funcionamiento de MPLS

Fuente: (Black, 2002)

2.3.5. Protocolos de Señalización

2.3.5.1. LDP

Es el protocolo que permite señalizar el establecimiento del LSP, descubre vecinos adyacentes a través de los paquetes HELLO[9] y luego establece una sesión TCP con ellos. Los hellos se envían periódicamente con dirección destino multicast (224.0.0.2, todos los enrutadores en el segmento) hacia el puerto UDP 646. Luego, el enrutador con el Router ID más alto (Active Node) inicia una sesión TCP hacia el puerto 646 con dirección destino unicast (la IP origen del Hello o la dirección de transporte anunciada en el Hello).

En el descubrimiento de los vecinos no adyacentes tan sólo difieren la dirección destino de los mensajes hellos. Se envían a la dirección IP unicast del vecino y luego el mecanismo de establecimiento es el mismo que para el caso de vecinos adyacentes (Andersson, y otros, 2007).

2.3.5.2. RSVP-TE

Este es un protocolo optimizado del RSVP convencional, especializado en la creación de rutas explicitas con o sin reserva de recursos y la distribución de etiquetas sobre MPLS, permitiendo además el re-encaminamiento de los LSP, lo que soluciona los problemas de congestión y cuellos de botella. Es otro de los protocolos de señalización que emplea MPLS y es equivalente de LDP.

Inicialmente RSVP-TE fue propuesto por la IETF como principal protocolo de señalización para MPLS por el simple hecho de era el más usado por las compañías en aquel entonces y por ende

[9] **HELLO.-** Mensajes de señalización que LDP utiliza para lograr establecer las sesiones respectivas. Definido en la RFC 5036, LDP Specification.

resultaba más económico su implementación, pero se obviaron algunas consideraciones que, posteriormente fueron superadas con el desarrollo de LDP.

El principio, es similar a LDP, sin embargo los mensajes referentes a la negociación de la etiquetas de LDP son sustituidas por RESV en RSVP-TE.

En caso de no poderse establecer un LSP se originan mensajes PATHERR y RESVERR. En este protocolo la actualización de los mensajes permite descubrir los enlaces activos. Para que este método de reconocimiento de fallas sea efectivo será necesario configurar un tiempo de actualización bastante pequeño. Esto se convierte en su principal desventaja. Para paliar parcialmente estas debilidades se emplean los mensajes HELLO, NOTIFY y NOTIFYREQUEST. Los dos últimos son los más rápidos en la detección de fallas de nodo a nodo.

Generalmente la implementación de RSVP- TE suele ser más compleja que la implementación LDP pero, este último no gestiona adecuadamente la reserva de recursos necesaria para la transmisión de grades volúmenes de datos o de tiempo real. Por esta razón, es posible combinar LDP y RSVP dentro de un dominio MPLS.

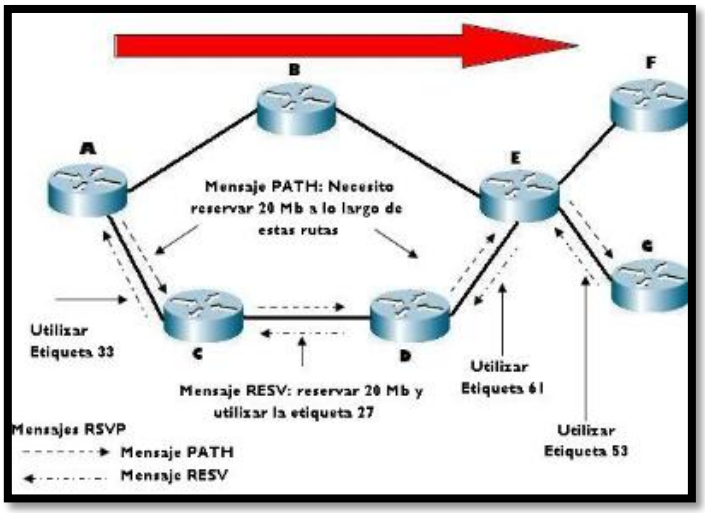


Figura II-22 Funcionamiento de RSVP

2.3.6. Creación de LSP's

Los IGP's propagan información de la situación de la red a todos los nodos que conforman la misma, permitiendo mantener la conectividad entre ellos e intercambiando información de la topología de la red. Esta información suele ser empleada para la creación de las LIB/FIB para mantenerlas coherentes en todo momento y evitar la pérdida de conectividad de extremo a extremo en caso de que algún enlace fallare.

Sin embargo, en ocasiones puede ser necesario definir explícitamente un LSP, lo cual es posible en MPLS y de hecho es el fundamento de RSVP. Como la ruta de extremo a extremo es conocida es monitorearla y administrarla. Desafortunadamente, un fallo de esta sería catastrófico debido a que como no su cuenta un protocolo automático de creación de rutas la perdida de conectividad sería inevitable. Siendo así, es necesario recurrir a técnicas auxiliares de recuperación como FRR de Cisco Systems.

Entonces un LSR o LER puede optar por un método de reenvió en función de cómo han sido creados los LSP.

MPLS tiene dos técnicas de reenvío o selección de ruta:

2.3.6.1. Enrutamiento Hop by Hop

En este tipo enrutamiento, un LSR selecciona a su criterio el siguiente salto para cada FEC y se construye automáticamente una topología lógica para usarla. Para esto utiliza un protocolo de enrutamiento IGP que además de llenar las tablas internas de direccionamiento, trazan las rutas a seguir. Esta selección está gobernada por un protocolo de creación automática de rutas conjuntamente con el IGP antes mencionado. Usualmente LDP suele emplear esta característica de reenvío.

Las capacidades de TE y QoS solamente están dadas por el protocolo IGP.

2.3.6.2. Enrutamiento Explicito

En el enrutamiento explicito existe una ruta preestablecida para cada FEC y cada una de ellas pueden tener asociados parámetros únicos de TE y QoS.

Para esto, el protocolo de señalización empleado debe permitir la personalización de los LSP, de forma tal que solo intercambie información entre los conmutadores de etiquetas preestablecidos y discrimine a los demás. Esto se logra cunado se implementa RSVP-TE.

Al hacer uso de esta característica, inherentemente se está haciendo uso de la ingeniería de tráfico y su eficiencia dependerá exclusivamente de la planificación realizada y los criterios técnicos que en ella se hayan utilizado.

El LER debe conocer que está usando el enrutamiento explícito, caso contrario el enrutamiento será hop-by-hop a pesar de que exista una ruta personalizada definida.

2.3.7. Tecnología AToM

La tecnología AToM (Any Transport over MPLS) es de propiedad de Cisco y simplifica enormemente la configuración de MPLS pero, principalmente permite el acople de cualquier datagrama para que pueda transitar a través de la nube MPLS.

AToM encapsula las tramas de capa 2 que ingresan por un LER, y las conduce a través de una ruta virtual (Pseudowire) hacia el otro LER. Este último remueve la encapsulación y recuera la trama de capa 2. Una ruta virtual establece la comunicación del tráfico encapsulado entre dos LER, evidentemente gracias a la existencia de un LSP ya establecido.

En realidad, los LER realizan el mayor trajo en todo el dominio al tener que acoplar los distintos flujos de tráfico. Los LSR se limitan a la gestión de etiquetas. Para que una ruta virtual se establezca se requiere.

- Especificar el tipo de tráfico a ser transportado.
- Conectividad entre los LER.
- Una combinación IP- VC ID de los LER.

El proveedor de servicio posee una red específica construida para transportar tráfico en capa 2 desde los clientes, pero los enrutadores de los clientes están interconectados en capa 3 y no interaccionan con los equipos del proveedor de servicio en capa 3, debido a que éste posee un backbone MPLS y la red por la cual se transporta tráfico en capa 2 desde los clientes es antigua AToM se encarga de transportar el tráfico en capa 2 desde los clientes hasta la red MPLS, eliminando la necesidad de trabajar con 2 redes separadas lado a lado, una en capa 2 y otra en capa 3 (Cisco Systems).

En la siguiente figura se puede observar un esquema de red AToM, donde los clientes están conectados a los PE mediante enlaces en capa 2, y a partir de estos, los paquetes son transportados a través de la red MPLS hacia los otros clientes.

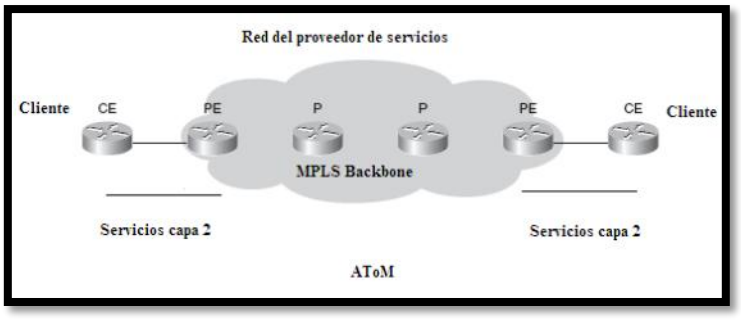


Figura II-23 Esquema de una red con tecnología AToM

Fuente: (Cisco Systems)

MPLS VPN provee el servicio de crear VPNs en capa 3, en cambio AToM crea VPNs en capa 2, algunas veces referida como L2VPN, la inteligencia de AToM reside en el Provider Edge (PE) por lo tanto es una tecnología de límite (Edge) y ésta se limita a crear servicios punto a punto en capa 2, también llamado como Virtual Private Wire Service (VPWS).

2.3.7.1. Arquitectura

La arquitectura está basada en rutas virtuales, éstos cargan el tráfico de los clientes en capa 2 de un lado al otro del núcleo de la red conmutada de paquetes, independientemente si este dominio es IP o MPLS. Las rutas virtuales son conexiones entre enrutadores PE, y emulan un circuito que está transportando tramas en capa 2 usando la técnica del tunelizado. Las tramas en capa 2 son encapsuladas en un paquete IP (L2TPv3) o etiquetadas (MPLS), su operación y características son emuladas a través de la red conmutada de paquetes (PSN).

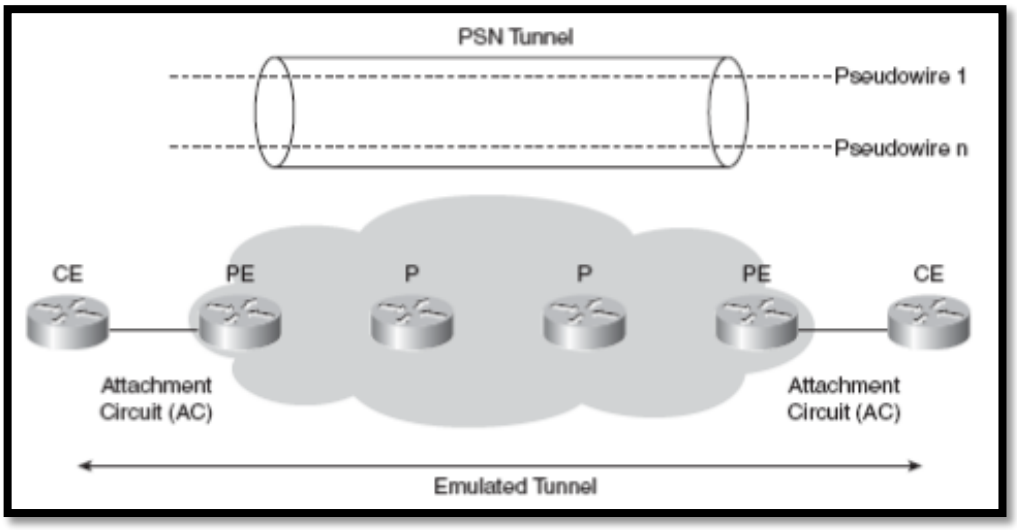


Figura II-24 Creación de una ruta virtual

Fuente: (Cisco Systems)

Dentro de los túneles pueden haber uno o más rutas virtuales que conectan a los circuitos (AC) por medio de los enrutadores PE, los circuitos AC pueden estar funcionando con protocolos como ATM, Frame Relay, Ethernet y HDLC, estas tramas al llegar a un enrutador PE son

encapsuladas y enviadas a través de un ruta virtual al enrutador remoto PE, el enrutador de egreso PE recibe el paquete de la ruta virtual y remueve lo encapsulado, éste extrae las tramas y las envía al circuito AC (attachment circuit) remoto.

Los túneles son LSP entre 2 enrutadores PE, la etiqueta asociada a ese túnel es llamada etiqueta de túnel en el contexto de AToM. En MPLS existen 2 tipos de señalización, el primero es mediante el protocolo LDP, que señaliza salto por salto entre 2 enrutadores PE, el segundo es estableciendo el LSP como un túnel MPLS implementado con ingeniería de tráfico (TE) que el RSVP señaliza con las extensiones necesarias para la ingeniería de tráfico.

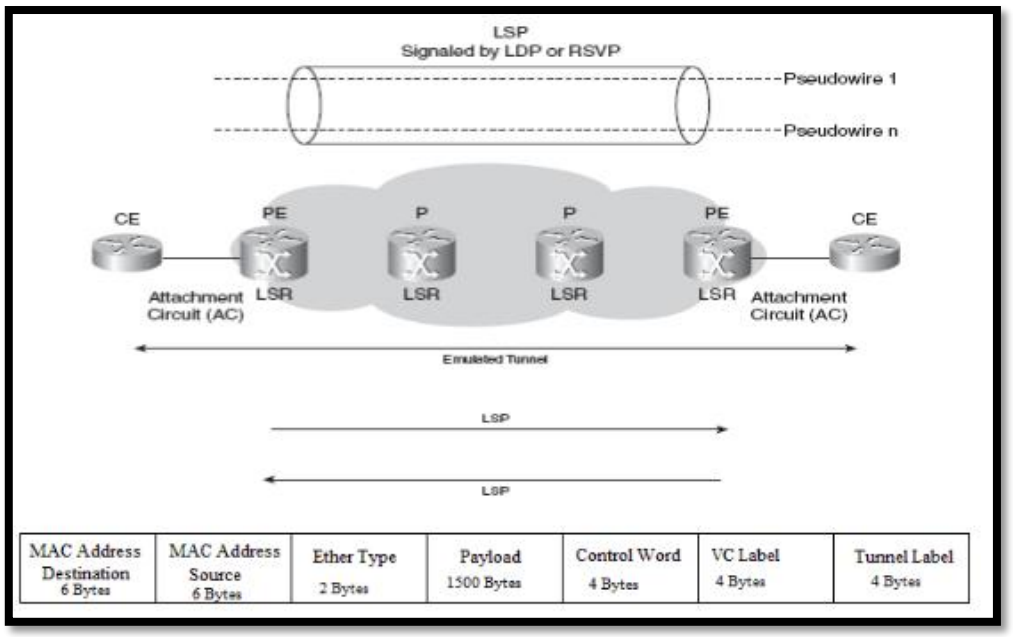


Figura II-25 Emulación de una seudo-ruta mediante protocolos

Fuente: (Cisco Systems)

La etiqueta de túnel cumple la función de identificar a cuál túnel de la red conmutada de paquetes pertenece la sesión del cliente, también permite transportar los paquetes desde un enrutador de ingreso a uno de egreso a través del núcleo MPLS. Para poder multiplexar algunas rutas virtuales a un túnel de la PSN, los enrutadores PE deben añadir otra etiqueta para

identificar la ruta virtual, esta etiqueta es llamada VC (circuito virtual) o PW (pseudowire) y es usada para identificar el VC o PW en la cual está multiplexada la trama.

Cabe destacar que los LSP son unidireccionales, y para establecer una ruta virtual se deben establecer 2 LSP entre 2 enrutadores PE, uno en cada dirección.

2.3.8. Ventajas de usar MPLS

La bondad de MPLS está en combinar eficazmente la simplicidad y la rapidez de la capa 2 y las funciones de control de enrutamiento de la capa 3 del modelo de referencia OSI.

Evidentemente, el tratamiento de etiquetas en vez de cabeceras, contribuye a ganar rapidez y sencillez en el procesamiento, lo cual es necesario en actuales redes en donde el tráfico es muy intenso. Como el procesamiento se lo realiza a través de software, una actualización del mismo en los equipos es suficiente para lograr migrar hacia MPLS, evitando gasto por concepto de nuevos equipos. Claro está, un análisis minucioso es necesario para justificar la migración y la debida planificación para minimizar cualquier afección a los usuarios.

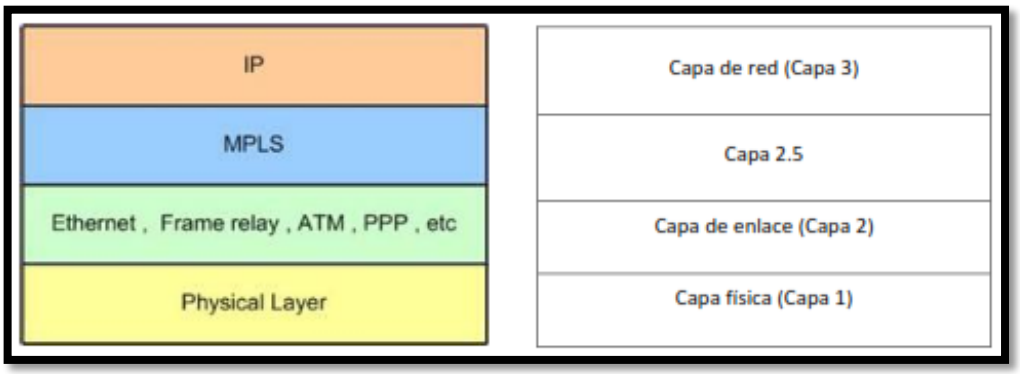


Figura II-26 Ubicación de MPLS en el modelo OSI

Fuente: (Alwayn, 2002)

En esta tecnología, el renvío de paquetes se lo realiza en función de cortos valores fijos denominados “etiquetas”, que marcan cada paquete que ingresa a un dominio MPLS. Todo

paquete entrante es etiquetado y en consecuencia, durante su recorrido a través de la nube MPLS, será tratado considerando el valor de sus etiquetas y no de la cabecera IP completa. Es necesario considerar que la etiqueta ira cambiando en cada conmutador dentro de la red MPLS.

Son mucha las ventajas que MPLS ofrece, de entre las cuales se pueden citar las siguientes:

- Mejora la escalabilidad del diseño de la red
- Provee flexibilidad de enrutamiento
- Incrementa el desempeño de la red
- Simplifica la integración de los equipos de red de tecnologías diferentes a IP
- Facilidad para realizar operaciones de TE y QoS.
- Integración de múltiples servicios en una misma plataforma de red.

CAPÍTULO III

DISEÑO Y SIMULACIÓN

En este capítulo se pretende definir un modelo de prueba en el cual se puedan medir ciertos parámetros con la finalidad de ajustarse a las necesidades que la hipótesis requiere para su verificación posterior. Estrictamente se trata de 4 modelos, cada uno de ellos, implementados con distintas tecnologías pero, conservando su topología física en su totalidad.

Se pretende dar una explicación técnica que justifique la consideración de 5 índices, todos ellos medibles, en base a recomendaciones y documentos técnicos emitidos por la ITU-T y la IETF. La misma explicación se busca también en cuanto a las aplicaciones software que se utilizaran tanto en la emulación, así como en la recolección de los datos.

Los escenarios serán analizados en la parte final de capítulo y, se concluye el mismo con la respectiva simulación y toma de resultados de los mismos. Por supuesto, la toma de muestras, también responde a criterios técnicos, lo cual valida el proceso a realizar.

3.1. Descripción y justificación de las aplicaciones software utilizadas

Parte de los buenos hábitos para la realización de un trabajo es la prueba los modelos diseñados antes de que estos sean implementados físicamente. La etapa de pruebas se la realiza después de finalizar el diseño respectivo y aplica a todas las ramas del conocimiento.

La informática juega un papel muy importante en esta etapa. Es posible realizar modelos computacionales que simulen una estructura física y de la cual podemos extraer información relevante. Las herramientas de simulación permiten estimar el comportamiento del diseño bajo condiciones críticas y por ende, permiten optimizar los modelos.

Para el diseño de las redes de datos también existen herramientas software que posibilitan simular o emular los modelos creados en ellos. Así también, se cuenta con sofisticadas aplicaciones que permiten monitorear el comportamiento de la infraestructura de red.

Para la realización del presente proyecto se ha utilizado las siguientes herramientas de software: GNS3, NetTools, VQManager.

3.1.1. GNS3

GNS3 es un entorno grafico que permite la emulación de complejas redes de datos. En sí, es un entorno de virtualización que emplea los IOS de Cisco Systems. Utiliza a Dynamips como aplicación de núcleo para permitir la emulación, sobre este actúa GNS3 creando una interfaz gráfica amigable para el usuario.

GNS3 también soporta la emulación de otros programas como Quemu, Pemu, entre otros. Estas aplicaciones pueden ser usadas para crear ambientes más reales con interactividad, a través de máquinas virtuales.

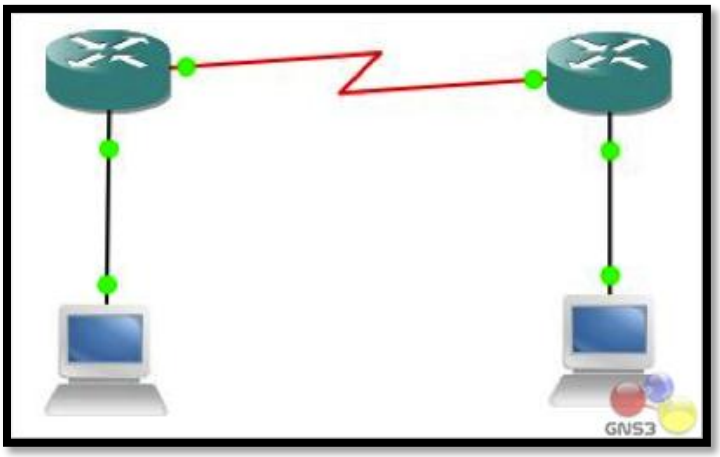


Figura III-1 Escenario virtual en GNS3

Fuente: (2013)

Está limitado en cuanto a los modelos de equipos que pueden ser emulados por cuanto es una herramienta de laboratorio. A pesar de esta desventaja, presenta todas cualidades de un equipo físico. Si se desea mayores características las actualizaciones del IOS son necesarias para los nodos involucrados.

GNS3 es de código abierto pero con algunas restricciones en su licencia. Adicionalmente, GNS3 limita el throughput a aproximadamente 1000 Packets/s, lo cual es necesario considerar ya que un enrutador real permitirá capacidades mucho más elevadas. Lo más destacable de GNS3 es su capacidad de poder interactuar con sistemas externos al entorno virtual. Esta capacidad está representada a través de las nubes existentes en el panel de dispositivos.

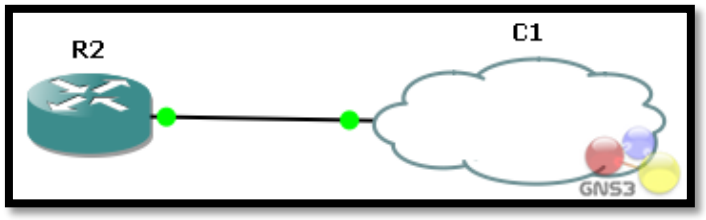


Figura III-2 Interconexión de GNS3 con sistemas reales

3.1.1.1. Características

Algunas de las características de GNS3:

- Plataformas: Windows, Linux, MacOS
- Arquitecturas: 32 y 64 bits
- Licencia: GNU
- Disponible en: http://www.gns3.net/download/

3.1.1.2. Utilización de recursos

Dynamips hace uso intensivo de memoria RAM y CPU en orden de lograr la magia de la emulación. Si la intención es de ejecutar una imagen de IOS que requiere 256 MB de RAM en un enrutador 7200 real, y dedica 256 MB de RAM a la instancia de su enrutador virtual, este utilizara 256 MB de memoria para funcionar. Dynamips también utiliza (por defecto) 64 MB de RAM por cada instancia en un sistema Unix (16 MB en Windows) para cachear (cache) las transacciones JIT[10]. Este será el tamaño total de trabajo; esto se debe a que Dynamips archivos para trazar un mapa de la memoria virtual de los enrutadores (2013).

Dynamips también hace uso intensivo de CPU, porque está emulando la CPU de un enrutador instrucción-por-instrucción. En principio no tiene manera de saber cuándo el enrutador virtual está

[10] **JIT.-** Just-In-Time, sistema de transacciones dinámicas.

en estado ocioso (idle), por esa razón ejecuta diligentemente todas las instrucciones que constituyen las rutinas de idle del IOS, igualmente que las instrucciones que conforman el "real" funcionamiento. Pero una vez que haya ejecutado el proceso de "Idle-PC" para una determinada imagen de IOS, la utilización de CPU decrecerá en forma drástica.

3.1.1.3. IOS

Las imágenes del Cisco IOS[11] están comprimidas. Estas imágenes comprimidas funcionan bien con Dynamips, aunque el proceso de arranque es significativamente más lento debido a la descompresión (igual que en los enrutadores reales). Es recomendable que descomprima las mismas de antemano así el emulador no tiene que realizar esa tarea.

3.1.1.4. Justificación de la utilización de esta aplicación

GNS3, gracias a su capacidad de emular múltiples plataformas hardware de enrutadores y, siendo el IOS de los mismos los que definen sus potencialidades, esta herramienta es la permite configurar el soporte multiprotocolo de MPLS a través de la tecnología AToM, a diferencia de otros simuladores de redes existentes. Por esta razón, esta es la herramienta ideal para la realización del presente proyecto. Además, se tiene el aval de muchas otras demostraciones y trabajos realizados con GNS3 en el campo del networking[12].

3.1.2. NetTools

Axence NetTools es una poderosa herramienta para medir parámetros de red y realizar un rápido diagnóstico de los problemas en la misma.

---

[11] Los IOS para el presente trabajo se lo extrajo de la página http://www.iosdownload.org/.

[12] Se han realizado varias tesis interesantes con GNS3 como "Evaluación de la herramienta GNS3 con conectividad a enrutadores reales" de Lisset Díaz Cervantes.

Su principal componente, NetWatch, permite obtener estadísticas de disponibilidad y pérdida de paquetes durante periodos de tiempo a la elección. Incorpora también otras herramientas de como lookup, port scanner, trace, network scanner, SNMP Browser, entre otras.

Una gran característica de esta aplicación es su atractiva interfaz gráfica lo que facilita su uso, sin dejar a un lado las potentes herramientas basadas en comandos (Axence, 2012).

3.1.2.1. Acerca de NetWatch

- Monitoreo de la disponibilidad y tiempo de respuesta de múltiples sistemas.
- Gráficos actuales e históricos de los tiempos de respuesta y del porcentaje de paquetes perdidos.
- Exportación de datos a XML, HTML, TXT.
- Monitoreo del tiempo de respuesta y el porcentaje de paquetes perdidos para HTTP, POP3, SMTP, FTP y 50 servicios más.
- Monitoreo de cualquier puerto TCP.
- Soporte a protocolos TLS/SSL en emails de alerta.

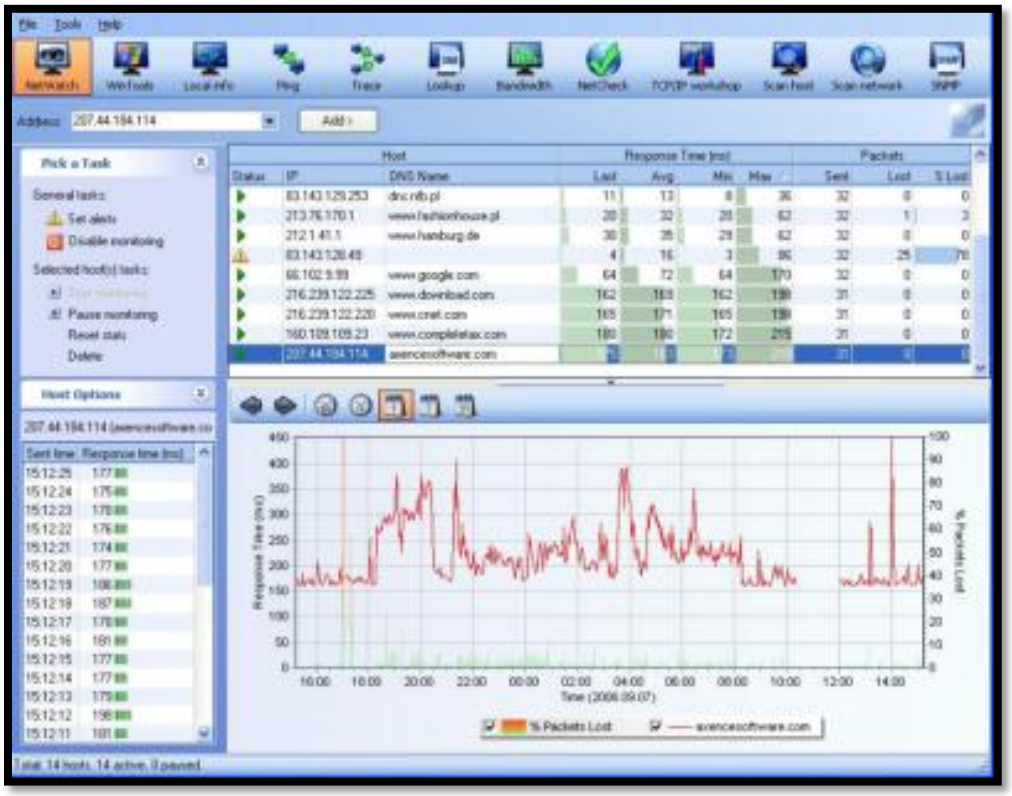


Figura III-3 Interfaz gráfica de NetTools

Fuente: (Axence, 2012)

Esta herramienta permite además la general alertas en función de los parámetros medidos, a los cuales el usuario debe especificar sus valores críticos.

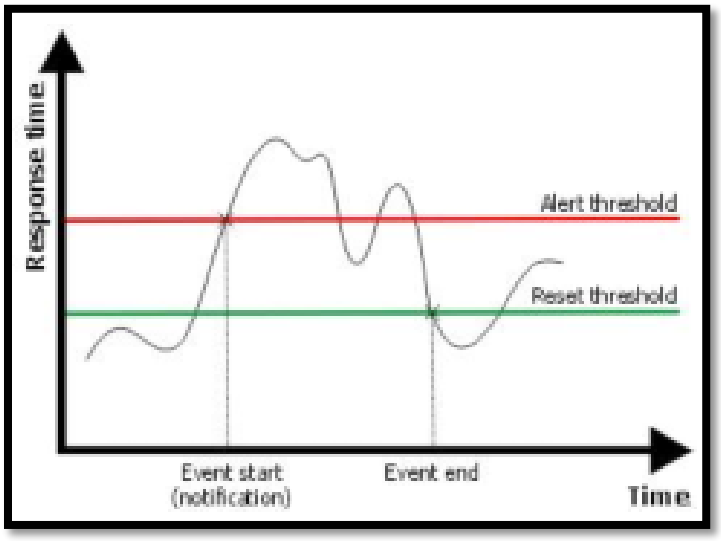


Figura III-4 Definición de umbrales de alerta.

Fuente: (Axence, 2012)

Para la realización del presente proyecto se usara la versión demo, con una duración de 30 días. Luego de este periodo se requiere la activación respectiva.

3.1.2.2. Características

Algunas características de NetTools son:

- Plataforma: Windows XP, Windows Vista, Windows 7.
- Sistema: 500 MHz o superior, al menos 128 MB en memoria RAM, tarjeta de video de 800x600 o superior, adaptador de red,
- Derechos de administrador son necesarios para la total ejecución de la aplicación.
- Posibilidad de ejecución a través de comandos.

3.1.2.3. Utilización de recursos

NetTools utiliza los datos ya existentes en la NIC del host para realizar los cálculos y estimaciones necesarios. Así, se minimiza la afección de las medidas reales de los índices que se están midiendo.

Algunas de la funciones como ping, trace, snmp, portscan, entre otras son las que necesitan enviar paquetes adicionales para cumplir sus cometidos. Sin embargo, la cantidad de paquetes que se generan no es significativo en relación al tráfico de red que comúnmente suele existir, por lo cual no se afecta significativamente las mediciones de latencia y ancho de banda.

Prácticamente, el uso de recursos por parte de NetTools se considera como bajo, consecuentemente, no se requieren potentes equipos hardware para ejecutarlo.

3.1.2.4. Justificación de la utilización de esta aplicación

La gran colección de herramientas, la facilidad con que estas pueden ser utilizadas y la fácil interpretación grafica de los resultados hacen que esta sea una eficiente herramienta de monitoreo para aquellos indicadores que no sean característicos del tráfico en tiempo real en el proyecto siguiente.

Además Axence NetTools[13] se ofrece de forma gratuita. Basta con registrarse para utilizar el software, incluso con fines comerciales.

3.1.3. VQManager

ManageEngine® VQManager es una herramienta de monitoreo de la calidad de servicio para sistemas VoIP. Soporta protocolos como SIP, Skinny, RTP/RTCP[14].

[13] Página de descarga de Axence NetTools: http://www.axencesoftware.com/es/nettools
[14] La NIC local es la que define los protocolos que serán aceptados para su análisis. Además, en esta se analiza el retardo agregado al tráfico de datos.

Figura III-5 Inicio de VQManager

Fuente: (AdventNet Inc., 2007)

VQManager se lo distribuye en dos ediciones diferentes: Standard y Professional.

Feature	Standard Edition	Professional Edition
SIP protocol Support	✓	✓
Cisco® Skinny Protocol Support	✗	✓
Live and History Reporting of QoS metrics and Bandwidth Utilization	✓	✓
Alarms on threshold violations	✓	✓

Figura III-6 Características de las ediciones VQManager

Fuente: (AdventNet Inc., 2007)

Se lo administra vía interfaz web por lo que facilita la rápida localización de fallos y el deterioro de la calidad. La aplicación soporta la especificación de umbrales que, una vez superados emiten mensajes de alerta a diferentes destinos, de acuerdo a las necesidades del usuario. Esto colabora a enfocar los esfuerzos en la zona del problema y ayudar a la rápida recuperación del sistema. Cuenta además con reportes predefinidos y configurables, estos soportes permiten tener una realizar un análisis completo y la optimización de la infraestructura de VoIP.

Presenta una agradable interfaz gráfica que permite visualizar todos los parámetros que están siendo monitoreados en una llamada activa o, en su defecto, el historial de las mismas. Esta

información gráfica puede ser fácilmente convertida en un reporte escrito en diferentes formatos de presentación que, también pueden ser personalizados (Security SRL, 2009).

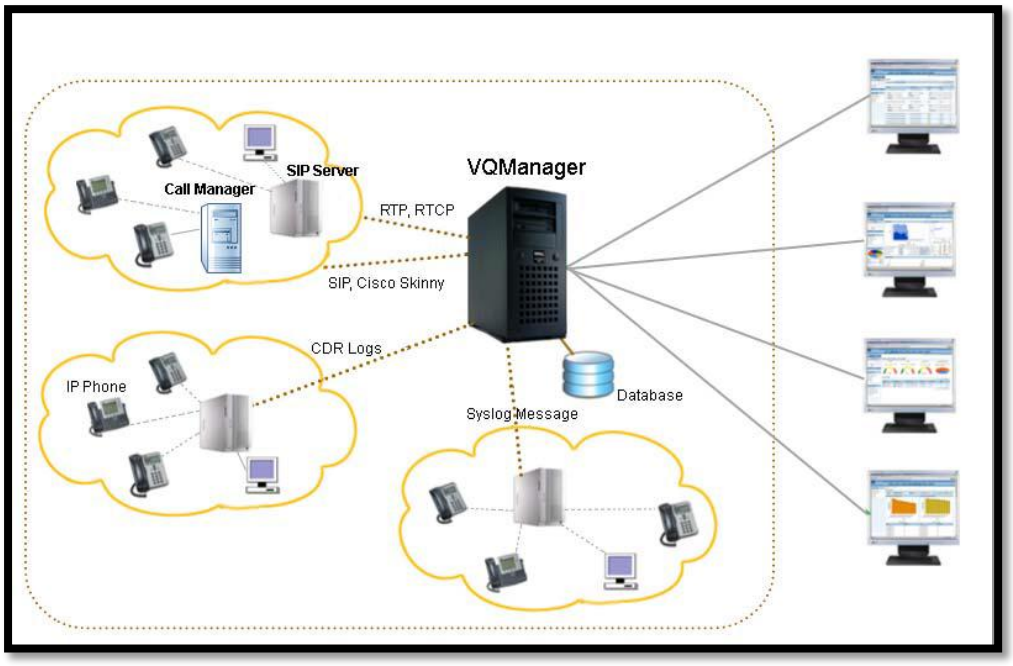


Figura III-7 Arquitectura de VQManager

Fuente: (AdventNet Inc., 2007)

La potencialidad de VQManager se debe a la medición en tiempo real y 24/7 de diferentes métricas características del tráfico de tiempo real y la exposición simultanea de los mismos a través de la interfaz web. Permite además la generación de reportes históricos desde la misma (AdventNet Inc., 2007).

3.1.3.1. Características

Las siguientes son algunas de las características de VQManager:

- Sistema: procesador 1,8 GHz, 1 GB de memoria RAM, 2 GB de espacio en disco para la aplicación y la base de datos, navegador web IE o Firefox.

- Plataformas: Windows, Linux Red Hat, Linux Mandrake.
- Monitoreo proactivo y continúo del BW y QoS de redes VoIP.
- Monitoreo de cualquier dispositivo o agente de usuario que soporte SIP, SKINNY o RTCP.
- Generación de alarmas basado en llamadas incompletas, retardo de respuesta, consumo de a BW por parte del tráfico de voz, entre otros parámetros.
- Monitoreo en tiempo real.
- Disponible en: www.vqmanager.com

3.1.3.2. Utilización de recursos

La aplicación requiere de una velocidad de procesamiento ligeramente elevada para poder procesar eficientemente los paquetes capturados, tarea que tiene una prioridad media en la jerarquía de procesos. La captura de los paquetes está a cargo de la interfaz de red y, la calidad de esta definirá el rendimiento de VQManager.

La aplicación requiere de un servidor web, que se instala junto a VQManager. Los navegadores que accedan a este servidor a través del puerto 8647 hacen uso intensivo de java por lo que existe un alto consumo de recursos. Por esta razón se recomienda que un estación de trabajo sea exclusivamente dedicada al proceso de monitoreo.

3.1.3.3. Justificación de la utilización de esta aplicación

Como se sabe, en una red conmutada un host en particular está imposibilitado de poder observar el tráfico de toda la red. Es necesario entonces contar con conmutadores administrables y

configurarlos con "Port-Mirroring[15]" para poder monitoreo cualquier llamada independientemente de donde se origine (AdventNet Inc., 2007).

Esta una de las pocas herramientas software especializadas en el análisis del tráfico en tiempo real e interactivo. Sus auspiciantes directos como Cisco, Microsoft, AVG, HP entre otras serias industrias de la informática aplicada a las redes de datos, dan cuenta de la enorme potencialidad de esta herramienta. Por esta, y otras ventajas citadas anteriormente, esta aplicación será usada en el modelo a proponerse para la toma de medidas de los parámetros característicos del tráfico en tiempo real: Jitter, porcentaje de pérdidas y el retardo en la interfaz local.

3.2. Parámetros de medición

Las redes de datos pueden ser evaluadas en torno a su rendimiento como una función del tráfico, potencia de equipos, protocolos, pero sobre todo, la capacidad de sus enlaces. Estos factores definen una gran cantidad de variables mensurables que afectan a las comunicaciones de acuerdo al tipo de datos que se manejen.

Entonces se tiene que el rendimiento de una red según la recomendación E.800[16] de la ITU es: "La habilidad de una red o una porción de red para proveer funciones relativas a comunicaciones entre usuarios".

De entre los distintos parámetros que pueden ser medidos en una red de datos, la RFC 6349[17] discute y define algunos de ellos para describir y comparar las características del rendimiento de una red entre las que tenemos:

---

[15] **Port-Miirroring**.- funcionalidad de los equipos de red que posibilita que una copia del tráfico de las interfaces necesarias sean enviadas hacia una en particular.
[16] **E.800. -** Terms and Definition Related to Quality of Service.
[17] **RFC 6349. -** Framework for TCP/IP Throughput Testing.

- Latencia
- Jitter
- Velocidad de Transmisión
- Retardo
- Perdida de paquetes

3.2.1. Latencia

También conocido como retardo, es el tiempo que una trama o paquete tarda en hacer el recorrido desde la estación origen hasta su destino final, es decir es la suma de retardos temporales dentro de una red.

Esencialmente, son tres los tipos de retardos que han de influenciar en la latencia de un flujo de datos:

- **Propagación de la señal.-** Se refiere al tiempo que toma a una señal viajar de un punto A hasta un punto B, considerándose que las señales electromagnéticas pueden propagarse a la velocidad de la luz; puede calcularse con la sencilla relación:

$$t = distancia/velocidad$$

- **Utilización de enlaces.-** Es el tiempo que le toma a un paquete de datos moverse a través de un enlace, en específico se refiere a los enlaces de acceso local.
- **Tiempo de serialización.-** Es el tiempo empleado por los equipos para el procesamiento de los paquetes, este tiempo es menor a los milisegundos y típicamente esta entre los 30 y 40 microsegundos.

- Los codificadores, los algoritmos empleados, la calidad de los enlaces, suelen ser los responsables directos del nivel de latencia en una red de comunicaciones (Cisco Systems, 2006).

En el presente estudio se ha considerado este parámetro ya que junto al ancho de banda son aspectos determinantes en la velocidad de una red, estos dos parámetros están definidos dentro del acuerdo del nivel de servicio, SLA, suscrito entre el cliente y el proveedor de servicio.

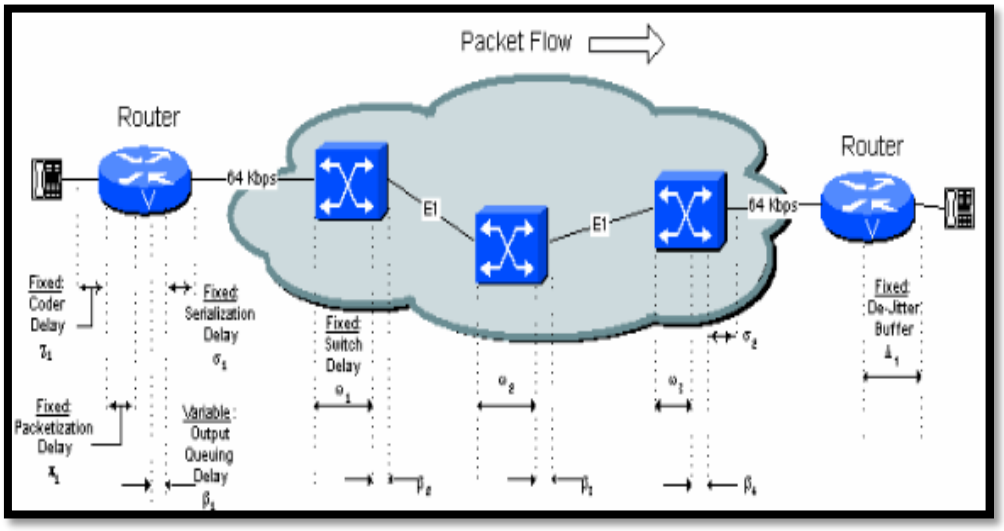


Figura III-8 La latencia como sumatoria de los retardos

Fuente: (Cisco Systems, 2006)

Además de los citado. La latencia, es un parámetro técnico que influye mucho en las comunicaciones, por tal razón se existe una norma que sugiere la correcta forma de evaluarla pero, sobre todo, en ella se establece ciertos valores de referencia; esta es la ITU-T G.114[18]. Son estas las normas que se consideran en el análisis de datos en el presente trabajo.

[18] **ITU-T G.114**.- One-way Transmission Time, recomendación que especifica la forma más adecuada para medir los retardos y sus valores máximos.

3.2.2. Jitter

Es la variación del tiempo en la llegada de los paquetes, causada por congestión de red, perdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino.

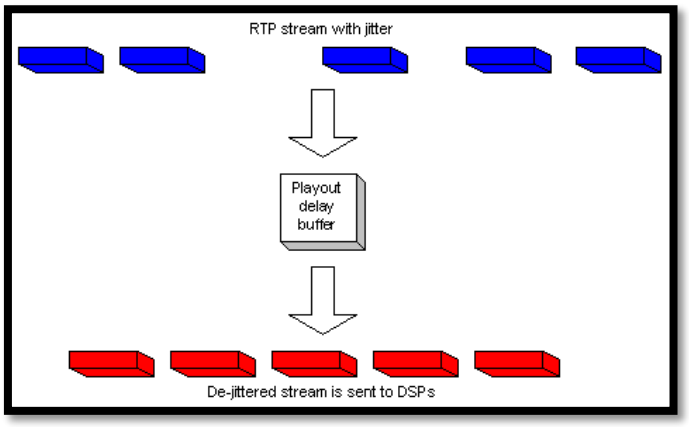


Figura III-9 Función del buffer frente al Jitter

Este indicador influye mayormente en el tráfico de tiempo real considerándose valores aceptables cualquiera que se situé en un valor inferior a los 50 [ms].

Valores comprendidos de 50-150 [ms] pueden ser considerados tolerables, mayor a los 150 [ms], se consideran valores críticos en el cual la comunicación se torna imposible.

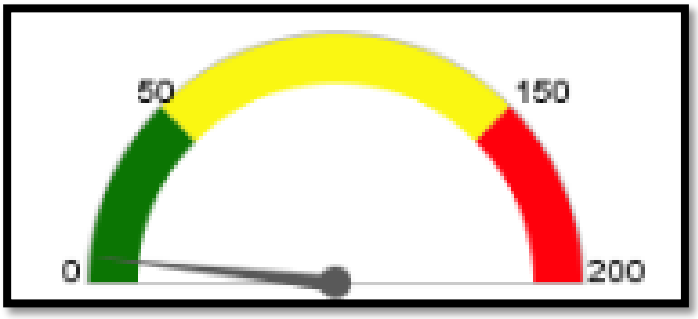


Figura III-10 Escala de medición de Jitter

Fuente: (AdventNet Inc., 2007)

Los valores indicados en la Figura III-10, se los puede encontrar en algunos documentos técnicos como la RFC 3550[19] o la RFC 3611[20], donde se sugiere como evaluar el Jitter y, sus resultados son aproximados a los mencionados anteriormente.

3.2.3. Velocidad de Transmisión

La velocidad de transmisión es la relación entre la información transmitida a través de una red de comunicaciones y el tiempo empleado para ello. La unidad para medir la velocidad de transmisión es el bit por segundo (bps) pero es más habitual el empleo de múltiplos como kilobit por segundo (kbps, equivalente a mil bps) o megabit por segundo (Mbps, equivalente a un millón de bps).

La importancia de este parámetro radica en que el rendimiento de una red de computadoras también es medido o cuantificado usando la velocidad de transmisión de datos. Es una medida concreta y de fácil cálculo, que permite saber si una red está funcionando en forma óptima.

El estándar ITU-T Y.1564[21] define las características que debe tener el ancho de banda para que se pueda obtener un mejor desempeño de la red a una velocidad de transmisión adecuada, evitando así problemas de congestión, pérdidas de paquetes, entre otros efectos dañinos a la salud de una red de comunicaciones. No especifica valores, ya que estos dependerán exclusivamente del proveedor de servicios sino, más bien define una metodología a seguir para su correcta administración y aprovechamiento.

---

[19] **RFC 3550. -** RTP, A Transport Protocol for real Time Applications.
[20] **RFC 3611.-** RTCP XR, Control Protocol Extended Report.
[21] **ITU-T Y.1564.-** estándar de ITU que define la metodología de pruebas para la activación de servicios de telecomunicaciones.

3.2.4. Retardo

Es un factor producido por la demora en la propagación y transmisión de paquetes dentro de la red.

El retardo se considera aceptable a cualquier valor que se situé en un valor inferior a los 180 [ms]. Valores comprendidos de 180-300 [ms] pueden ser considerados tolerables, mayor a los 300 [ms] se consideran valores críticos en el cual la comunicación se torna imposible (Cisco Systems, 2006).

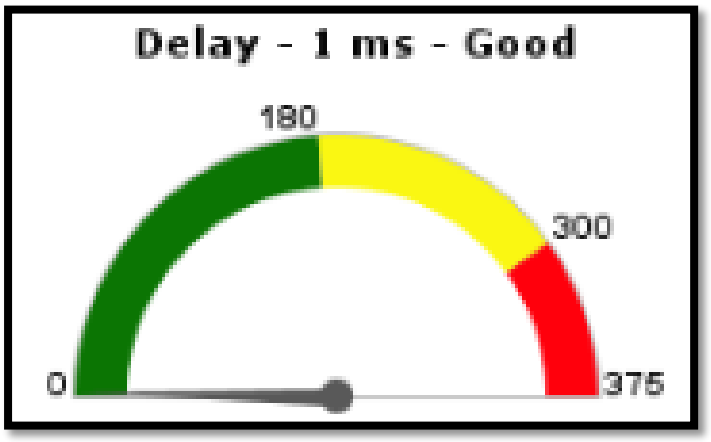


Figura III-11 Escala de medición del Retardo

Fuente: (AdventNet Inc., 2007)

El retardo puede ser agregado en los diferentes dispositivos que conforman la red, en el presente trabajo se mide el retardo agregado en la interface local de la estación de monitoreo.

3.2.5. Pérdida de Paquetes

Las aplicaciones de tiempo real, convierten las señales análogas en una serie de muestreos, las evalúa y las codifica para luego enviarlas en paquetes sin necesidad de un acuse de recibo. Esto último es el principal inconveniente ya que, sin un paquete se avería durante su recorrido, la porción de información que contenía se pierde definitivamente, entonces sin el porcentaje de perdidas es elevado, las comunicaciones no serán legibles. De allí la importancia de medir esta característica.

La pérdida de paquetes generalmente se debe a la congestión de la red. Siendo hasta el 10 [%] un valor aceptable, de entre un 10 y 30 [%] un valor tolerable y mayor que 30 [%] un valor crítico.

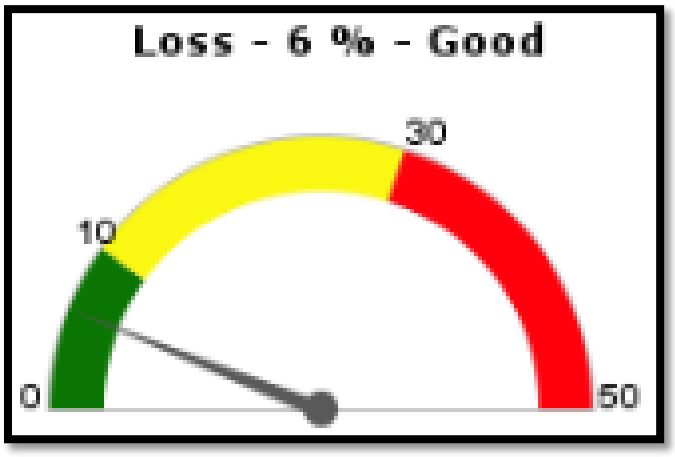


Figura III-12 Escala de medición de la pérdida de paquetes

Fuente: (AdventNet Inc., 2007)

Los valores umbrales anteriormente mencionados para la perdida de paquetes también han sido recomendados por el IETF a través de las RFC 1242 y RFC 254422, por lo cual se lo han considerado en este estudio.

3.2.6. Resumen de los indicadores a medir

Cada uno de los parámetros descritos, han sido medidos con las herramientas mencionadas anteriormente como son NetTools y VQManager.

Consecuente de lo expuesto con anterioridad y, con el debido sustento técnico de las recomendaciones mencionadas en el detalle de cada índice, tanto de la ITU-T y la IETF, se expone una tabla resumen con los valores que serán considerados para cada parámetro a medir.

[22] **RFC 1242. -** Terminology for Network Interconnection Devices.

Tabla III-I Resumen de los Parámetros de Medición

INDICADORES	MEDIBLE CON	UNIDADES	ÓPTIMO	TOLERABLE	CRÍTICO
Latencia	NetTools	ms	La más baja	-	La más alta
Jitter	VQManager	ms	< 50	50-180	>180
BW	NetTools	Kbps	La más alta	-	La más baja
Retardo	VQManager	ms	< 180	180-300	>300
Pérdida	VQManager	%	< 10	10-30	>30

3.3. Planteamiento y Definición del Modelo de Simulación

El buen funcionamiento y éxito de una red depende de la disposición en capas, basadas en modelos jerárquicos, para aprovechar las ventajas de modularidad a medida en que la red crece. Para el caso de una red de backbone es necesario asignar tareas específicas a los dispositivos de conmutación y enrutamiento para tener la diferenciación entre el acceso, borde y núcleo para operar y mantener una red multi-servicio.

A partir de esta consideración y siguiendo los criterios establecidos en el RFC 3031[23], donde se especifican los componentes de una arquitectura MPLS, la misma que está conformada por LSR[24] y LER[25], que son enrutadores que conforman el dominio MPLS que junto a una variedad de protocolos hacen de MPLS una red de siguiente generación.

Entonces tenemos que una red MPLS en su estructura más básica necesita de tres enrutadores, 2 LER, que serán los dispositivos que operan en el borde de la red de acceso y el dominio MPLS, los mismos que se encargaran de insertar las etiquetas basándose en la información de

[23] **RFC 3031**.- Multiprotocol Label Switching Architecture
[24] **LSR.-** Label Switching Router.
[25] **LER.-** Label Edge Router.

enrutamiento; y un LSR que es un enrutador especializado en el envío de paquetes etiquetados por MPLS. Este enrutador es de alta velocidad y está ubicado en el corazón de la red MPLS.

Teniendo en cuenta estos aspectos en esta investigación se presenta una topología de red conformada por un núcleo MPLS de 4 enrutadores (LSR) y 2 enrutadores (LER) en el borde del dominio MPLS, como se puede observar en la **Figura III-13**[26], la misma que fue tomada de escenarios utilizados para el análisis de entornos reales.

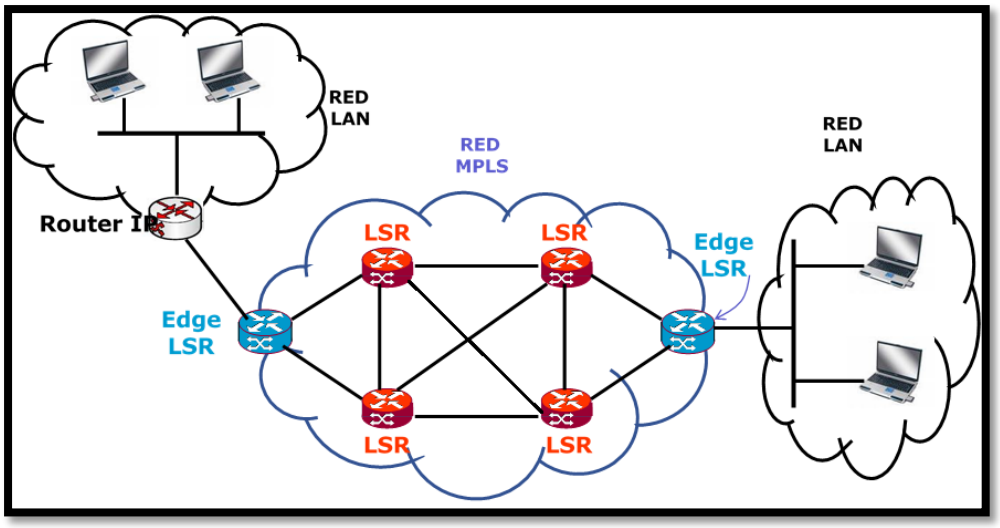


Figura III-13 Componentes del dominio MPLS con topología en malla

Este diseño permite la creación de varios LSP's, es decir los paquetes que atraviesen el núcleo MPLS tendrán la posibilidad de elegir entre uno y otro camino, y es en ese momento en que los protocolos de señalización entraran en juego mostrando sus mejores aportes en el tratamiento de paquetes.

[26] Referenciado de Alta Velocidad y Calidad de Servicio en Redes IP
García Tomas Jesús, Raya Cabrera José Luís, Raya Víctor Rodrigo
Alfa omega, 2008.

El principal objetivo de la simulación de este escenario es demostrar el comportamiento de Ethernet y Frame Relay individualmente, cuando estas cruzan a través de un dominio de MPLS, con la finalidad de encontrar la que mejor se acople considerando los enrutamientos hop-by-hop y explicito analizados igualmente por separado.

En la Figura III-14, se detallan las tecnologías involucradas en el escenario de simulación propuesto:

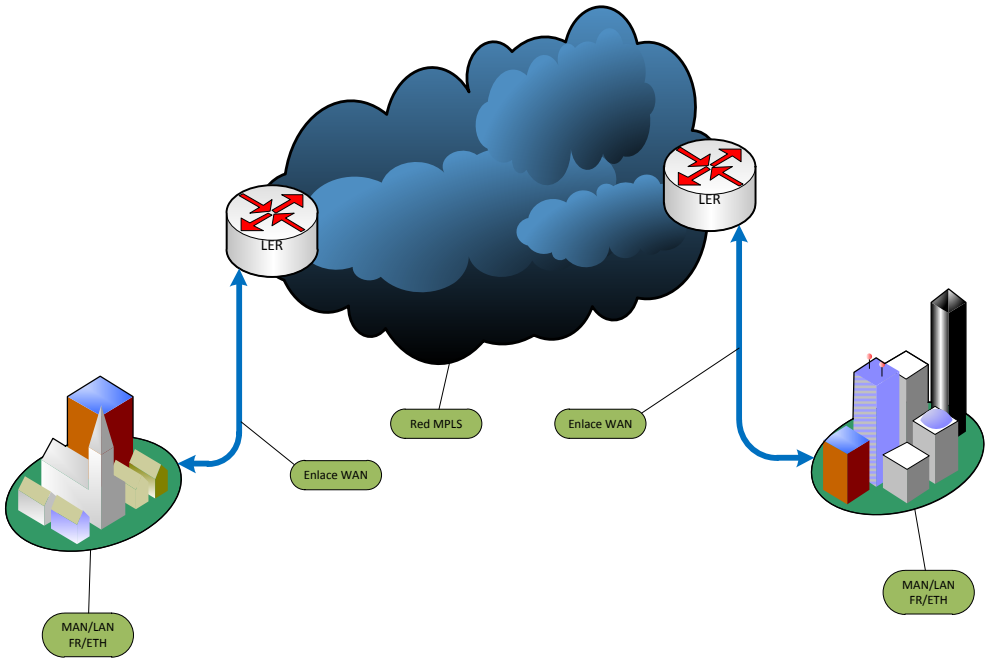


Figura III-14 Esquema propuesto para la simulación

Esto se resume en cuatro escenarios de pruebas distintas:

- Ethernet y LDP
- Ethernet y RSVP
- FR y LDP
- FR y RSVP

Los modelos de pruebas han de ser configurados en la plataforma de GNS3 en los cuales, se emularan los enrutadores Cisco c7200 con sus respectivos IOS de la versión 12.4. El dominio MPLS contendrá 6 enrutadores, dos de los cuales han de ser LER, entre todos pertenecerán a una topología de malla. El dominio MPLS puede estar conformado por un número indefinido de LSR o LER ya que nuestro estudio no se basa en la complejidad de la estructura de MPLS, sino más bien, en la rapidez con que encapsula/des encapsula una trama de capa 2 para, en función de aquello, definir la que mejores resultados ofrezca. Además, a MPLS le es indiferente el tipo de tráfico o la longitud que haya que recorrer dentro del núcleo.

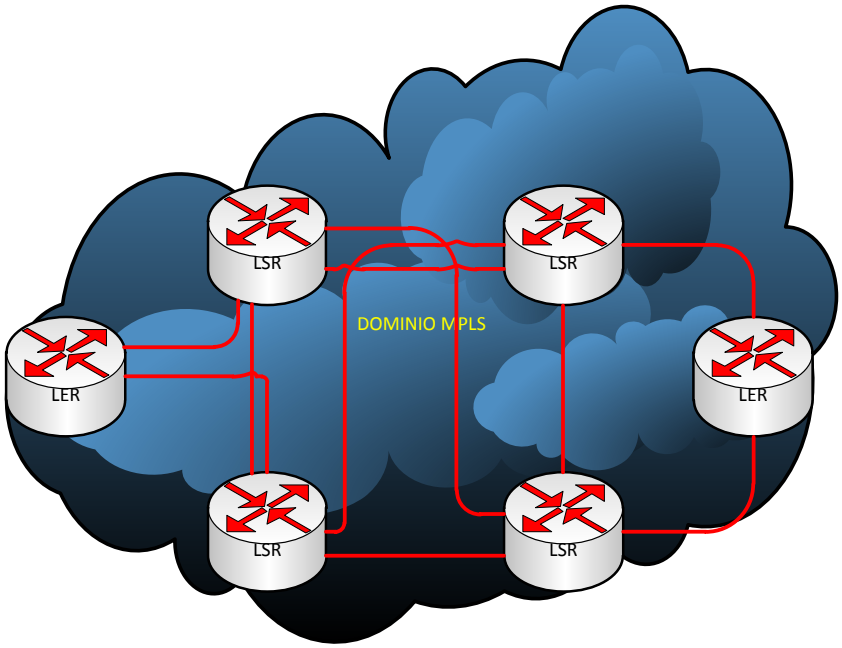


Figura III-15 Estructura del dominio MPLS

La red anexa al dominio MPLS, en la cual se encuentran los usuarios prescinde de enrutadores de altas prestaciones ya que solo se limitan a la interconexión de dos redes LAN. Uno de ellos será configurado con la funcionalidad de CME con la finalidad de poder observar el comportamiento del tráfico en tiempo real.

Para las pruebas, las redes LAN intercambiaran tráfico de voz y un flujo adicional de datos en el transcurso de un minuto por prueba. Se realizarán 10 pruebas por escenario y los promedios respectivos se podrán utilizar para su comparación.

De la recomendación de la IETF, RFC 2544 y RFC 1242, se extrae que las pruebas han de durar entre 60 y 120 segundos y, se han de repetir de entre 10 a 20 veces, de acuerdo a la complejidad de la infraestructura y la rigurosidad del análisis. Así, la metodología sugerida en estas recomendaciones y la topología sugerida para efectuar las pruebas coincide con la implementada para las pruebas de desempeño en el presente proyecto de investigación.

Algunos enrutadores exportaran datos NetFlow hacia las estaciones de monitoreo en donde se realizaran las mediciones. Se consideran importantes los LER's y a aquel en donde se implementó el CME. La aplicación VQManager es compatible con los datos de NetFlow de allí la necesidad de habilitar dichos flujos. Así, el escenario en cuestión es el siguiente:

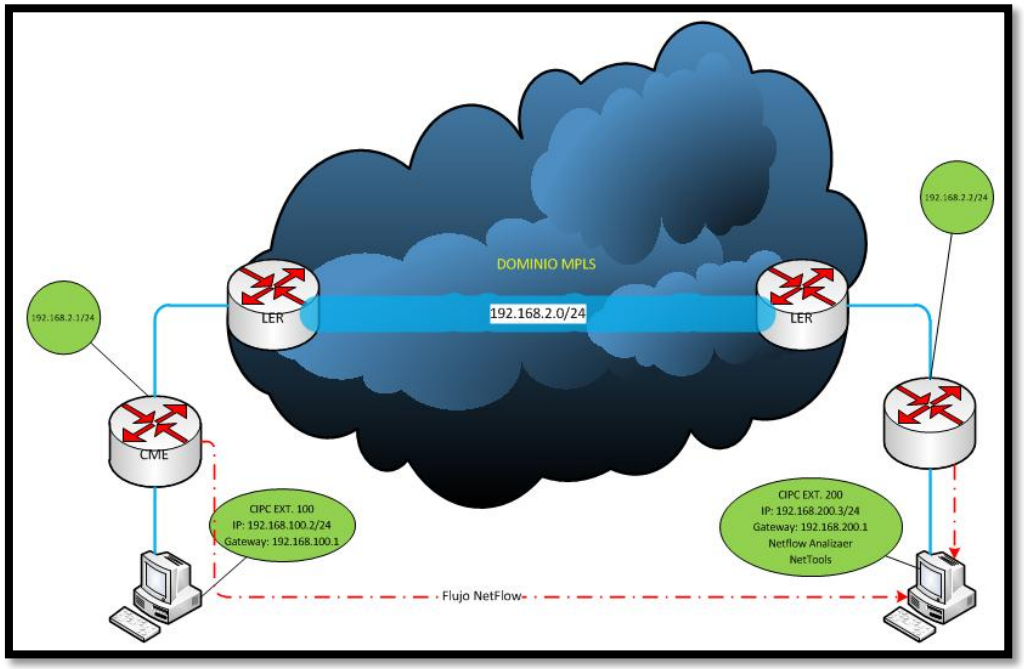


Figura III-16 Interconexión a través del dominio MPLS

El soporte multiplataforma del dominio MPLS será gestionado con la tecnología AToM de Cisco. Las tecnologías más adecuadas serán aquellas, en la que sus indicadores se acerquen más a los valores óptimos especificados anteriormente en la Tabla III-I.

Es necesario aclarar que el enlace que une al usuario con dirección IP 192.18.100.2 y el enrutador de acceso es un enlace Ethernet, o sea, la velocidad máxima del enlace es de 10 Mbps. En cambio, el enlace que une al usuario con una dirección IP 192.168.200.3 y su correspondiente enrutador de acceso, es de tipo Fast Ethernet el cual puede alcanzar una velocidad máxima de 100 Mbps.

Así, en el mejor de los casos, la velocidad real de enlace de los entre los equipos en ningún caso deberá sobrepasar los 10 Mbps. Sin embargo hay que considerar el dominio MPLS entre los terminales. Por tanto, las velocidades de acceso a los medios serán relativamente lenta.

3.4. Configuración de Parámetros

Considerando que el presente estudio se centra en encontrar la combinación de tecnologías de más alto desempeño, siendo precisamente la rapidez del encapsulamiento de las tramas de capa 2 el factor predominante, el dominio MPLS será lo más básico posible. En la configuración de MPLS –TE no se incorporaran técnicas de rutas alternativas ni auto detección del ancho de banda, sino solamente una ruta explicita con reserva fija de recursos. Es decir se utiliza el protocolo de señalización RSVP-TE pero sin aprovechar sus potencialidades.

El soporte multiprotocolo está dado por la tecnología AToM de Cisco.

3.4.1. Comandos de configuración

3.4.1.1. Protocolos de enrutamiento

Como se menciona, MPLS no reemplaza el enrutamiento clásico IP. El escenario de propuesto implementa OSPF como protocolo IGP, pero puede ser otro. OSPF es el protocolo IGP más utilizado en el internet debido a su gran versatilidad y eficiencia en enrutamiento de paquetes, permitiendo entre otras cosas, una efectiva gestión del tráfico, un excelente control y sincronización entre enrutadores vecinos, único en la gestión de MPLS y sus tablas de estado. A pesar de la complejidad del algoritmo, en relación a sus enormes ventajas, OSPF es el protocolo preferido en el diseño de redes, siendo este un justificativo para ser usado en este trabajo.

Tabla III-II Resumen de comandos de configuración OSPF

	Comando	Propósito
1	configure Ejemplo: router# configure	Ingresa al modo de configuración global.
2	router ospf process-name Ejemplo: router(config)# router ospf 1	Habilita el enrutamiento OSPF. Nota. El argumento process-name es un identificador dl dominio OSPF. Puede tener hasta 40 caracteres.
3	router-id {router-id} Ejemplo: router(config-ospf)# router-id 192.168.4.3	Configura un identificador para el proceso OSPF. Es recomendable usar una dirección IP estable.
4	area area-id ejemplo: router(config-ospf)# area 0	Configura el área para el proceso OSPF. El argumento area-id puedes en notación decimal o notación IPv4.
5	network {broadcast | non-broadcast | {point-to-multipoint [non-broadcast] | point-to-point}} ejemplo: router(config-ospf-ar)# network non-broadcast	Configura el tipo de red OSPF al añadir una red en su tabla local de enrutamiento.

La implementación de BGP es opcional si se trata de un dominio MPLS normal, es decir, que sirva solo de transporte y sobre ella no se hayan construido túneles VPN. BGP gestiona las VRF de las VPN construidas.

En el escenario propuesto se contempla la implementación del mismo a pesar de no ser necesario.

Para habilitar BGP se requiere digitar las siguientes instrucciones.

Tabla III-III Resumen de comandos de configuración BGP.

	Comando	Propósito
1	Router(config)# router bgp as-number	Habilita el proceso de enrutamiento BGP.
2	Router(config-router)# neighbor {ip-address | peer-group-name} remote-as as-number	Específica a un vecino en el dominio BGP.

3.4.1.2. Protocolo MPLS

MPLS tiene la ventaja de ser implementado con tan solo una actualización del sistema operativo de los equipos red. Es decir, las instrucciones para habilitar las funciones avanzadas del mismo son similares a las conocidas para habilitar otras características. A pesar de las múltiples aplicaciones de MPLS, en este trabajo solo se contempla la activación del mismo para que el dominio tenga la posibilidad comportarse como un medio de transporte.

Si el IOS de los enrutadores lo soporta, las siguientes instrucciones inician el MPLS:

Tabla III-IV Resumen de comandos para la configuración de MPLS.

	Comando	Propósito
1	Router(config)# ip cef	Habilita la funcionalidad Cisco Express Forwarding.
2	Router(config-router)# mpls ip	Habilita la funcionalidad MPLS.
3	Router(config-router)# mpls label protocol {ldp | tdp}	Configura el protocolo de distribución de etiquetas utilizado.
4	Router(config)#interface interface-type	Ingresa al modo de configuración de interfaces.
5	Router(config-if)#mpls ip	Habilita la funcionalidad de MPLS en la interfaz de red.
6	Router(config-if)#mpls mtu mtu	Configura el MTU correspondiente a la interfaz.

3.4.1.3. AToM

Como se ya se vio en el Capítulo II, AToM encapsula las tramas de capa 2 que ingresan por un LER, y las conduce a través de una ruta virtual (Pseudowire) hacia el otro LER.

Los LER que van a servir como acople entre las distintos dominios de comunicaciones deberán poseer las capacidades multiprotocolo respectivas.

La principal tarea de AToM es construir rutas virtuales entre los PE y permitir el transporte de tramas de capa 2.

En el escenario propuesto, este soporte lo ofrece AToM de Cisco. Los siguientes comandos permiten habilitar el transporte multiprotocolo de MPLS.

Tabla III-V Resumen comandos de configuración AToM

	Comando	Propósito
1	Router> enable	Ingresa al modo EXEC privilegiado.
2	Router# configure terminal	Ingresa al modo de configuración global.
3	Router(config-if)# interface gigabitethernet4/0	Especifica la interfaz a configurar.
4	Router(config-subif)# xconnect 10.0.0.1 123 encapsulation mpls	Habilita AToM sobre la interfaz identificando el destino del túnel.

3.5. Simulación del Modelo Propuesto

A continuación se exponen los escenarios desarrollados en GNS3 conectando redes de acceso de tecnología Ethernet y Frame Relay, cada una de estas con su respectivo escenario. Estos escenarios serán probados en un dominio MPLS con señalización LDP y a otro con señalización RSVP. Esta combinación da como resultado 4 escenarios de prueba:

- Ethernet y MPLS con señalización LDP
- Ethernet y MPLS con señalización RSVP
- Frame Realy y MPLS con señalización LDP
- Frame Relay y MPLS con señalización RSVP

Los valores correspondientes al retardo, la perdida de paquetes y el Jitter se han obtenido con la aplicación VQManager, mientras que el retardo y la velocidad de transmisión se han obtenido con la herramienta NetTools.

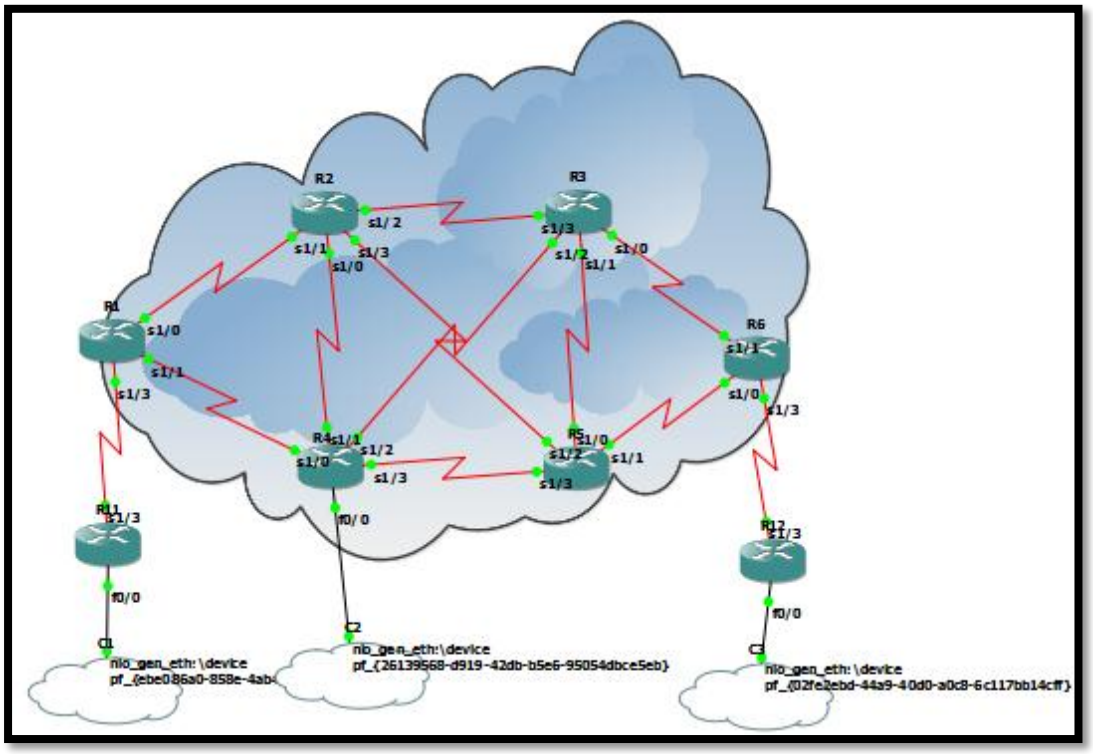


Figura III-17 Escenario construido en GNS3

En el escenario, la nube central permite el monitoreo del dominio MPLS con la herramienta NetFlow Analyzer™. La exportación de las estadísticas de NetFlow está habilitada en todos los enrutadores del dominio MPLS y estas direccionadas hacia el host 192.168.1.42.

Se han realizado las mediciones bajo condiciones de uso de red y desuso de la misma, con la finalidad de apreciar mejor la diferencia en el rendimiento.

3.6. Direccionamiento

En la tabla Tabla III-VI, se especifican el nombre de cada uno de los dispositivos utilizados dentro del escenario de simulación así como las respectivas direcciones IP asignadas a cada una de sus interfaces, también se puede observar la función que cumple cada dispositivo.

Tabla III-VI Direccionamiento IP del escenario propuesto

DISPOSITIVO	FUNCIÓN	INTERFACE	DIRECCIÓN	MASCARA
R1	LER	Loopback	192.168.1.201	255.255.255.255
		S1/0	192.168.1.21	255.255.255.252
		S1/1	192.168.1.21	255.255.255.252
		S1/3	no set	no set
R2	LSR	Loopback	192.168.1.202	255.255.255.255
		S1/0	192.168.1.33	255.255.255.252
		S1/1	192.168.1.2	255.255.255.252
		S1/2	192.168.1.5	255.255.255.252
		S1/3	192.168.1.25	255.255.255.252
R3	LSR	Loopback	192.168.1.203	255.255.255.255
		S1/0	192.168.1.9	255.255.255.252
		S1/1	192.168.1.37	255.255.255.252
		S1/2	192.168.1.30	255.255.255.252
		S1/3	192.168.1.6	255.255.255.252
R4	LSR	Loopback	192.168.1.204	255.255.255.255
		S1/0	192.168.1.22	255.255.255.252
		S1/1	192.168.1.34	255.255.255.252
		S1/2	192.168.1.29	255.255.255.252
		S1/3	192.168.1.17	255.255.255.252
R5	LSR	Loopback	192.168.1.205	255.255.255.255
		S1/0	192.168.1.38	255.255.255.252
		S1/1	192.168.1.13	255.255.255.252
		S1/2	192.168.1.26	255.255.255.252
		S1/3	192.168.1.18	255.255.255.252
R6	LER	Loopback	192.168.1.206	255.255.255.255
		S1/0	192.168.1.14	255.255.255.252
		S1/1	192.168.1.10	255.255.255.252
		S1/3	no set	no set
R11	CE	FastEth0/0	192.168.100.1	255.255.255.0
		S1/3.1	192.168.2.1	255.255.255.0
R12	CE	FastEth0/0	192.168.137.1	255.255.255.0
		S1/3.1	192.168.2.2	255.255.255.0

3.7. Selección del Tráfico de la Red

El tráfico de red es la cantidad de información que se envía o recibe en una red. La importancia de su análisis se debe a que mediante éste, se puede conocer el estado y funcionamiento general de la red, y tendremos la capacidad de establecer los estados de congestión de la misma y el rendimiento.

El tráfico de la red dependerá en gran manera de la topología lógica de la red, así también como la topología física de la misma. Otro factor importante para el análisis de tráfico en la red, son las aplicaciones que están usando la red.

A continuación en la Figura III-18, se presenta el tipo de tráfico que circula por una red de datos, y otras características asociadas a los mismos[27].

Tráfico	Latencia	Fluctuación de Fase	Ancho de Banda
Voz	Bajo	Bajo	Medio
Datos de transacción	Medio	Medio	Medio
Mensajería	Alto	Alto	Alto
Transferencia de archivos	Alto	Alto	Alto
Datos en lote	Alto	Alto	Alto
Administración de red	Alto	Alto	Bajo
Videoconferencia	Bajo	Bajo	Alto

Figura III-18 Tráfico que circula por una red de datos

De acuerdo con lo expuesto en la figura anterior se ha seleccionado, para la presente investigación al tráfico de voz, transferencia de archivos y transmisión de video, estas transmisiones se las realizará simultáneamente con el objetivo de conocer el comportamiento de la red MPLS frente a las distintas tecnologías de acceso estudiadas en este trabajo como son Ethernet y Frame Relay.

En cuanto al tamaño de las tramas en lo que tiene que ver con los datos se usaran un tamaño de 1024 bytes, valor ha sido recomendado por el RFC 2544[28], en cuestiones de evaluación de redes.

[27] Evaluación de Redes-EPN, Guido Pineda Reyes

[28] **RFC 2544. -** Benchmarking Methodology for Network Interconnect Devices.

Para las cuestiones de voz hay que manejar un códec, en este caso se utilizara el códec G729, ya que este utiliza la misma calidad por menor ancho de banda, es pertinente, porque con este códec se puede calcular el ancho de banda, que se requiere para trasmitir todos los servicios que necesite una red.

De acuerdo con las consideraciones de la ITU-T G729[29] se tiene entonces que el tamaño de un paquete de voz es de 98 bytes.

3.8. Obtención de Resultados

Dentro de esta sección se muestra los resultados obtenidos de las mediciones realizadas con las herramientas de monitoreo VQManager y NetTools, de donde se recogieron datos sobre: Latencia, Jitter, Velocidad de Transmisión, Retardo y Pérdida de Paquetes que ya fueron especificados en la sección de Parámetros de Medición.

En la obtención de estos resultados se ha considerado un escenario con y sin carga, ya que al analizar un escenario sin carga podemos ver cuál es comportamiento de la red cuando solamente circulan paquetes de actualización de los diferentes protocolos que intervienen dentro de este diseño y como estos pueden influir en el paso los distintos datos que atraviesan la red. En cada una de las tablas presentadas se tiene el símbolo “ȳ” el cual representa el promedio de los valores obtenidos de cada parámetro medido, los mismos que servirán para realizar el proceso de comparación entre Ethernet y Frame Relay.

---

[29] **ITU-T G729.-** Codificación de la voz a 8 kbit/s.

3.8.1. Ethernet y LDP

Del escenario donde fluye el tráfico de ETH que atraviesa un dominio MPLS haciendo uso de un LSP construido mediante el protocolo LDP, se ha obtenido las siguientes mediciones de cada uno de los parámetros en estudio, las mismas que son tabuladas y representadas gráficamente cómo se las puede observar a continuación:

3.8.1.1. Jitter

Como se puede observar en la Tabla III-VII, para un escenario con sin carga se alcanzado un promedio de 8.4 [ms], mientras que para un escenario con carga 9.1[ms], lo que nos hace pensar que los protocolos que forman parte de la red MPS tambien aportan con cierto trafico circulante que genera un valor de jitter.

Tabla III-VII Valores de Jitter para la combinación ETH + LDP

	ETH + LDP	
Prueba N°	**Sin carga [ms]**	**Con carga [ms]**
1	7	9
2	8	8
3	5	8
4	8	9
5	11	9
6	9	9
7	8	10
8	8	11
9	12	8
10	8	10
$\bar{y}$	8,4	9,1

En la Figura III-19, se puede apreciar de una mejor manera los valores del jitter para los escenarios con carga y sin carga, donde existen puntos en los que el jitter muestra mayor variacion mientras que para esnarios con carga el jitter tiende a ser constante.

Esto se debe a que para escenarios sin carga los protocolos que generan tráfico solo lo hacen cada ciertos periodos de tiempo.

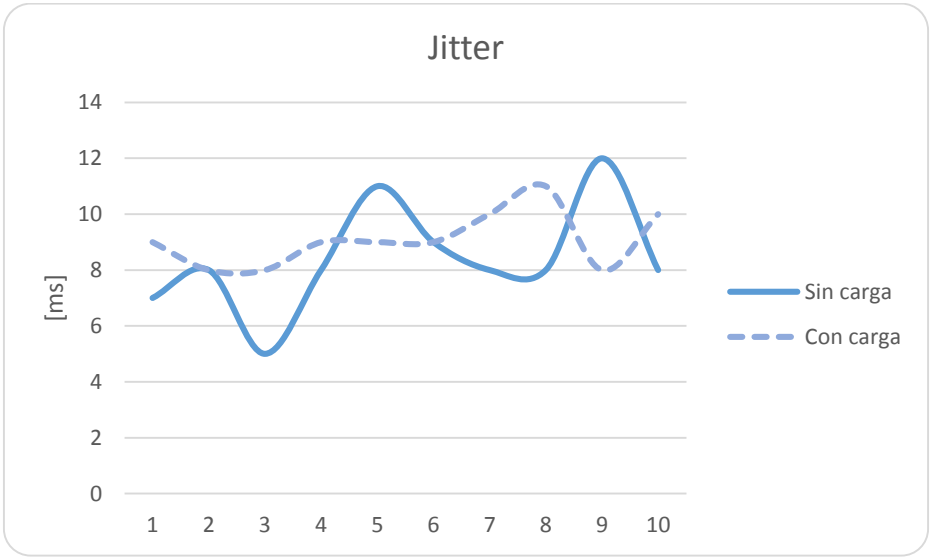


Figura III-19 Representación del Jitter para la combinación ETH + LDP

Fuente: Autores

3.8.1.2. Pérdida de Paquetes

En la Tabla III-VIII, se muestran perdidas las perdidas minimas para los escenarios de prueba es decir que para una la tecnologia de acceso ETH con señalizacion LDP el porcentaje de perdidas es insignificante llegandoa un 0.3 %.

Tabla III-VIII Valores de pérdida de paquetes para la combinación ETH + LDP

	ETH + LDP	
Prueba N°	**Sin carga [%]**	**Con carga [%]**
1	0	0
2	0	0
3	0	0
4	0	0
5	1	0
6	1	0
7	0	0
8	0	0
9	1	0
10	0	0
ȳ	0,3	0

En la Figura III-20, se observa que para el trafico de un escenario sin carga existe un cierto porcentenje de perdidas de paquetes de actualizacion mientra que para con carga los paquetes tienen un promedio del 0%.

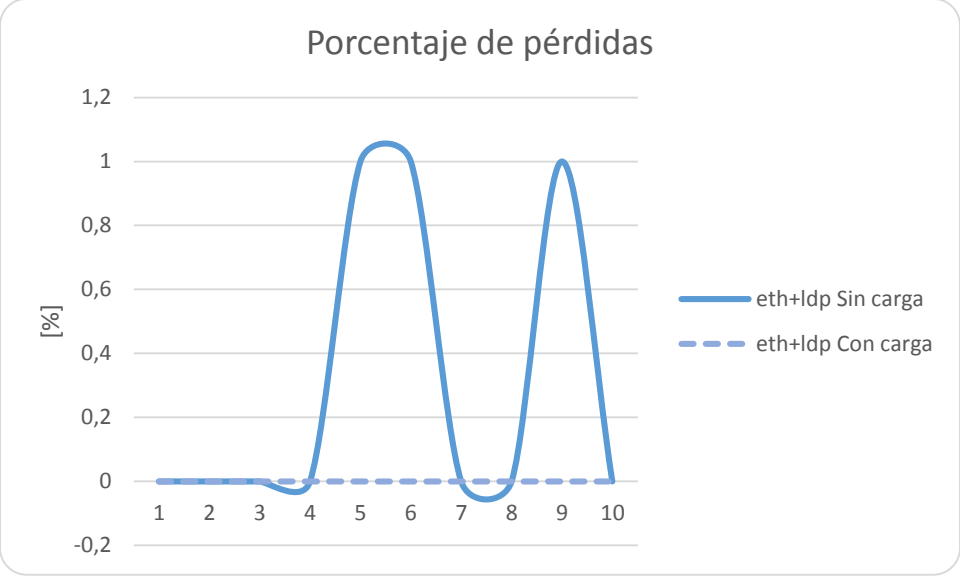


Figura III-20 Representación de pérdida de paquetes en la combinación ETH + LDP

3.8.1.3. Latencia

Con respecto a la latencia con la tecnología ETH con señalización LDP, en la Tabla III-IX, se tiene un promedio de 2543[ms], la que sobrepasa por mucho a un escenario con si carga que tan solo alcanzo un promedio de 226[ms].

Tabla III-IX Valores de Latencia para la combinación ETH + LDP

	ETH + LDP	
Prueba N°	**Sin carga [ms]**	**Con carga [ms]**
1	114	2686
2	125	2131
3	127	2014
4	873	2008
5	3064	3255
6	1845	2459
7	202	2483
8	226	2964
9	240	2543
10	206	2717
$\bar{y}$	702,2	2526

En la Figura III-21, se aprecia de una mejor manera la Latencia alcanzando un pico de 3255 [ms], para un escenario con carga.

Este valor resulta ser muy elevado, sin embargo la probalidad de estos tiempos se presenten es muy baja pero, no nula; por eso la importancia de considerarlos.

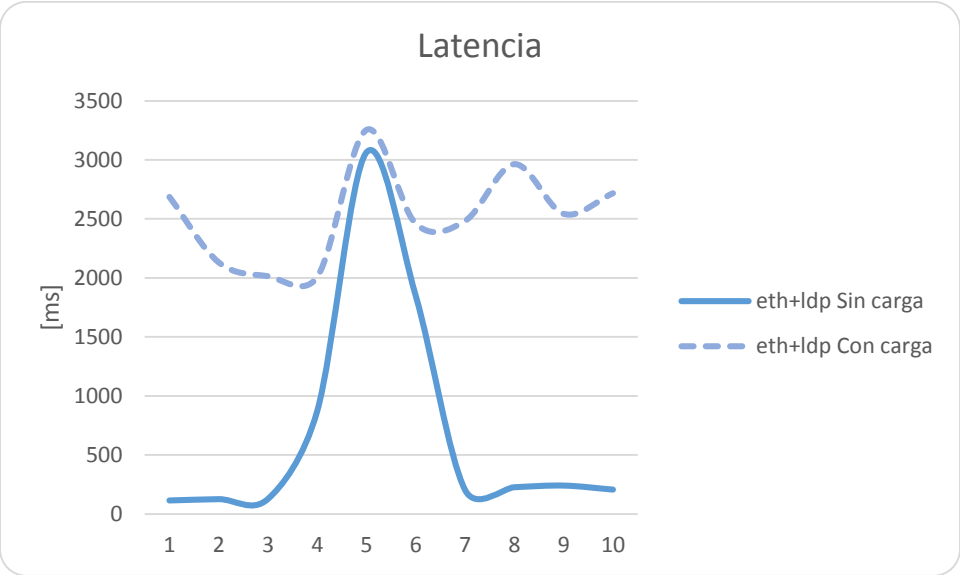


Figura III-21 Representación de la Latencia en la combinación ETH + LDP

3.8.1.4. Velocidad de transmisión

Respecto a la velocidad de transmisión, obviamente se tiene una mayor velocidad en un escenario sin carga con 120[Kbps] y 7[Kbs] para una red cargada.

Se ve una gran diferencia entre éstos ya que al cruzar paquetes de aplicaciones en tiempo real y datos la red requiere de un mayor ancho de banda y por ende de una mayor velocidad en su transmisión.

Estos valores dependen también del tamaño y la complejidad de los paquetes que se estén tratando, entre otros aspectos.

Tabla III-X Valores de la Velocidad de Tx para la combinación de ETH + LDP.

	ETH + LDP	
Prueba N°	**Sin carga [Kbps]**	**Con carga [Kbps]**
1	140,95	6,20
2	138,65	7,91
3	151,32	10,15
4	142,3	9,30
5	107,5	5,00
6	100,7	7,07
7	122,3	6,50
8	96,17	5,46
9	98,38	7,20
10	105,47	6,18
ȳ	120,374	7,097

La Figura III-22, muestra claramente la variación de la velocidad de transmision para un escenario con carga y sin carga, donde es evidente el decremento de l avelocidad al saturar la red.

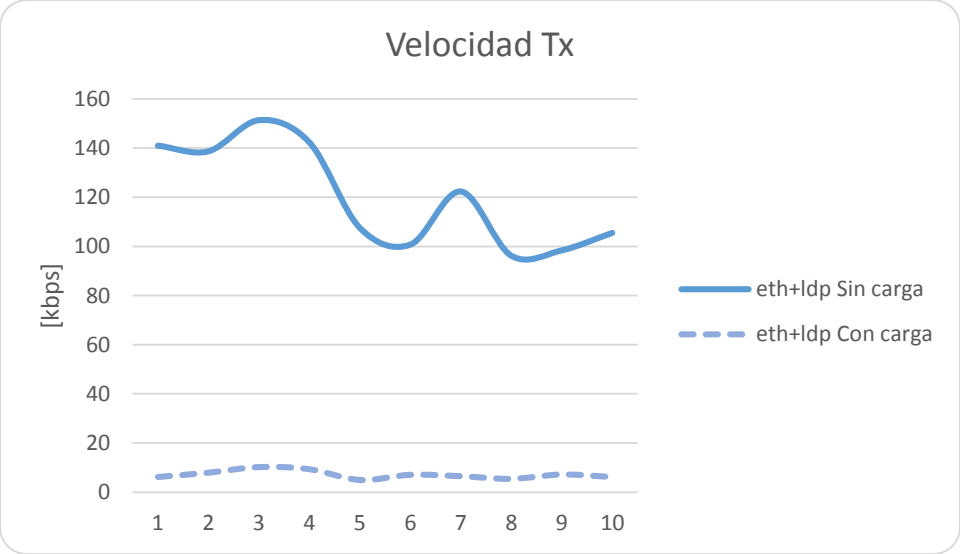


Figura III-22 Representación de la Velocidad Tx en la combinación ETH + LDP

3.8.1.5. Retardo

En retardo que presenta esta combinación de tecnologías ETH+LDP, es mínimo tanto para una red cargada como sin carga llegando un promedio en ambos casos de 0,5 [ms], el mismo que es muy bajo con relación a los valores establecidos en la sección, Parámetros de Medición resumida en la Tabla III-XI.

Tabla III-XI Valores de Retardo para la combinación ETH + LDP.

	ETH + LDP	
Prueba N°	**Sin carga [ms]**	**Con carga [ms]**
1	2	1
2	1	1
3	2	3
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
$\bar{y}$	0,5	0,5

Al observar la Figura III-23, se puede notar que en la prueba 3 para un escenario sin carga existe un notable crecimeinto del retardo llegando hasta los 3[ms].

A pesar de estas observaciones, el retardo suele ser minimo y permitira tener una buena calidad de comunicaiones, al menos desde este punto de vista.

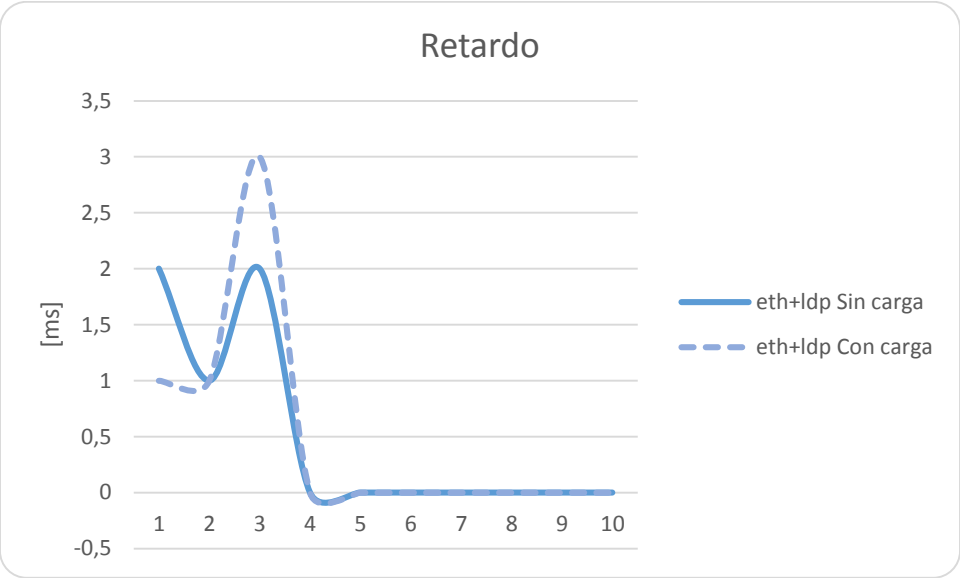


Figura III-23 Representación del Retardo en la combinación ETH + LDP.

3.8.2. Ethernet y RSVP

Para el tráfico de ETH que atraviesa un dominio MPLS haciendo uso de un LSP construido mediante el protocolo RSVP, se ha obtenido las siguientes mediciones para los parámetros de medición estudiados:

3.8.2.1. Jitter

El Jitter para la combinación ETH+RSVP mejora en relación al uso del protocolo de señalización LDP, ya que disminuyo hasta llegar a un promedio de 6,4 [ms] y 8,6 [ms] para un escenario sin carga y con carga respectivamente como se muestra en la Tabla III-XII.

Tabla III-XII Valores de Jitter para la combinación ETH + RSVP

	ETH + RSVP	
Prueba N°	**Sin carga [ms]**	**Con carga [ms]**
1	7	8
2	6	9
3	6	7
4	6	8
5	7	8
6	6	8
7	6	10
8	7	9
9	6	10
10	7	9
ȳ	6,4	8,6

La Figura III-24, muestra una notable variación, llegando así a un valor máximo de 10 [ms] para un escenario cargado, valores que fueron medidos para las pruebas 7 y 9.

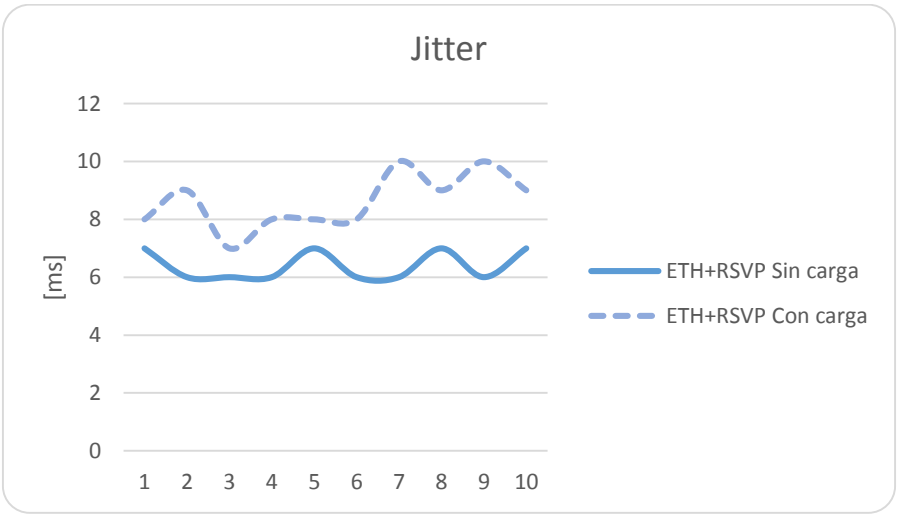


Figura III-24 Representación del Jitter en la combinación ETH + RSVP

3.8.2.2. Pérdida de Paquetes

Al usar el protocolo RSVP, se tiene un promedio de pérdida de paquetes del 1 %, el mismo que es menor al medido usando el protocolo LDP.

Tabla III-XIII Valores de pérdida de paquetes en la combinación ETH + RSVP

	ETH + RSVP	
Prueba N°	**Sin carga [%]**	**Con carga [%]**
1	2	0
2	0	0
3	0	0
4	0	0
5	0	0
6	2	0
7	0	0
8	0	0
9	6	0
10	0	0
ȳ	1	0

La Figura III-25, muestra claramente qu existio mayor perdida en la prueba 9 llegando a un valor de 6 %, que en las pruebas restantes son bastantes reducidas.

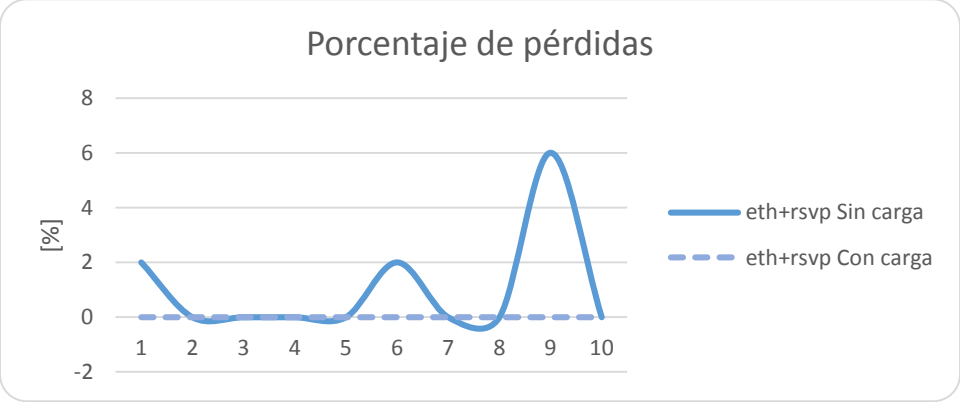


Figura III-25 Representación de pérdida de paquetes en la combinación ETH + RSVP

3.8.2.3. Latencia

En la Tabla III-XIV, para la combinacion ETH+RSVP tenemos un promedio de 164.3 [ms] y 1110 [ms] para un escenario sin carga y con carga respectivamente. Concluyendo asi que se presenta un incremento considerable entre un escenario y otro.

Tabla III-XIV Valores de Latencia en la combinación ETH + RSVP

	ETH + RSVP	
Prueba N°	**Sin carga [ms]**	**Con carga [ms]**
1	119	1141
2	121	994
3	114	1117
4	174	1141
5	175	997
6	202	1002
7	182	1247
8	171	1184
9	168	1115
10	217	1171
$\bar{y}$	164,3	1110,9

Al observar la Figura III-26, se nota claramente el incremento de Latencia para un escenario cargado valores que permanecen presenta ciertas variaciones en cada prueba llegando a un valor máximo de 1247 [ms].

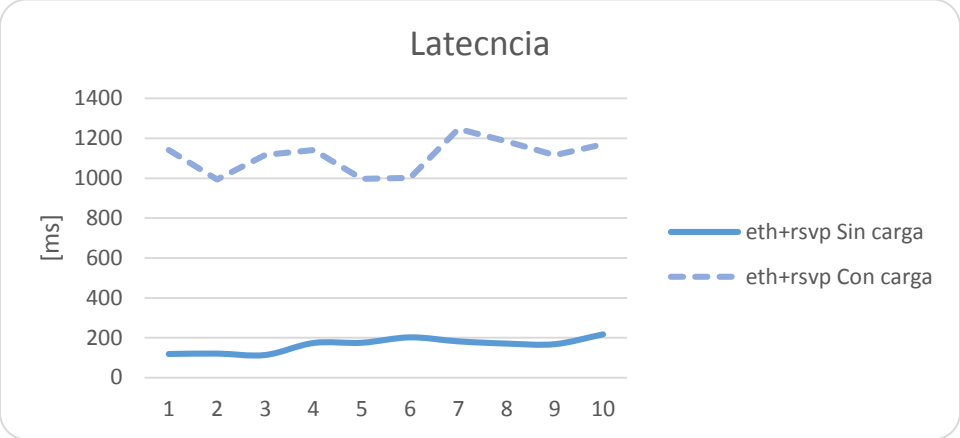


Figura III-26 Representación de la Latencia en la combinación ETH + RSVP

3.8.2.4. Velocidad de transmisión

La velocidad de transmisión q se muestra en la Tabla III-XV, a mejorado casi al doble en relacion al uso de ETH + LDP, entonces cada vez se puede notar que el protocolo de señalizacion RSVP trata de mejor manera la transmision de trafico a traves del domino MPLS.

Asi tenemos un promedio de 130 [Kbps] y 15 [Kbps] para los escenarios sin carga y con carga espectivmanete.

Tabla III-XV Valores de la Velocidad de Tx en la combinación ETH + RSVP

	ETH + RSVP	
Prueba N°	**Sin carga [Kbps]**	**Con carga [Kbps]**
1	145,65	14,95
2	145,62	16,71
3	142,41	15,06
4	102,48	14,52
5	138,74	16,11
6	111,45	16,07
7	129,06	14,05
8	128,67	14,80
9	112,88	14,73
10	150,37	14,28
$\bar{y}$	130,733	15,128

La Figura III-27, muestra que la velocdad de transmision alcanza hasta una velocidad maxima de 145 [Kbps] para una red sin carga y un valor de 16 [Kbps] para uno transmitiendo informacion.

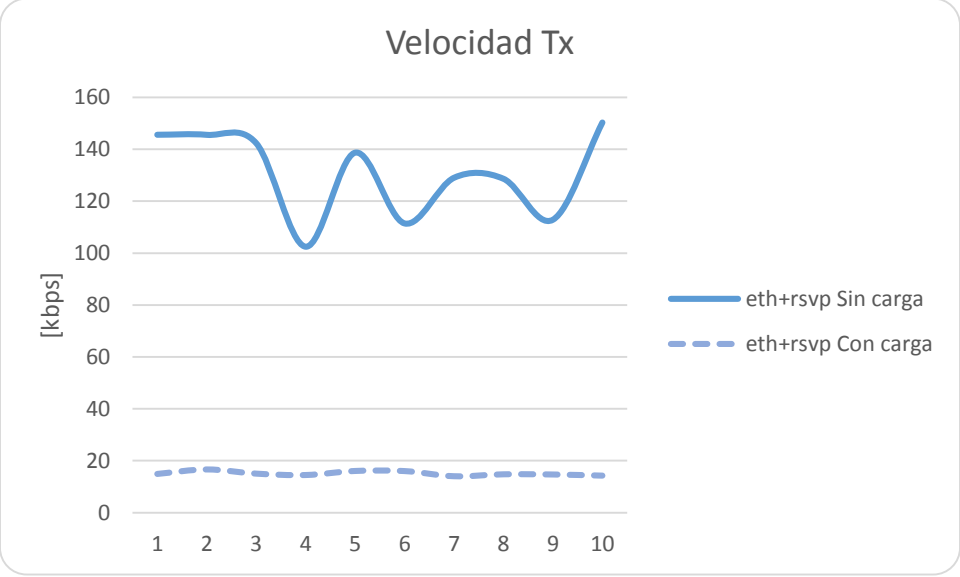


Figura III-27 Representación de la Velocidad Tx en la combinación ETH + RSVP

3.8.2.5. Retardo

Los datos del retardo mostrados en la Tabla III-XVI, llegan a un promedio de 1 y 1.8 [ms] para una red sin carga y cargado, que en relacion al uso del protocolo LDP representan valores mayores por que se le puede restar un punto al protocolo de señalizacion RSVP que es utilizado en esta combinacion de tecnologías.

Tabla III-XVI Valores del Retardo en la combinación ETH + RSVP

	ETH + RSVP	
Prueba N°	**Sin carga [ms]**	**Con carga [ms]**
1	1	2
2	1	0
3	1	2
4	1	2
5	1	2
6	1	2
7	1	2
8	1	2
9	1	2
10	1	2
$\bar{y}$	1	1,8

En la Figura III-28, se observa que el retardo permanece constante para unescenario sin carga con un valor de 1 [ms], mientras que para una red carcagda existe una variacion entre 0 y 2 [ms].

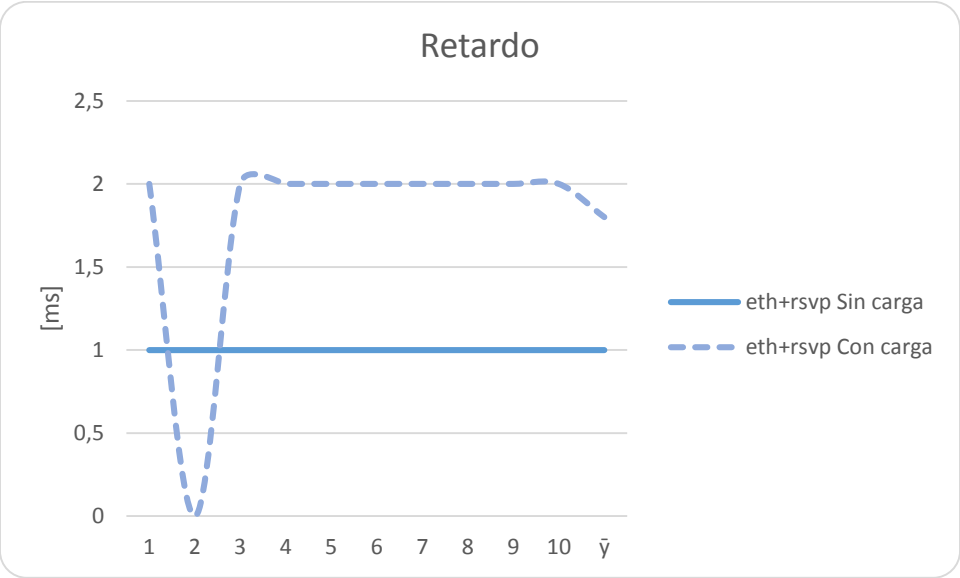


Figura III-28 Representación del Retardo en la combinación ETH + RSVP

3.8.3. FR y LDP

Para el tráfico de FR que atraviesa un dominio MPLS haciendo uso de un LSP construido mediante el protocolo LDP, se ha obtenido los siguientes los valores para los parámetros de medición:

3.8.3.1. Jitter

En cuanto al Jitter con tecnología FR, en la Tabla III-XVII, se tiene un promedio de 22,2 [ms], la que sobrepasa a un escenario sin carga que tan solo alcanzó un promedio de 7,9 [ms].

Tabla III-XVII Valores del Jitter para la combinación FR + LDP

	FR + LDP	
Prueba N°	**Sin carga [ms]**	**Con carga [ms]**
1	6	9
2	9	9
3	6	8
4	7	15
5	9	19
6	9	26
7	9	33
8	10	37
9	7	33
10	7	33
$\bar{y}$	7,9	22,2

En la Figura III-29, se observa como el jitter crece hasta alcanzar un pico de 37 [ms], para un escenario cargado, mientras que para un escenario sin carga se mantiene una curva casi constante con un valor máximo de aproximadamente 10[ms].

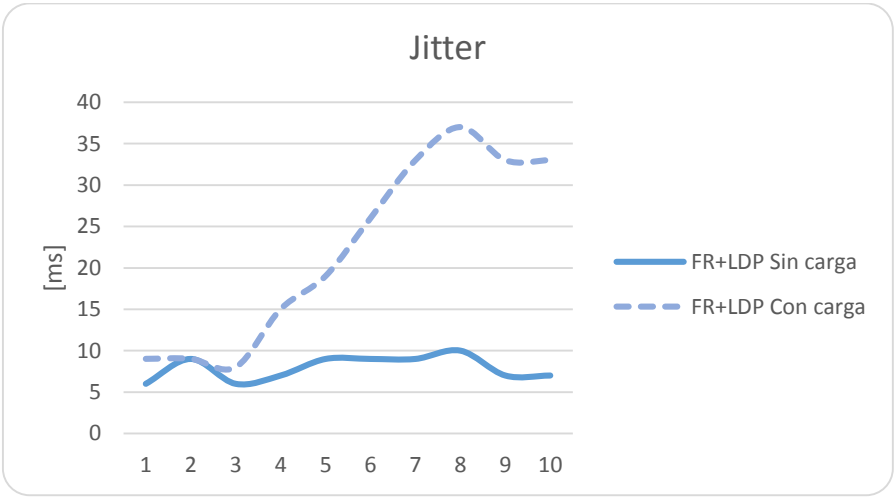


Figura III-29 Representación del Jitter para la combinación FR + LDP

3.8.3.2. Pérdida de Paquetes

En cuanto a la perdida de paquetes, en la Tabla III-XVIII, se tiene un promedio de 10,2 [%] en un escenario congestionado, lo que sobrepasa a un escenario sin carga que se mantuvo en 0 [%].

Tabla III-XVIII Valores de la perdida de paquetes para la combinación FR + LDP

	FR + LDP	
Prueba N°	**Sin carga [%]**	**Con carga [%]**
1	0	0
2	0	0
3	0	0
4	0	0
5	0	6
6	0	9
7	0	20
8	0	20
9	0	22
10	0	25
$\bar{y}$	0	10,2

La Figura III-30, muestra como el porcentaje de pérdidas crece hasta llegar a un 25 %, esto sucede para un escenario cargado, mientras que para uno sin carga se mantiene en 0%.

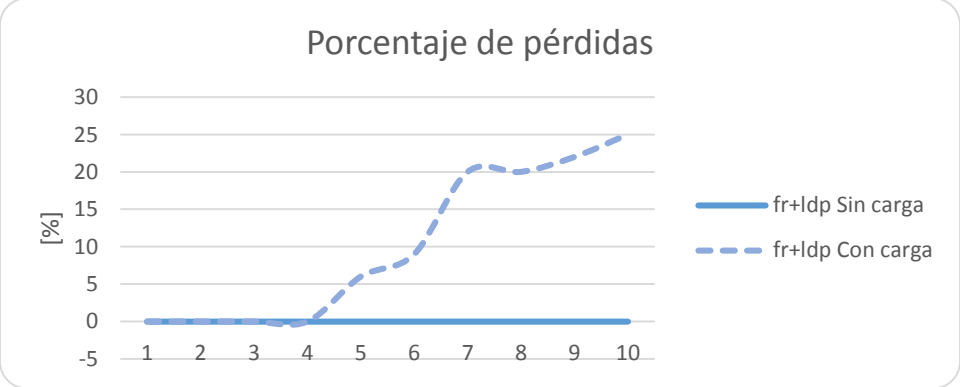


Figura III-30 Representación de la perdida de paquetes para la combinación FR + LDP

3.8.3.3. Latencia

En lo referente a la latencia, en la Tabla III-XIX, se tiene un promedio de 1853,9 [ms] en un escenario congestionado, en relación a 101,9 [ms] en un escenario sin congestión.

Tabla III-XIX Valores de la latencia para la combinación FR + LDP

	FR + LDP	
Prueba N°	**Sin carga [ms]**	**Con carga [ms]**
1	99	1149
2	105	1166
3	98	1205
4	103	1192
5	102	1198
6	107	2134
7	107	2597
8	100	2621
9	99	2662
10	99	2615
$\bar{y}$	101,9	1853,9

Para la latencia en la Figura III-31, se observa que existe una variación que alcanza un valor máximo de 2662 [ms] el mismo que por un lapso de tiempo permanece constate para una red congestionada y para una red sin congestión se tiene un valor casi constante de 100 [ms].

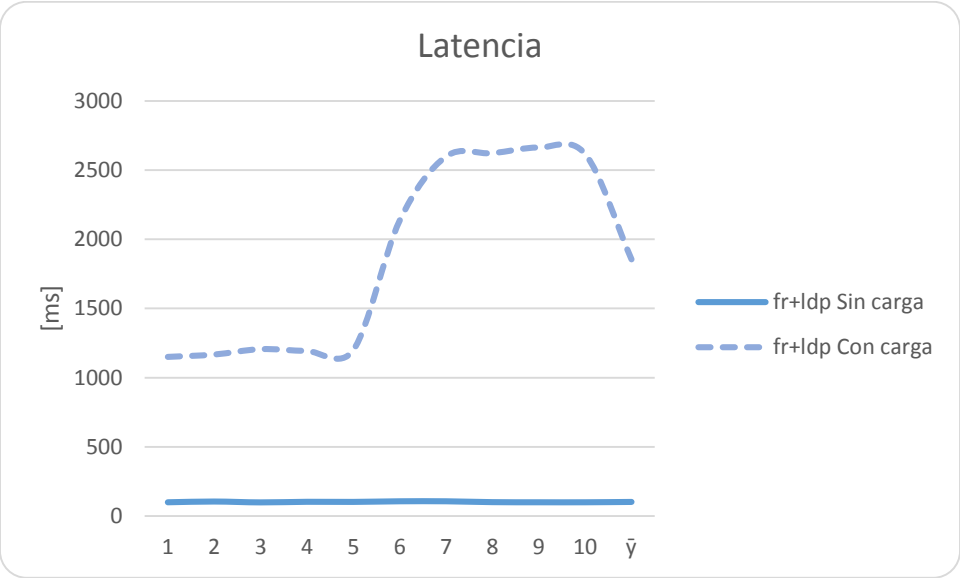


Figura III-31 Representación de la latencia para la combinación FR + LDP

3.8.3.4. Velocidad de Transmisión

En cuanto a la velocidad de transmisión, en la Tabla III-XX, se tiene un promedio de 10,58 [kbps] en un escenario congestionado, que dista bastante de 149,8 [kbps] en un escenario sin congestión.

Tabla III-XX Valores de la velocidad de Tx para la combinación FR + LDP

	FR + LDP	
Prueba N°	**Sin carga [Kbps]**	**Con carga [Kbps]**
1	100	14,71
2	162,73	15,00
3	160	13,81
4	168,28	14,45
5	164,4	13,85
6	157,74	7,83
7	162,79	6,44
8	159,05	6,40
9	105	6,48
10	158,29	6,90
ȳ	149,828	10,587

En la Figura III-32, se muestra que la velocidad de transmisión alcanza un valor máximo de 15 [Kbps], mientras que para un escenario sin cargar este valor obviamente se incrementa hasta llegar a un valor de aproximadamente de 162 [Kbps].

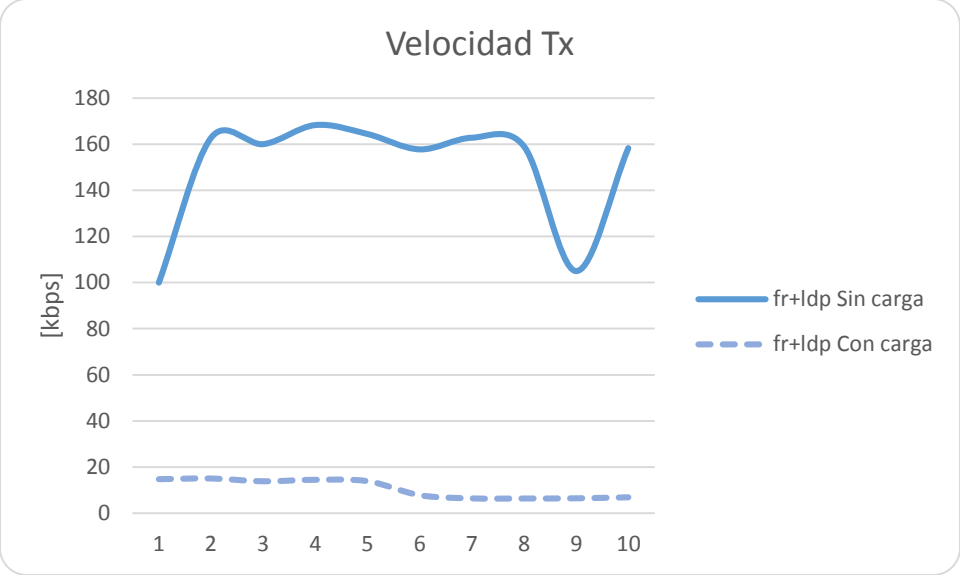


Figura III-32 Representación de la Velocidad Tx para la combinación FR + LDP

3.8.3.5. Retardo

El retardo experimentado en la tecnología FR se aprecia en la Tabla III-XXI; se tiene un promedio de 0,6 [ms] en un escenario congestionado, en relación a 1,5 [ms] en un escenario sin congestión.

Tabla III-XXI Valores del retardo para la combinación FR + LDP

	FR + LDP	
N°	Sin carga [ms]	Con carga [ms]
1	2	1
2	1	2
3	1	1
4	1	1
5	1	1
6	2	0
7	2	0
8	2	0
9	2	0
10	1	0
ȳ	1,5	0,6

El retardo para FR+LDP presenta un descenso, como se puede ver en la Figura III-33, ya que este valor que en un principio está en 2 [ms] baja hasta llegar 0[ms], esto para una red congestionada, en tanto para una red sin congestión se tiene una variación de entre 1 y 2[ms].

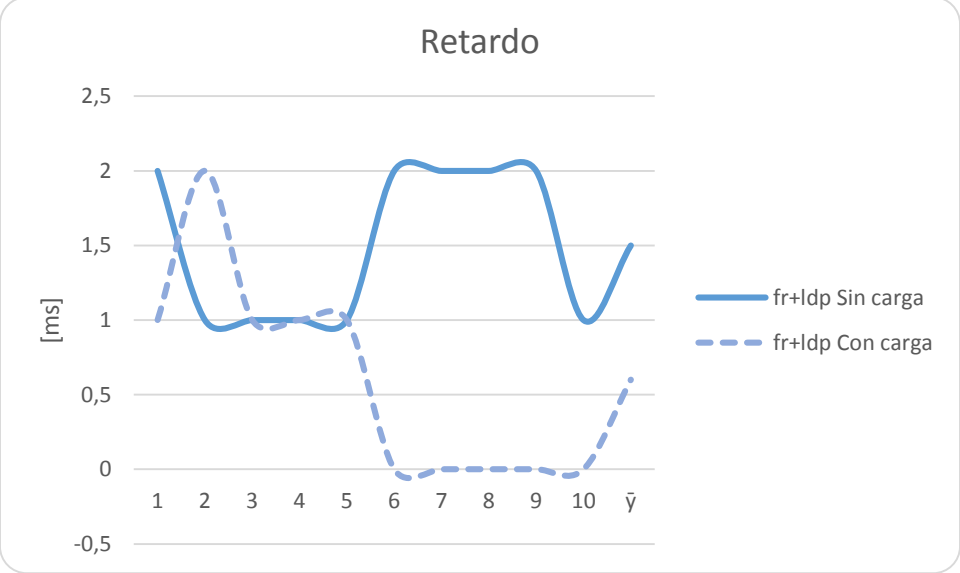


Figura III-33 Representación del retardo para la combinación FR + LDP

3.8.4. FR y RSVP

Para el tráfico de FR que atraviesa un dominio MPLS haciendo uso de un LSP construido mediante el protocolo RSVP, se obtuvieron las siguientes mediciones para los parámetros de medición estudiados:

3.8.4.1. Jitter

En cuanto al Jitter con tecnología FR incluyendo RSVP, en la Tabla III-XXII, se tiene un promedio de 22,2 [ms], la que sobrepasa a un escenario sin carga que tan solo alcanzó un promedio de 8,6 [ms].

Tabla III-XXII Valores del Jitter para la combinación FR + RSVP

	FR + RSVP	
N°	Sin carga [ms]	Con carga [ms]
1	6	24
2	6	22
3	7	26
4	6	27
5	19	28
6	8	21
7	8	20
8	10	19
9	8	18
10	8	17
$\bar{y}$	8,6	22,2

El jitter para esta combinacion de tecnologias FR + RSVP, alcanza un pico de 28 [ms], dentro de un escenario con carga mientras que en un escenario sin carga este valor tan solo alcanza 19 [ms], como se lo puede observar en la Figura III-34.

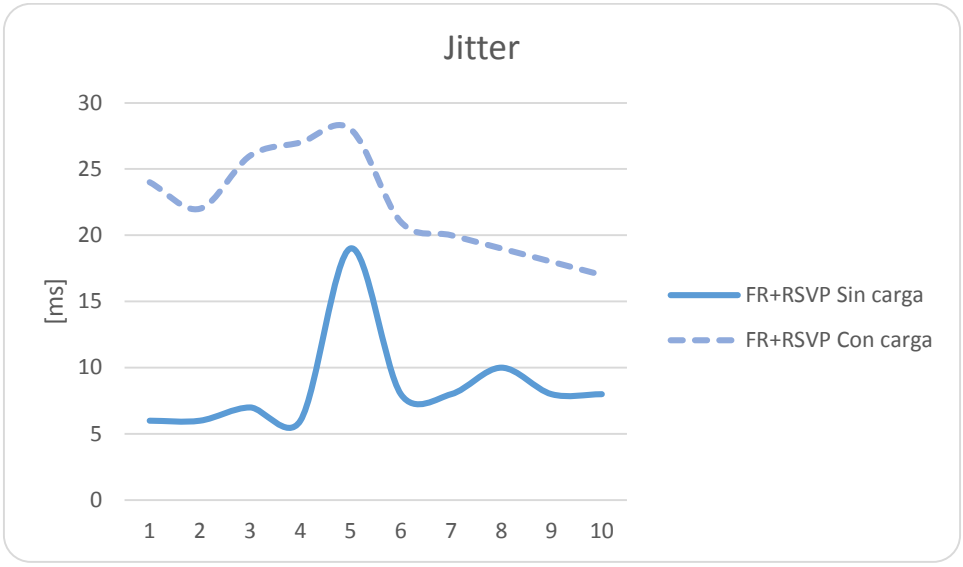


Figura III-34 Representación del Jitter para la combinación FR + RSVP

3.8.4.2. Pérdida

En cuanto a la pérdida de paquetes, en la Tabla III-XXIII, se tiene un promedio de 7,4 [%] en un escenario congestionado, lo que sobrepasa a un escenario sin carga que se mantuvo en 0 [%].

Tabla III-XXIII Valores de la perdida de paquetes para la combinación FR + RSVP

	FR + RSVP	
Prueba N°	**Sin carga [%]**	**Con carga [%]**
1	0	5
2	0	11
3	0	9
4	0	10
5	0	11
6	0	7
7	0	5
8	0	6
9	0	5
10	0	5
$\bar{y}$	0	7,4

La Figura III-35, presenta un porcentaje de pérdidas que alcanza el 11% para un escenario congestionado y un 0% para uno descongestionado.

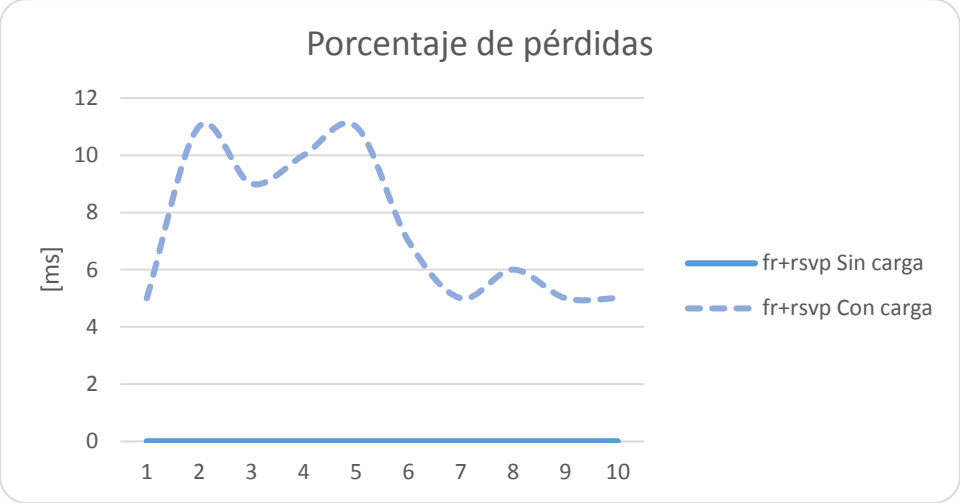


Figura III-35 Representación de la perdida de paquetes para la combinación FR + RSVP

3.8.4.3. Latencia

En lo referente a la latencia, en la Tabla III-XXIV, se tiene un promedio de 2126,6 [ms] en un escenario congestionado, en relación a 113,2 [ms] en un escenario sin congestión.

Tabla III-XXIV Valores de la latencia para la combinación FR + RSVP

	FR + RSVP	
Prueba N°	**Sin carga [ms]**	**Con carga [ms]**
1	101	1440
2	103	2567
3	103	2549
4	119	2749
5	113	2157
6	117	2080
7	115	2050
8	125	2057
9	114	2228
10	122	1389
$\bar{y}$	113,2	2126,6

En la Figura III-36, se observa como la latencia dentro de un escenario congestionado llega a un valor máximo de 2749 [ms], mientras que en un escenario sin congestión mantiene valores constantes de que bordean aproximadamente los 100[ms].

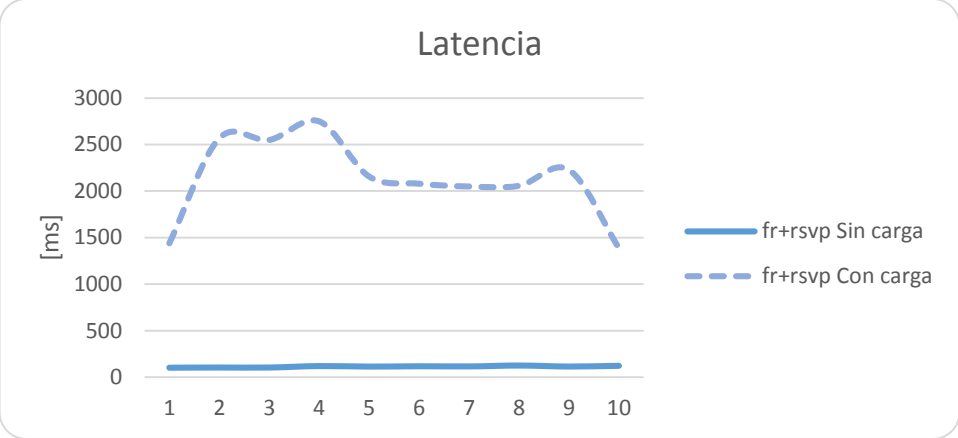


Figura III-36 Representación de la latencia para la combinación FR + RSVP

3.8.4.4. Velocidad de transmisión

En cuanto a la velocidad de transmisión, en la Tabla III-XXV, se tiene un promedio de 7,97 [kbps] en un escenario congestionado, que dista bastante de 150,3 [kbps] en un escenario sin congestión.

Tabla III-XXV Valores de la Velocidad de Tx para la combinación FR + RSVP

	FR + RSVP	
Prueba N°	**Sin carga [Kbps]**	**Con carga [Kbps]**
1	164,04	11,58
2	160,72	6,67
3	163,46	6,66
4	143,22	2,26
5	149,08	7,90
6	148,41	8,55
7	150,82	8,23
8	133,34	8,85
9	149,53	7,50
10	140,4	11,54
ȳ	150,302	7,974

En la Figura III-37, se observa que la velocidad de transmisión para un escenario sin congestión alcanza un valor de 164 [kbps], el mismo que decrece lentamente conforme pasa el tiempo. En cuanto a un escenario congestionado vemos que su velocidad mantiene un valor casi constante de 8 [kbps].

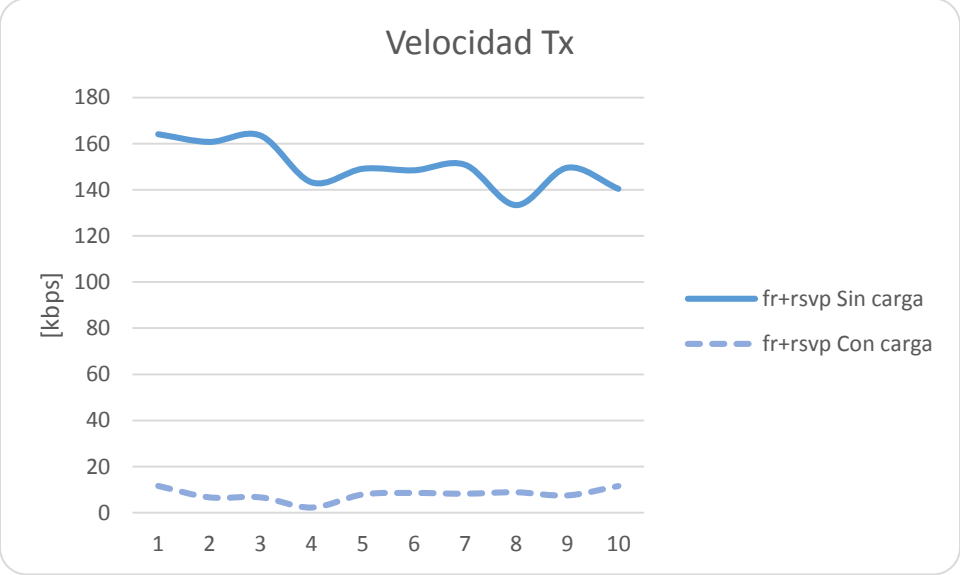


Figura III-37 Representación de la Velocidad Tx para la combinación FR + RSVP

3.8.4.5. Retardo

El retardo experimentado en la tecnología FR se aprecia en la Tabla III-XXVI; donde se tiene un promedio de 0,8 [ms] en un escenario congestionado, en relación a 1,1 [ms] en un escenario sin congestión.

Los valores para los dos casos son bajos y no afectan el rendimiento general de las comunicaciones, sean de tiempo real o no.

Tabla III-XXVI Valores del retardo para la combinación FR + RSVP

	FR + RSVP	
Prueba N°	**Sin carga [ms]**	**Con carga [ms]**
1	0	0
2	1	0
3	1	0
4	1	2
5	1	0
6	2	1
7	1	1
8	2	1
9	0	1
10	2	2
$\bar{y}$	1,1	0,8

La Figura III-38, presenta al retardo con visibles variaciones tanto para un escenario con carga y sin carga, alcanzando picos de 2 [ms] en ambos casos.

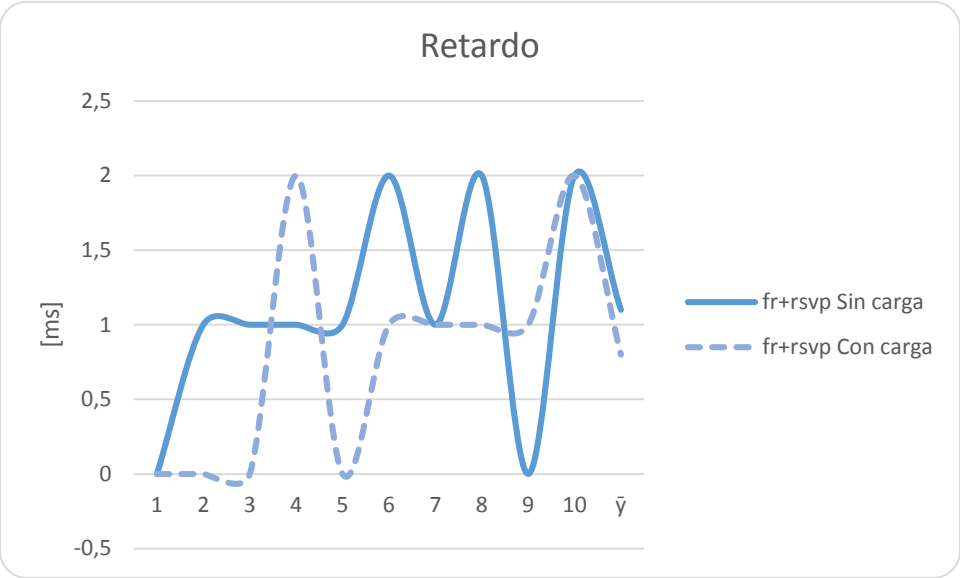


Figura III-38 Representación del retardo para la combinación FR + RSVP

3.9. Resumen de Parámetros de Medición

Finalmente, lo que interesa para realizar la comprobación de la hipótesis, en el capítulo siguiente, es un resumen conformado por los promedios del conjunto de mediciones relacionadas. Es decir se tomara cada uno de los promedios (ȳ) calculadas en las tabulaciones representadas en la sección anterior para cada uno de los parámetros como son: jitter, latencia, perdida de paquetes velocidad de transmisión y retardo.

En la TablaIII-XXVII, se presentan los promedios de cada uno de estos parametros, se toman las mediciones para un escenario congestionado, que es lo que se necesita para empezar con el analisis de los resultados obtenidos por las herramientas de medicion VQManager y NetTools.

Tabla III-XXVII Resumen de los Parámetros Medidos

	ETH + LDP	ETH + RSVP	FR + LDP	FR + RSVP
Jitter [ms]	9,1	8,6	22,2	22,2
Retardo [ms]	0	1,8	0,6	0,6
Pérdida [%]	0	0	10,2	7,4
Latencia [ms]	2526	1110,9	1853,9	2126,6
Velocidad Tx [kbps]	7,1	15,13	1,59	7,97

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

En el presente capítulo se pretende realizar un análisis técnico de los datos recolectados y expuestos anteriormente. Para eso, primeramente, se explicara la metodología de investigación utilizada así como los instrumentos que permitan validar la hipótesis.

Existen diferentes indicadores que pueden referenciar el rendimiento de una red, cada uno de ellos basados en distintos parámetros, y por ende aplicables de acuerdo al tipo de tráfico que circule por determinada topología de red. Sin embargo existen indicadores que pueden ser comunes entre si y pueden ser aplicables a cualquier escenario, determinando así las potencialidades de la misma.

Considerando la convergencia actual de las redes, en las cuales el principal tráfico circulante es el tiempo real y siendo precisamente este el que tiende a crecer con mayor rapidez a futuro se considera al Jitter, a la perdida de paquetes y al retardo como los indicadores más influyentes en la

determinación de QoS. Pero como es lógico de imaginar, las redes nunca se verán saturadas con tráfico de tiempo real solamente. El tráfico de datos es indispensable, y este no es sensible a los indicadores antes mencionados por lo que también es importante medir la velocidad de transferencia y la latencia.

Cada uno de los cinco parámetros a estudiarse mantiene ciertos valores límites recomendados por los organismos especializados en las redes de datos para garantizar una exitosa, segura y confiable comunicación. A partir de estos valores puede existir una cierta tolerancia alrededor de los mismos, lo cual se revisara a través del análisis respectivo.

Aquella combinación de tecnologías, en la que sus indicadores presente la menor variación entorno los valores sugeridos puede considerarse la más adecuada.

4.1. Metodología de investigación utilizada

En este trabajo se ha utilizado el método deductivo ya que a partir de conceptos generales se ha llegado a una suposición que después de la experimentación a través del tratamiento de los datos obtenidos de las mediciones se llegara a comprobar la suposición planteada.

Por esto es necesario conocer un poco más acerca del método deductivo el cual se explica a continuación.

4.1.1. Método Deductivo

En el método deductivo, se suele decir que se pasa de lo general a lo particular, de forma que partiendo de unos enunciados de carácter universal y utilizando instrumentos científicos, se infieren enunciados particulares, pudiendo ser axiomático-deductivo, cuando las premisas de partida están

constituidas por axiomas, es decir, proposiciones no demostrables, o hipotéticos-deductivo, si las premisas de partida son hipótesis contrastables.

Este método obliga al investigador a combinar la reflexión racional o momento racional, o sea, una relación entre un criterio hipotético con la razón, con la observación de la realidad o momento empírico.

4.1.2. Fases del método deductivo

Las siguientes son las fases en las cuales se desarrolla el método deductivo, y se seguido en el desarrollo de la presente investigación:

- **Observación.-** Se ha realizado un análisis previo en el cual se pudo verificar la viabilidad del presente trabajo de investigación, debido a carencia de un estudio que verifique el rendimiento Frame Relay y Ethernet al integrarse a un dominio MPLS.
- **Planteamiento de hipótesis.-** en base a la observación y la experiencia, se emitió un criterio hipotético que prioriza a una tecnología en particular frente a MPLS.
- **Deducciones de conclusiones a partir de conocimientos previos.-** los conocimientos previos adquiridos por la experiencia de los proponentes de la investigación y los estudios realizados con anterioridad, han influido para emitirse una propuesta hipotética y una metodología para lograr desmentirla.
- **Verificación.-** tras seguir un adecuado marco metodológico, se procede a la comparación de los resultados estadísticos obtenidos en los escenarios de prueba con la finalidad de comprobar el criterio hipotético.

El método deductivo es influenciado por principio y teorías ya aceptadas con anterioridad por la comunidad científica y las utiliza para inferir una situación particular del tema de estudio. Sin embargo no profundiza en sus causas.

Esta particularidad, hace que el método deductivo sea el adecuado en el tratamiento del presente tema de investigación, ya que se propone un criterio a partir los estándares existentes en el campo de las telecomunicaciones, utilizando para ello algunos índices medibles, pero sin profundizar en el cómo y el porqué de los mismos.

4.1.3. Caracterización de la hipótesis

La hipótesis planteada al inicio de la presente investigación fue:

Hi: Las redes Ethernet sobre una arquitectura MPLS proporcionará un mejor rendimiento que una red Frame Relay bajo similares condiciones de prueba.

Como se puede apreciar, esta es una hipótesis que de antemano, se anticipa a los resultados, y esta afirmación se la realiza en función de los conocimientos teóricos de los autores y otros estudios relacionados al tema que ya han sido desarrollados.

Entonces, se concluye que esta hipótesis es el de tipo descriptiva. En estas, se puede prescindir de variables y su comprobación se reduce a un sencillo análisis estadístico de los valores definidos para ciertos índices, los mismos que están relacionados con algunos indicadores de acuerdo a su afinidad.

En base a este criterio, a continuación se agruparán a los índices medidos en indicadores para su posterior tratamiento.

4.1.4. Determinación de Indicadores e Indicadores

En el Capítulo 3 se consideraron algunos aspectos técnicos mensurables que, tras su respectiva justificación, se consideraron como los necesarios para demostrar la hipótesis planteada y, en efecto, fueron medidos.

En realidad, estos son índices que permiten evaluar la calidad de una red de datos y, posiblemente de cualquier red de comunicaciones.

Sin embargo, para un análisis estadístico más meticuloso, es necesario la agrupación de estos índices en grupos, denominados indicadores.

La necesidad de integrar comunicaciones de voz, video y datos ha provocado la aparición de nuevas redes y protocolos, dando a conocer la enorme importancia de las comunicaciones de tiempo real y el rendimiento de este tipo de tráfico podrá ser evaluado en función de tres índices: Jitter, retardo, pérdidas de paquetes. Sin dejar a un lado las comunicaciones corrientes de datos, este tráfico será evaluado por los siguientes 2 parámetros: latencia y la velocidad de transmisión, también denominados índices para este estudio.

Tabla IV-I Determinación de indicadores y sus índices

Indicador	**Índice**
Transmisión RT	Jitter
	Retardo
	Pérdidas
Transmisión NRT	Latencia
	Velocidad Tx

Se ha considerado estos indicadores ya que, es este el tipo de tráfico que circula por el escenario de simulación planteado en el Capítulo III.

Esta agrupación se la realiza para poder reducir la complejidad en el tratamiento final de los datos, pero sobre todo, para darle más sentido al uso de cada índice, ya que justifica que estos influyen directamente a un indicador en especial.

El indicador 1 hace referencia a las transmisiones en tiempo real (RT, Real Time) mientras que el indicador 2, a las transmisiones normales de datos, conocidas también como transmisiones en tiempo no real (NRT, Non Real Time).

4.1.4.1. Transmisión RT

Este indicador trata de describir, a través índices, ciertos inconvenientes que pueden llegar a tener las comunicaciones de tiempo real, durante su viaje por una red de comunicaciones y que difieren de una comunicación normal de datos, cuyo tratamiento no es el mismo.

4.1.4.2. Transmisión NRT

Siempre ha de existir tráfico convencional, de carga y descarga hacia el internet, en el que se puede prescindir la priorización necesaria como en el caso del tráfico RT, siendo finalmente la velocidad de transferencia el principal punto a considerar. Este indicador nos ayuda a verificar la eficiencia de una red para este tipo de tráfico.

Una vez que han sido definidos los indicadores e índices, se procederá a la comparación respectiva y la comprobación de la hipótesis con la debida formalidad del caso.

4.2. Evaluación y comparación de los indicadores

En esta sección del capítulo se van a consideran las medidas obtenidas de cada índice y, se evaluará cada indicador. La suma de los dos indicadores estará evaluada sobre un 100%.

Para poder definir valores en función de porcentajes, es necesario tener valores referenciales para cada índice, es decir un valor que permita establecer una relación de los valores obtenidos con las herramientas de medición y sus respectivos porcentajes. Estos valores se los muestra en la Tabla IV-2 donde se tiene que el índice es mejor si es menor que el referencial (<), o también puede ser mejor si es mayor que el referencial es decir los que tienen el símbolo (>).

Tabla IV-II Resumen de indicadores en conjunto con sus valores de Referencia

Índice	Referencia	Mejor?
Jitter	50,00	mejor si <
Retardo	180,00	mejor si <
Pérdidas	10,00	mejor si <
Latencia	3000	mejor si <
Velocidad Tx	100	mejor si >

Como se recordara las relaciones expuestas en la Tabla IV-II, se trata de un resumen tomado de la sección Parámetros de Medición que ya fueron explicadas en el Capítulo III, valores extraídos específicamente de la **Tabla III-I Resumen de los Parámetros de Medición**.

4.2.1. Ponderación de los índices

Para poder llegar a nuestro objetivo que es la comparación del rendimiento de la tecnología Ethernet y Frame Relay es necesario establecer la prioridad que tiene cada parámetro esto se puede establecer de acuerdo a la severidad con que estos pueden afectar a la realización y el mantenimiento de una conexión de datos. En la Tabla IV-III, se presentan las prioridades, o pesos, distribuidas de acuerdo la importancia cada indicador:

Tabla IV-III Pesos asignados para cada índice

Índice	Peso [%]
Jitter	30
Pérdidas [%]	30
Retardo [ms]	20
Latencia [ms]	10
Velocidad Tx [kbps]	10
∑	100

Considerando la tendencia de las redes a ser convergentes en donde, sobresalen las aplicaciones de tiempo real y, siendo efectivamente el Jitter, el factor que produce perdidas de sincronía, y la pérdida de paquetes la que ocasiona errores en la reconstrucción de la información, se tiene a estos como los factores más críticos dentro de una red de comunicaciones[30], por ende estos índices reciben la más alta ponderación; 30 % cada uno de ellos.

Además, siendo MPLS considerada como una NGN las mismas que nacen a partir de las nuevas tecnologías de capa física[31], en donde la velocidad de transmisión puede equipararse con la velocidad de la luz, por lo que los inconvenientes del retardo y la latencia han de ser superados, siendo cada vez menos relevantes su importancia es menor. Por ello el retardo posee una ponderación del 20 % y la latencia un 10 %.

Lo anterior también da cuenta que el estudio de MPLS, o cualquier otro protocolo equivalente, se centra en la capacidad de gestión por parte del protocolo para optimizar el uso del medio de trasmisión y, es la capa física misma la que define la velocidad máxima.

[30] Digital communications test and measurement,
Dennis Derickson, Marcus Müller.
[31] Análisis basado en http://www.networkworld.es/actualidad/las-10-tendencias-clave-en-telecomunicaciones

Entonces el número de equipos que están involucrados en el sistema no influirán en mayor medida en velocidad, sino más bien en sincronización.

Las NGN están pensadas principalmente en brindar a sus usuarios el acceso a sus datos desde cualquier lugar con tan solo disponer de un dispositivo conectado a la red, cosa que es posible con el desarrollo de centros de datos en la nube o cloud cumputing.

La simultaneidad del acceso requiere altas tasas de transmisión. La velocidad de acceso por parte del usuario hacia la red, en este estudio, toma un valor de 10%. Este valor no desmerece a este índice, sino más bien, es debido a que se prioriza la calidad del tráfico de tiempo real.

La sumatoria de los dos indicadores da como resultado el 100% que deben alcanzar las tecnologías Ethernet y Frame Relay, para comprobar el rendimiento que estas ofrecen dentro del dominio MPLS con uno de los protocolos de señalización ya sea LDP o RSVP.

4.2.2. Analizando el Indicador 1

En este indicador, como se mencionó, se analizan los índices correspondientes a las comunicaciones de tiempo real; vale la pena recordar estos índices, los mismos que se exponen en la Tabla IV-IV.

Tabla IV-IV Índices para el indicador 1

Índice	Referencia
Jitter	50,00
Retardo	180,00
Pérdidas	10,00

A través de las mediciones realizadas en el capítulo 3 se expone un resumen de los valores de para los índices del indicador 1, los cuales se las muestra en la Tabla IV-V.

Tabla IV-V Media aritmética para los índices del indicador 1

Transmisión RT				
índice	**ETH + LDP**	**ETH + RSVP**	**FR + LDP**	**FR +RSVP**
Jitter [ms]	9,10	8,60	22,20	22,20
Retardo [ms]	0,00	1,80	0,60	0,60
Pérdidas [%]	0,00	0,00	10,20	7,40

Para una comprensiva visualización de los valores mostrados en la Tabla IV-V, se han transformado a estos valores a porcentajes, es decir se realizó un regla de tres teniendo como 100% a los valores de los índices establecidos en la Tabla IV-IV.

Al realizar esta pequeña operación se obtuvo como resultado los datos mostrados en la Tabla IV-VI, los cuales están evaluados sobre un 100%.

Tabla IV-VI Porcentajes correspondientes para cada índice del indicador 1

Transmisión RT				
Índice [%]	**ETH + LDP**	**ETH + RSVP**	**FR + LDP**	**FR + RSVP**
Jitter	18,20	17,20	44,40	44,40
Retardo	0,00	1,00	0,33	0,33
Pérdidas	0,00	0,00	102,00	74,00

Para estos índices, mientras mayores sean sus valores, la calidad de las comunicaciones empeorara. Entonces es necesario realizar una diferencia en relación al 100%, para de este modo tener valores que representen una buena calidad de la comunicación. Así se tiene:

Tabla IV-VII Diferencia en relación al 100% en función de su contribución

Transmisión RT				
Índice [%]	**ETH + LDP**	**ETH + RSVP**	**FR + LDP**	**FR + RSVP**
Jitter	81,80	82,80	55,60	55,60
Retardo	100,00	99,00	99,67	99,67
Pérdidas	100,00	100,00	0,00	26,00

En la Figura IV-1, se visualiza de mejor manera las variaciones que presentan los índices Jitter, retardo y pérdida de paquetes, frente a las diferentes combinaciones de tecnologías.

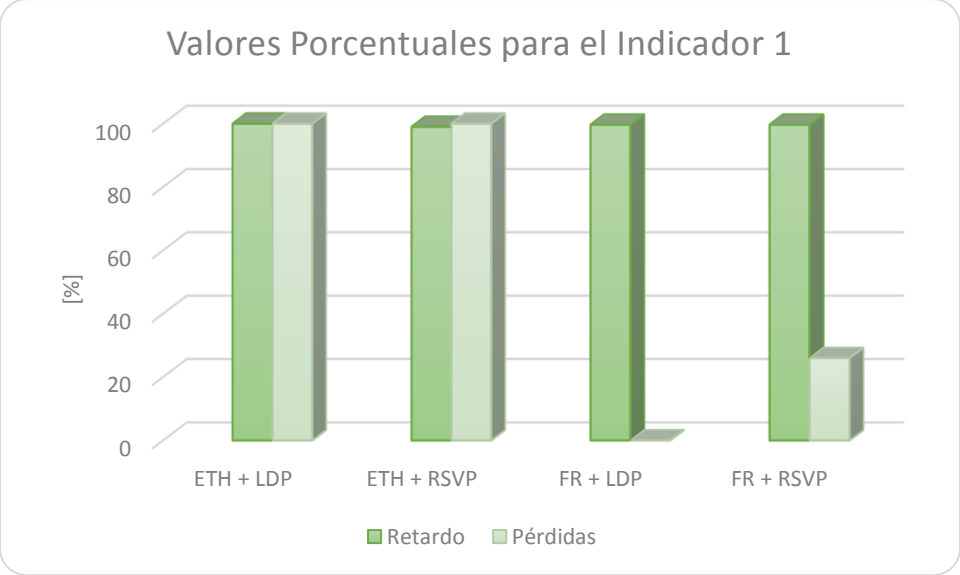


Figura IV-1 Representación de los índices del Indicador 1 para cada combinación de tecnologías

A continuación, se procede al desglose de los valores con los cuales se han elaborado las tabulaciones anteriores.

Estos valores provienen de la media aritmética de los valores medidos en el capítulo 3, específicamente en la sección de Obtención de Resultados, entonces para cada escenario se tiene:

4.2.2.1. Jitter

Todos los escenarios presentan el valor para este indicador muy por debajo de su umbral de tolerancia de 50 [ms], es decir el Jitter se encuentra en su valor óptimo y no incide en las comunicaciones de tiempo real.

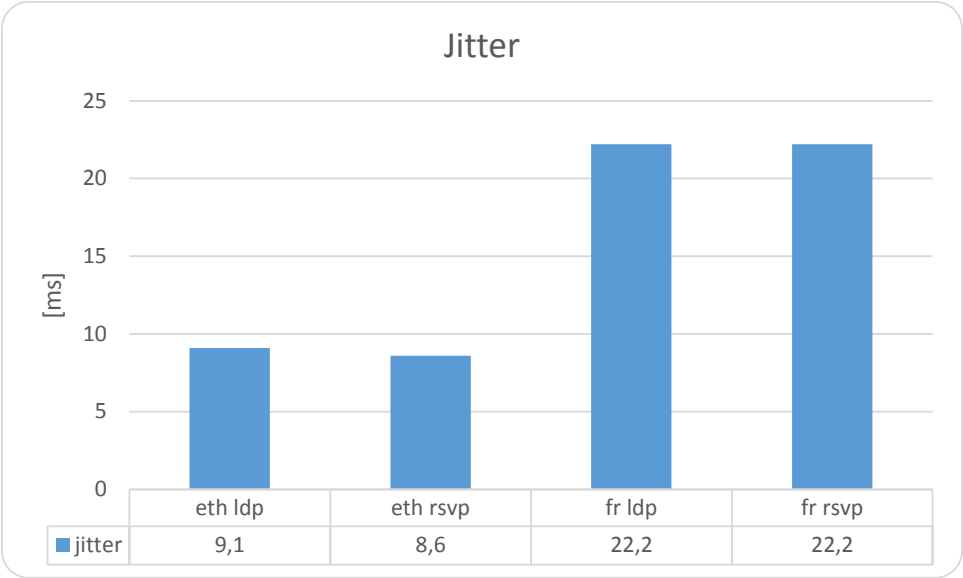


Figura IV-2 Representación del valor promedio para el Jitter

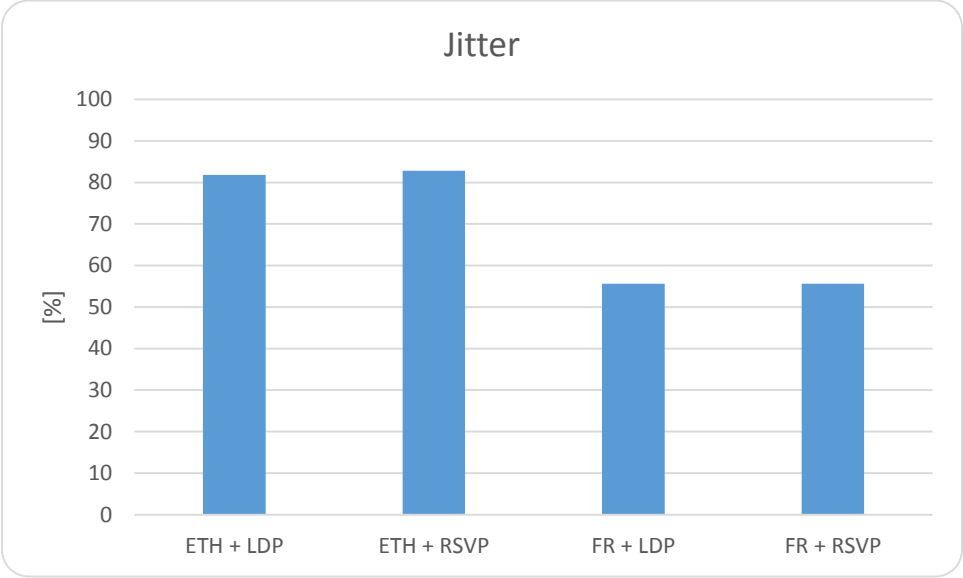


Figura IV-3 Representación del Jitter en valores porcentuales

Gráficamente, se puede observar que la tecnología FR presente los más altos valores correspondientes a este índice en relación a la tecnología ETH. Particularmente, si la señalización dentro del dominio MPLS está dado por el protocolo RSVP, el valor de este índice mejora levemente.

La tecnología ETH presenta una velocidad de trasmisión mucho más elevada, en consecuencia, los retardos de propagación han de ser muy bajos, solamente se considerarán los retardos generados en el hardware; entonces los retardos experimentados por los paquetes han de tender a ser uniformes, siendo esto equivalente a un bajo Jitter. La tecnología FR en cabio, al hacer uso de interfaces de tipo serie, las mismas que poseen una velocidad de transmisión reducida, podría verse saturado al intentar pasar un alto volumen de tráfico a pesar de la existencia de mecanismos para la gestión de congestión[32].

A pesar de que con FR se puede alcanzar un Jitter de 22 [ms], este valor está dentro del rango considerado como aceptable; si se quiere, se puede proyectar que si se elevase el volumen de tráfico el valor de este índice se elevara aún más, desbordándose del valor adecuado.

4.2.2.2. Pérdida de Paquetes

A continuación, una exposición correspondiente al nivel de pérdidas de paquetes para los cuatro escenarios de prueba y la respectiva interpretación de estos.

Nuevamente, la tecnología ETH ha dado los mejores niveles (0 %) en relación a la otra tecnología de análisis: FR. Parte de estos resultados se debe, nuevamente a la mayor velocidad de transmisión por parte de la tecnología FR por lo cual la probabilidad de que los paquetes se pierdan por colisiones, interferencias, o cualquier otro factor, es mínimo.

[32] Existen tres mecanismos de gestión de congestión en Frame Relay: BECN, FECN, DE. Estos mecanismos se limitan a le eliminación de paquetes para combatir la congestión, lo cual, obviamente, no es la mejor solución.

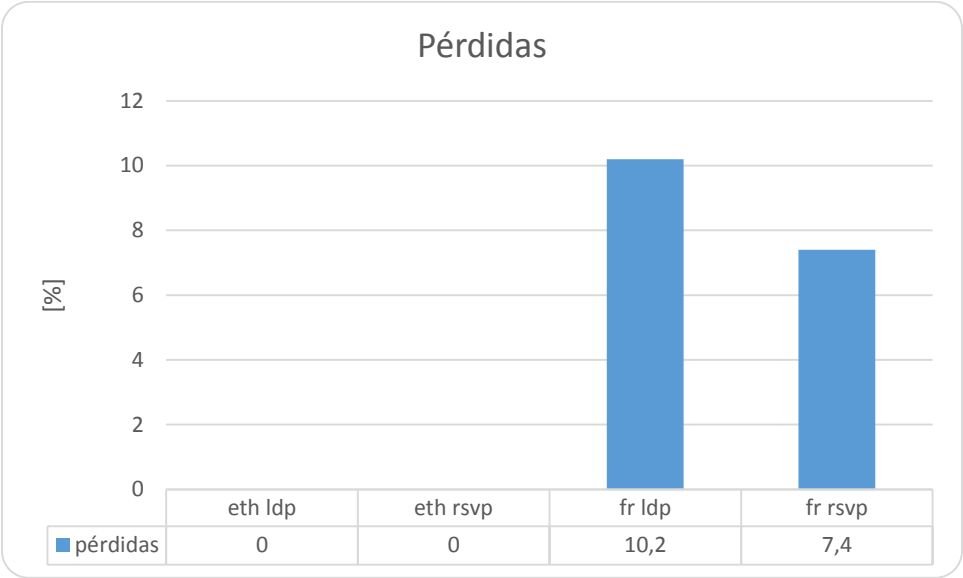


Figura IV-4 Representación de la pérdida de paquetes

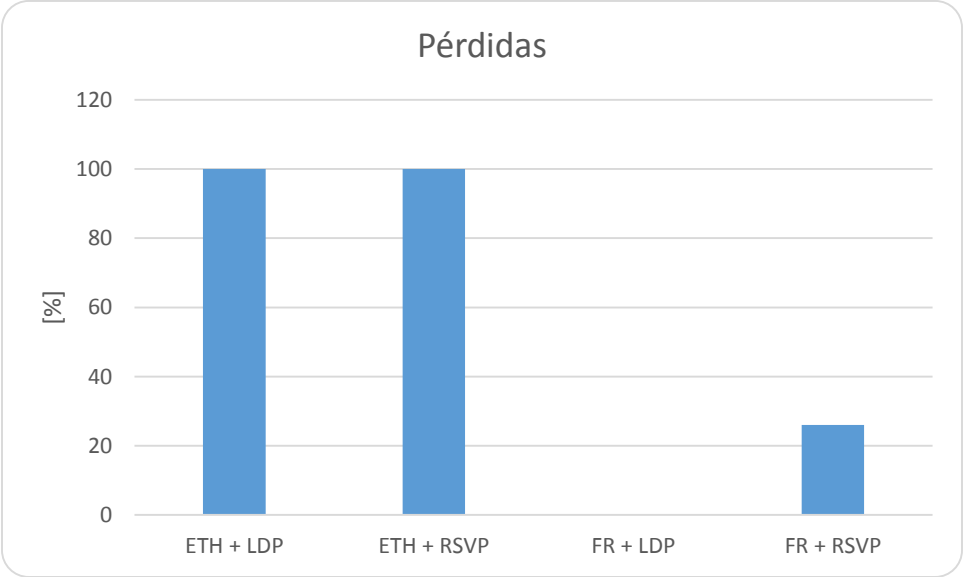


Figura IV-5 Representación de Pérdida de paquetes en valores porcentuales

Por supuesto, como se mencionó anteriormente, la eliminación de paquetes como técnica de descongestión, como lo hace Frame Relay, no es la mejor solución para combatir el problema de la congestión, más aun si se trata de comunicaciones interactivas de tiempo real. ETH por su parte, deja la gestión de los errores graves a las capas superiores; generalmente al hacerse uso de IP se

procede a las retransmisiones en caso de ser necesario. En definitiva, al tener un gran ancho de banda, se tiene menor probabilidad de pérdidas de paquetes.

Para este índice, también los valores para ambas tecnologías están dentro del nivel aceptable.

4.2.2.3. Retardo

Para este indicador se han registrado retardos mínimos en todas las combinaciones de tecnologías. Es necesario recordar que estos valores son registrados en la tarjeta local de red. Consecuentemente, estos valores bajos podrían ser omitidos; pero si eleva el volumen de tráfico, estos valores podrán tornarse significativos.

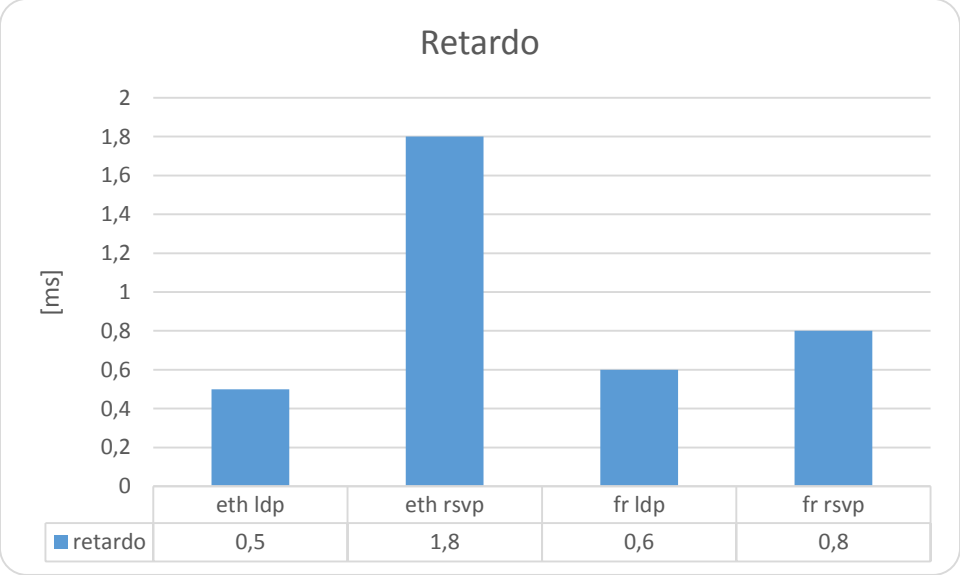


Figura IV-6. Representación del promedio del Retardo

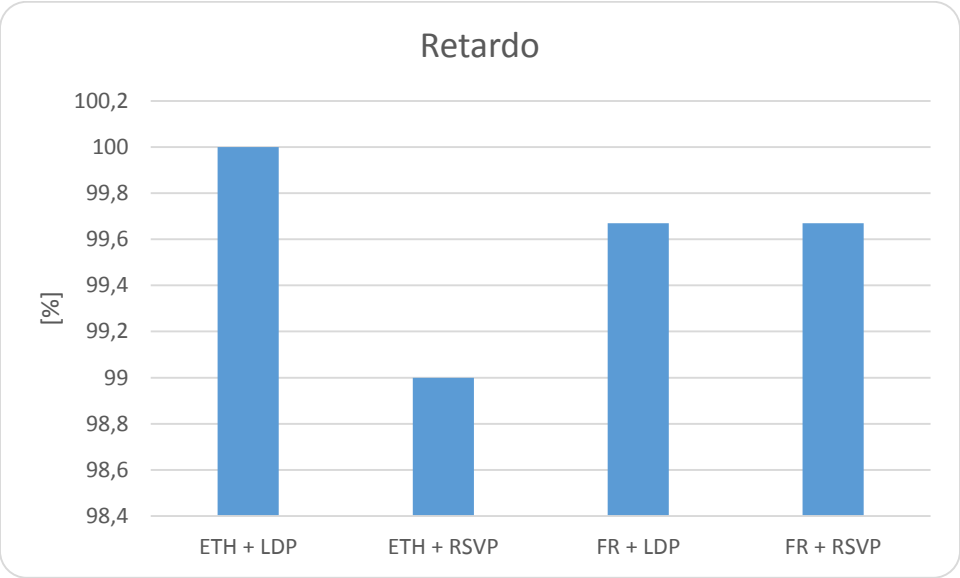


Figura IV-7 Representación del Retardo en valores porcentuales

La ligera superioridad en el nivel del retardo para ETH puede ser una consecuencia de que esta tecnología utiliza tramas de 1500 Bytes, ocasionando así, un mayor nivel de carga en el buffer de los equipos; a pesar de que este índice también está dentro de los valores recomendados para las tecnologías analizadas. Sin embargo el elevado ancho de banda de logra superar este inconveniente; esto se demuestra al observar una diferencia máxima de 1 [ms], por lo que se puede considerar como despreciable, sin embargo, todos los valores serán considerados en este estudio.

4.2.2.4. Resumen para el indicador 1

Considerando los pesos asignados en la Tabla IV-III, se puede observar que el indicador 1 aporta con el 80% del resultado final. Entonces como se puede apreciar en la Tabla IV-VIII, se tiene los valores del indicador de transmisión en tiempo real para todas las combinaciones de tecnologías.

Tabla IV-VIII Resumen de mediciones

Transmisión RT				
Índice [%]	**ETH + LDP**	**ETH + RSVP**	**FR + LDP**	**FR + RSVP**
Jitter	24,54	24,84	16,68	16,68
Retardo	20,00	19,80	19,93	19,93
Pérdidas	30,00	30,00	0,00	7,80
∑ sobre 80%	74,54	74,64	36,61	44,41

En la Figura IV-8, se muestra el valor de cada índice que pertenece a las transmisiones de tiempo real, el cual es un indicador que aporta con el 80%, al valor final del rendimiento de las tecnologías de acceso FR y ETH; donde la barra amarilla representa la suma total de los índices jitter, retardo y pérdida de paquetes.

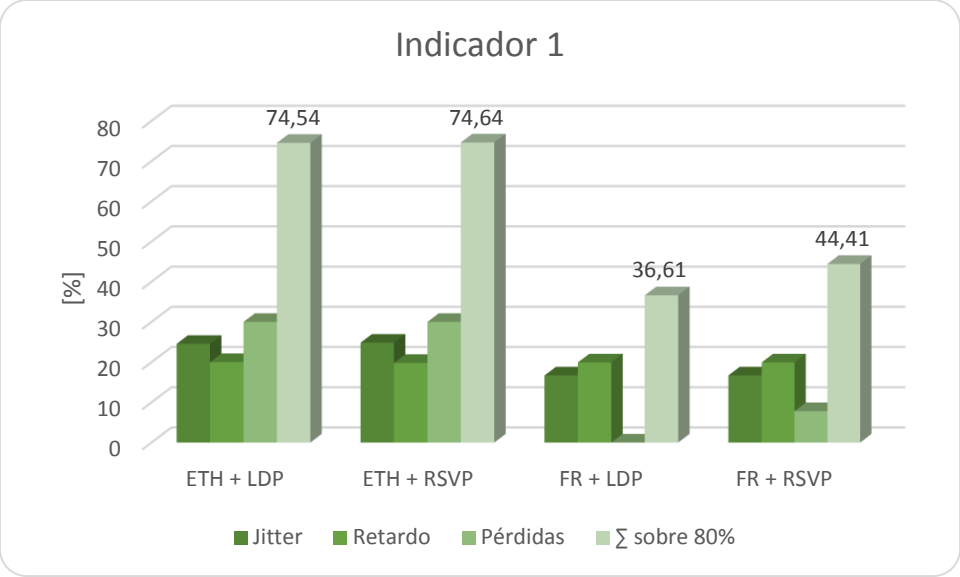


Figura IV-8 Presentación gráfica de los índices del indicador 1 evaluados sobre el 80%

Hasta aquí, se ha podido comprobar que la tecnología Ethernet posee mejores cualidades en función del análisis que se está analizando en este estudio.

4.2.3. Analizando el Indicador 2

Es necesario recordar los índices para este indicador, el cual está relacionado con el tráfico de datos, o sea, tráfico en tiempo no real.

Tabla IV-IX Índices para el indicador 2

Índice	Referencia
Latencia	3000
Velocidad Tx	100

Siguiendo el mismo procedimiento que para el indicador 1, se toma los valores obtenidos de las mediciones hechas en el Capítulo III, los mismos que son valores promedios de las pruebas realizadas con cada una de las tecnologías de acceso.

Tabla IV-X Media aritmética para los índices del indicador 2

Transmisión NRT				
Índice	**ETH + LDP**	**ETH + RSVP**	**FR + LDP**	**FR + RSVP**
Latencia [ms]	2526	110,9	1853,9	2126,6
Velocidad Tx [kbps]	7,1	15,13	10,59	7,97

Al igual que en el indicador 1, se procede a transformar los valores promedios de las mediciones de la Tabla IV-X en valores porcentuales, teniendo como referencia del 100% a los datos establecidos en la Tabla IV-IX.

Después de la transformación hecha a los datos de la Tabla IV-X, se obtienen los valores para el indicador 1, los mismos que están evaluados sobre el 100%, como se puede ver en la Tabla IV-XI.

Tabla IV-XI Porcentajes correspondientes para cada índice del indicador 1

Transmisión NRT				
Índice [%]	**eth ldp**	**eth rsvp**	**fr ldp**	**fr rsvp**
Latencia	84,20	3,70	61,80	70,89
Velocidad	7,10	15,13	10,59	7,97

Para este indicador, mientras mayor sea su valor, la calidad de las comunicaciones mejora y por tal motivo no es necesario realizar una operación de diferencia con respecto al 100%, como se lo realizo apara el caso del indicador 1.

En la Figura IV-9, se puede observar las variaciones de la latencia y velocidad de transmisión tanto para ETH y FR con sus respectivos protocolos de señalización, donde se ve claramente que ETH presenta un cierto nivel de superioridad en relación a las demás combinaciones de tecnologías.

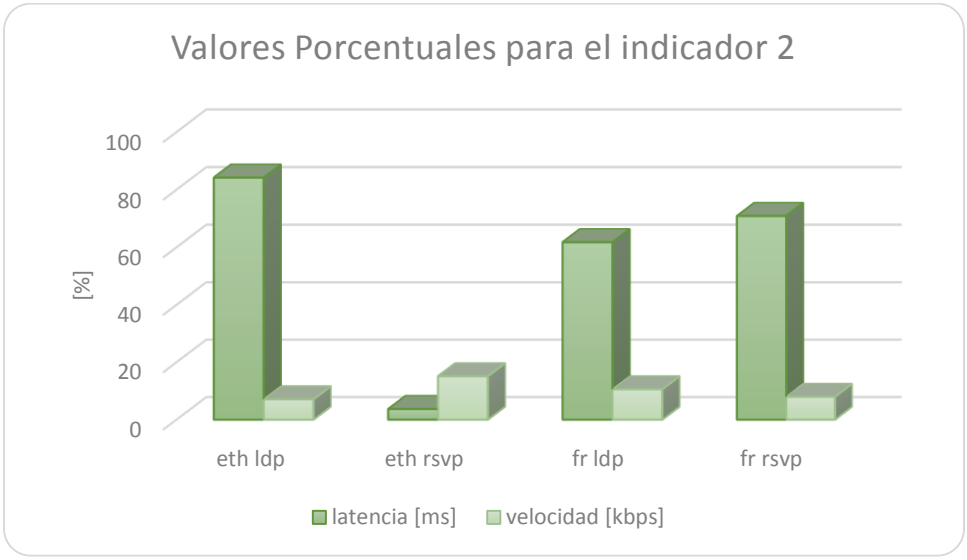


Figura IV-9 Representación de los índices del Indicador 1 para cada combinación de tecnologías

A continuación, se expone el análisis de los índices correspondientes a este indicador relacionado con el tráfico de datos.

4.2.3.1. Latencia

En un escenario congestionado el nivel de latencia supone un ligero incremento debido a la saturación que se producen en los enlaces que conforman la red.

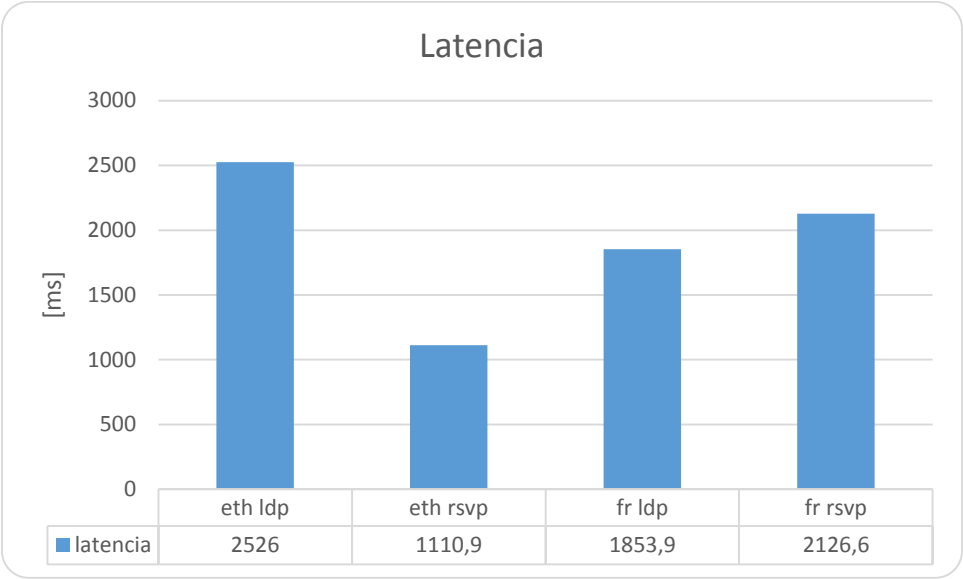


Figura IV-10. Representación de promedio de Latencia

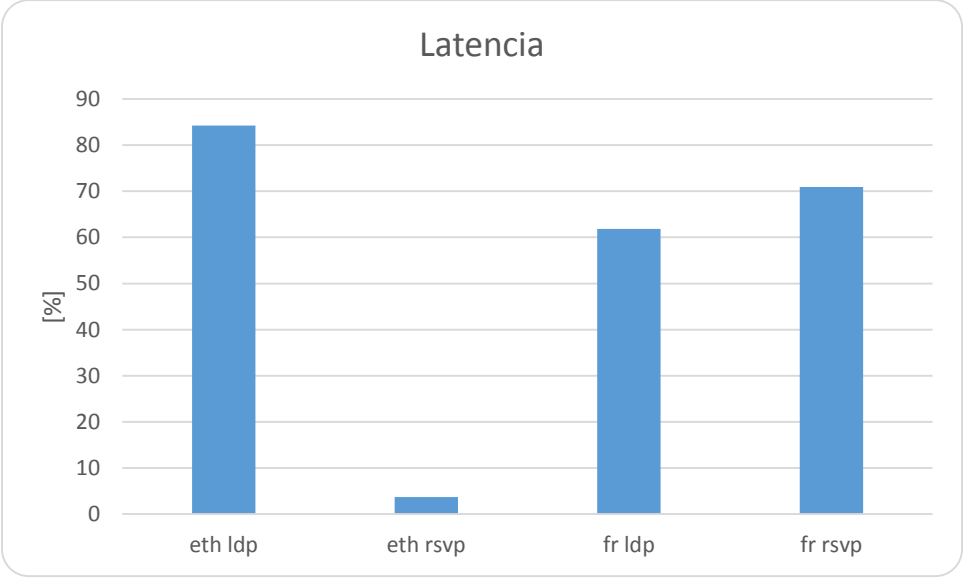


Figura IV-11 Representación de la Latencia en función

Para este índice se puede concluir que la el protocolo RSVP gestiona mejor el trafico dentro del dominio MPLS cuando se cruza trafico Ethernet a través del mismo; LDP no sería el adecuado. FR, con el tráfico usado en este análisis, también ha dado buenos resultados pero, está ya llegando al borde de sus capacidades a diferencia de ETH, el cual tiene mucho más por ofrecer y es la tecnología con mayor desarrollo tecnológico.

4.2.3.2. Velocidad de Transmisión

La velocidad de transmisión tiene función directa con el ancho de banda, este índice se inclina bastante hacia ETH, y es lógico que así sea. Esta tecnología en los últimos años ha sido desarrollada enormemente, y conforma casi todas las LAN´s en el mundo entero gracias a su alto desempeño, su gran capacidad de transmisión, pero sobre todo, por su sencillez de configuración e instalación.

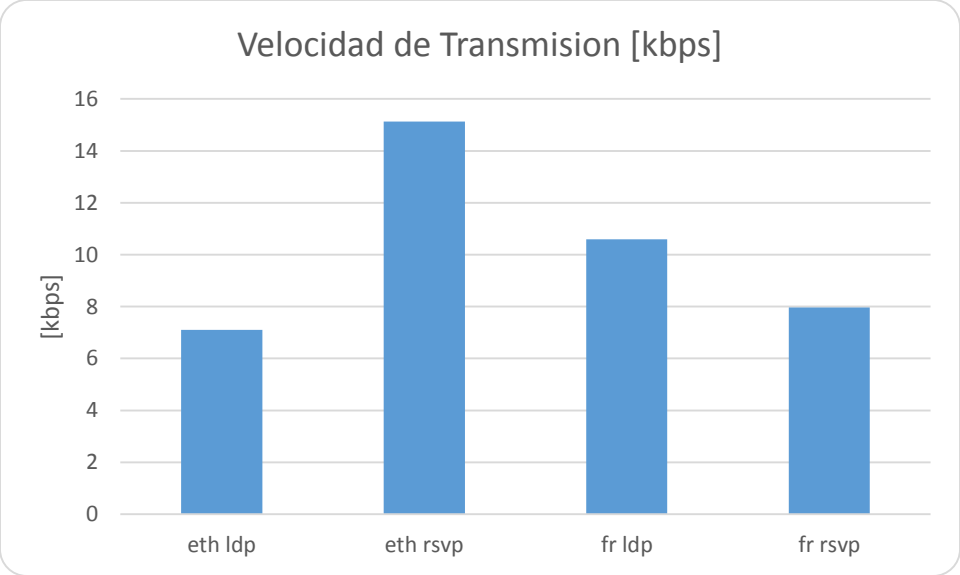


Figura IV-12. Representación del promedio la velocidad de Transmisión

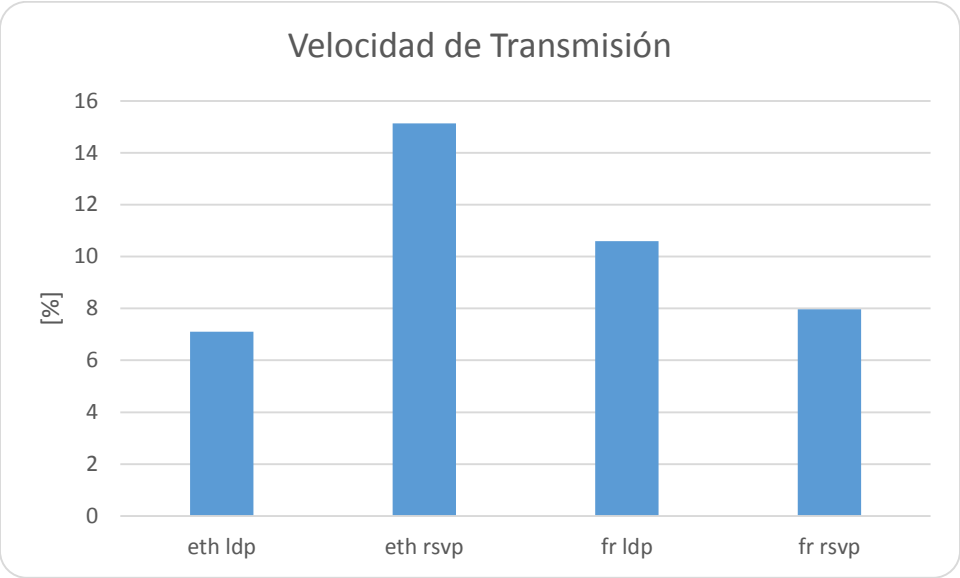


Figura IV-13 Representación de la velocidad de transmisión en valores porcentuales

Así, la tecnología ETH junto con RSVP como protocolo de señalización dentro del dominio MPLS, brindará el mejor desempeño. Se debe considerar que en el desarrollo y ejecución de los escenarios de prueba la velocidad de neta de transmisión no podrá pasar de 10 Mbps y, en la actualidad podemos hablar de 10 Gbps o, al menos de 100 Mbps para ETH. Al hacer uso de estos enlaces y el hardware respectivo que los soporte, entonces la ventaja de ETH sobre MPLS se incrementará exponencialmente.

4.2.3.3. Resumen para el Indicador 2

Considerando los pesos asignados en la Tabla IV-III, de la sección **Ponderación de Índices**, se puede observar que el indicador 2 aporta con el 20 % del resultado final.

Entonces al relacionar estos los índices del indicador 2 (Latencia y velocidad de transmisión) con sus respectivos pesos se puede ver en la Tabla IV-XII, los resultados obtenidos para cada combinación de tecnología sobre el 20%.

Tabla IV-XII. Resumen para el indicador 2

Transmisión NRT				
Índice	**ETH + LDP**	**ETH + RSVP**	**FR + LDP**	**FR + RSVP**
Latencia [ms]	1,58	9,63	3,82	2,91
Velocidad Tx [kbps]	0,71	1,51	1,06	0,80
∑ sobre 20%	2,29	11,14	4,88	3,71

Al analizar la Figura IV-14, claramente se nota que ETH + RSVP presenta cierta superioridad frente a las demás combinaciones ya que representa el 11.14 % de un 20%.

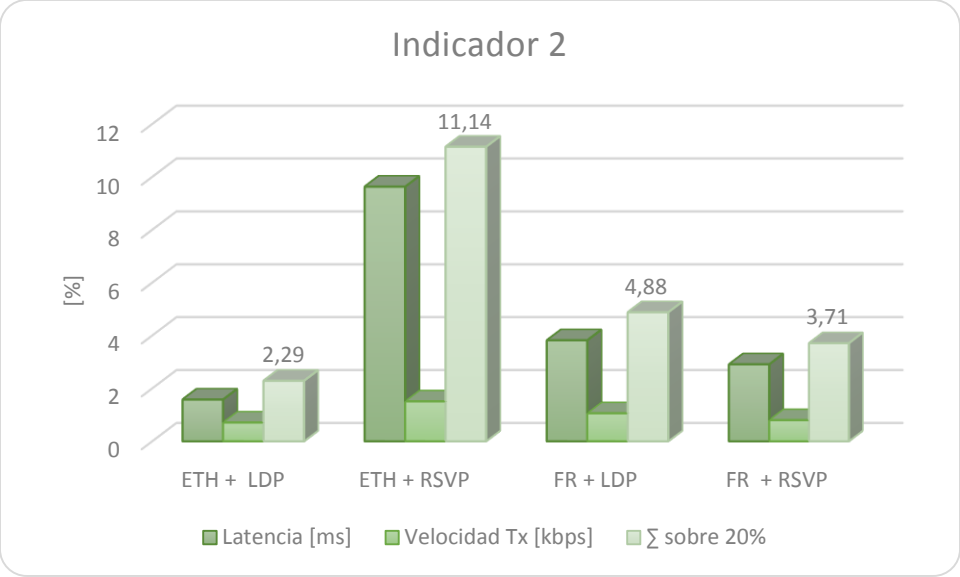


Figura IV-14 Presentación gráfica de los índices del indicador 1 evaluados sobre el 20%

4.3. Resultado Final de Indicadores

En la Tabla IV-XIII, se exponen los resultados finales para cada indicador, como también los totales sobre el 100%, donde el máximo valor representa la tecnología que tiene mejor rendimiento frente a las otras. Siendo en este caso ETH con señalización RSVP, al tener el 85.78 %, desplazando a Frame Relay con casi un 38%.

Tabla IV-XIII. Evaluación final de indicadores

	ETH + LDP	ETH + RSVP	FR + LDP	FR + RSVP
Indicador 1	74,54	74,64	36,61	44,41
Indicador 2	2,29	11,14	4,87	3,71
∑ Total	76,83	85,78	41,49	48,12

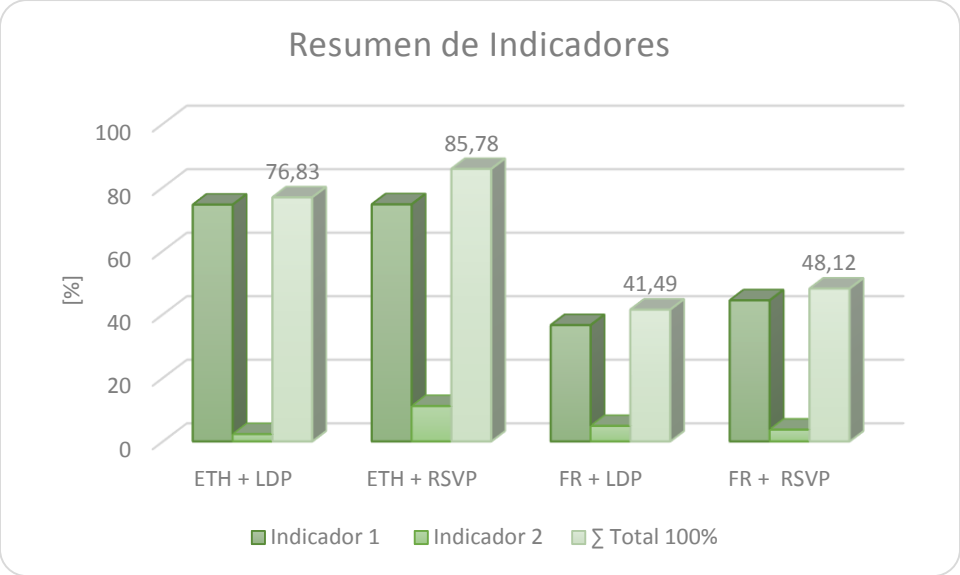


Figura IV-15 Representación final de cada uno de los indicadores de la Tabla IV-XIII

4.3.1. Interpretación final del Análisis

Aunque en todos los escenarios probados mantienen los indicadores de calidad dentro de los valores permitidos para que se pueda dar una óptima comunicación, existe una en particular que sobresale por su efectiva gestión del ancho banda, el cual es un recurso limitado e indispensable en todas las redes de datos. Así, se hace referencia a las tecnologías ETH para, a través de un análisis teórico establecer las razones de sus ventajas.

Antes que nada, es notable que la tecnología ETH presenta altas prestaciones en cuanto a la velocidad de transmisión y su delegación de la corrección de graves errores a las capas superiores; estos contribuye a que el ancho de banda disponible en el enlace de comunicación sea aprovechado

al máximo, minimizando la pérdidas de paquetes retardos de propagación y por ende una latencia menos, una mayor capacidad de transmisión.

A esto se le deberá añadir la ventaja de que en el dominio MPLS, mediante el uso de RSVP se ha logrado estables un LSP único lo cual agiliza, más de lo que comúnmente lo hace MPLS, el proceso de decisión por parte los conmutadores involucrados en dicho dominio.

Así, ETH y RSVP, a través del análisis realizado, son las tecnologías que mejor se adaptan a un entorno en el que las comunicaciones de tiempo real necesitan fluir bajo óptimas condiciones.

4.4. Comprobación de hipótesis

La hipótesis planteada es:

Hi: Las redes Ethernet sobre una arquitectura MPLS proporcionará un mejor rendimiento que una red Frame Relay bajo similares condiciones de prueba.

La hipótesis descrita anteriormente es de tipo descriptiva, este tipo de hipótesis solamente tiene una variable que en este caso es el **rendimiento,** donde se está asegurando que Ethernet proporciona mejor rendimiento dentro de una arquitectura MPLS. Para la comprobación de una hipótesis descriptiva se hace uso de la Estadística Descriptiva, la misma que es un conjunto de procedimientos que tienen por objeto presentar masas de datos por medio de tablas, gráficos y/o medidas de resumen[33].

Así dentro de la estadística descriptiva se hace uso del promedio y de la diferencia de porcentajes. Se aplicó el promedio a las mediciones realizadas a los índices jitter, retardo, pérdida de paquetes,

[33] Estadística Descriptiva
Santiago Fernández, José María Cordero Sánchez, Alejandro Largo Córdoba, José María Cordero, Alejandro Córdoba Largo. ESIC Editorial, 2002.

latencia y velocidad de transmisión, estos valores se los presenta en la Tabla III-XXVII, posteriormente se procede a transformar estos datos a valores porcentuales con el fin de determinar la tecnología que presente el mejor rendimiento dentro de una arquitectura MPLS.

De acuerdo con esto en la Tabla IV-XIV, se presenta los resultados finales del rendimiento de las tecnologías Ethernet y Frame Relay sobre una arquitectura MPLS, con cada uno de los protocolos de señalización involucrados en este estudio.

Tabla IV-XIV Resultado final de la medición del rendimeinto de Tecnologías

	LDP		RSVP	
Índice	**ETHERNET**	**FRAME RELAY**	**ETHERNET**	**FRAME RELAY**
Jitter	24,54	16,68	24,84	16,68
Retardo	20	19,93	19,8	19,93
Pérdidas	30	0	30	7,8
Latencia	1,58	3,82	9,63	2,91
Velocidad	0,71	1,06	1,51	0,8
Rendimiento	**76,83**	**41,49**	**85,78**	**48,12**

En la Figura IV-16, se puede ver claramente que con el uso del protocolo de señalización LDP, Ethernet presenta un rendimiento del 76.83 % frente a Frame Relay que tiene un 41.49 %, superándolo de esta manera en aproximadamente un 35%.

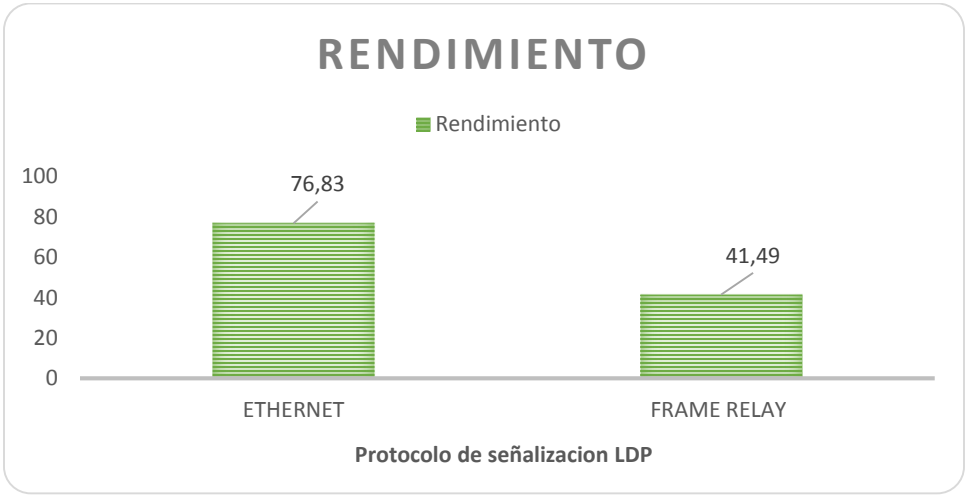


Figura IV-16 Rendimiento de ETH vs FR con señalización LDP

Mientras que para el protocolo de señalización RSVP, en la Figura IV-17, observamos que Ethernet presenta un rendimiento del 85,78%, frente a Frame Relay que tan solo tiene 48,12%, superándolo así por aproximadamente un 38%. Valor que es ligeramente superior al que se tiene con el protocolo LDP.

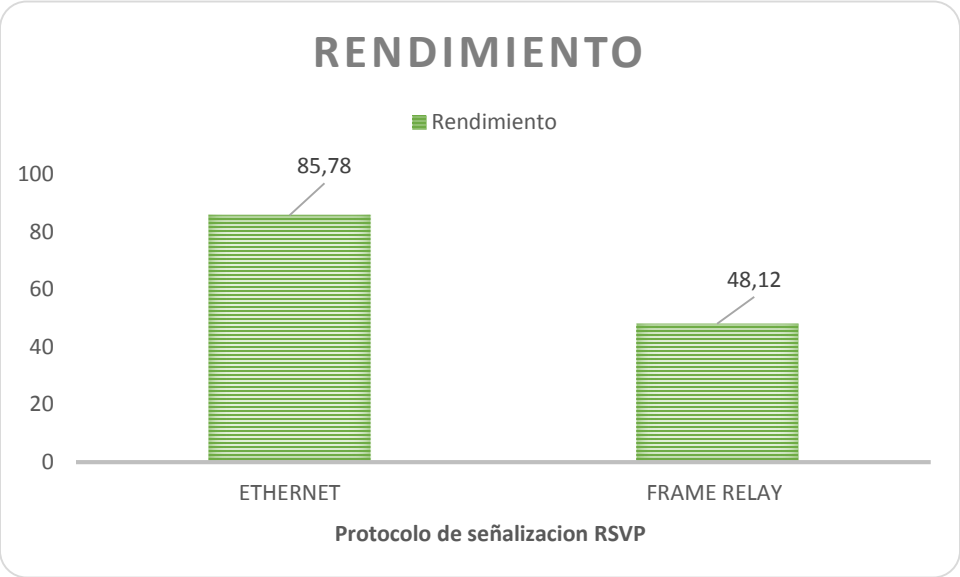


Figura IV-17 Rendimiento de ETH vs FR con señalización RSVP

Conclusión: Considerando el análisis ya descrito, se ha llegado a una evaluación final, donde el uso del protocolo de señalización RSVP presenta valores superiores con relación a LDP por lo que se concluye que Ethernet es la tecnología que proporciona un mejor rendimiento sobre una arquitectura MPLS, con un 85.78%, superando a Frame Relay en aproximadamente un 38% de su rendimiento. Valores que han sido determinados después del análisis minucioso de cada indicador involucrado dentro de esta investigación. Por lo tanto la Hi planteada es verdadera.

4.9. Guía técnica de implementación

Después del análisis realizado y teniendo a FR con RSVP como las tecnologías más aptas que ofrecen el mejor rendimiento, se procede a resumir lo necesario para la implementación del escenario que se muestra Figura IV-18, el mismo que trata de emular un núcleo MPLS y sus clientes que se comunicaran a través del mismo.

4.9.1. Escenario

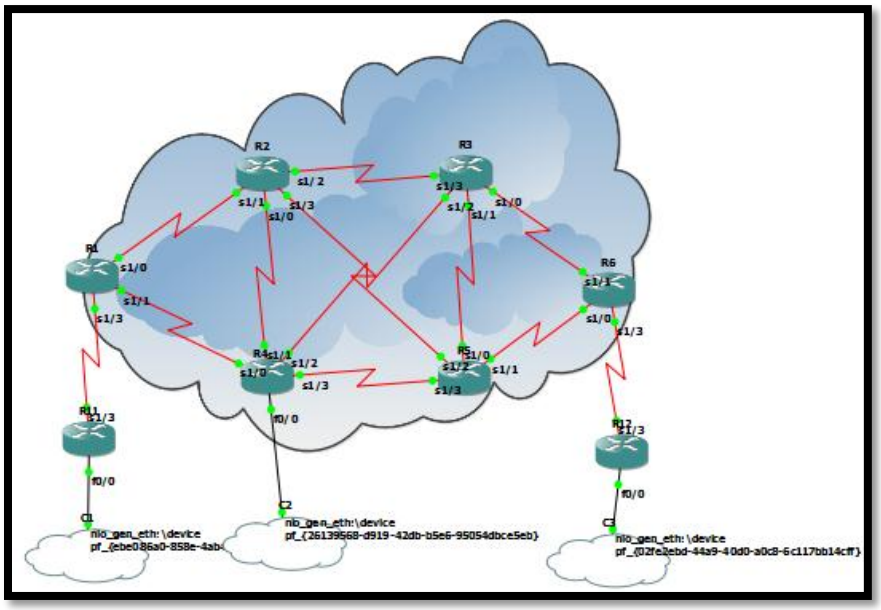


Figura IV-18 Escenario realizado en GNS3

Es necesario aclarar que el terminal identificado con la dirección IP 192.168.100.2 ha sido implementado de tal forma que el enlace hacia su enrutador de acceso sea de 10 Mbps de tecnología Ethernet. El otro terminal, identificado con la dirección IP 192.168.200.3, tiene una conexión hasta su enrutador de acceso de 100 Mbps de tecnología Ethernet.

En cada terminal se ha instalado la aplicación Cisco IP Communicator el cual emula a un teléfono IP y que servirá para generar el tráfico de tiempo real. El tráfico convencional de datos se lo realiza a través la transferencia de archivos desde y hacia las carpetas compartidas de las de las terminales.

Este escenario fue realizado en la plataforma de GNS3 versión 0.8.3.1, en el cual se han utilizado:

Tabla IV-XV Descripción de los dispositivos utilizados

Dispositivo	Cantidad	IOS	Porque?
Router Cisco c7200	6	c7200-adventerprisek9-mz.124-24.T6	Este enrutador, junto con su respectivo IOS, es el único que en GNS3 puede soportar el transporte multiprotocolo.
Router Cisco c3660	2	c3660-ik9o3s-mz.122-40	Es un enrutador de gama media, que en GNS3, con el IOS indicado, actúa también como CME. Características propias de un enrutador de acceso.
Cloud	3	--------	Necesarias para poder interconectar el escenario simulado en GNS3 a una infraestructura física.

En resumen: los enrutadores c7200 conformaran el dominio MPLS, mientras que los enrutadores c3660 conforman las redes LAN anexas. Las nubes de GNS3 permitirán la interconexión del escenario virtual con el mundo real.

4.9.2. Direccionamiento

En la Tabla IV-XVI, se especifican las funciones de cada enrutador además del direccionamiento IP utilizado para sus interfaces.

Tabla IV-XVI Direccionamiento IP

DISPOSITIVO	FUNCIÓN	INTERFACE	DIRECCIÓN	MASCARA
R1	LER	Loopback	192.168.1.201	255.255.255.255
		S1/0	192.168.1.21	255.255.255.252
		S1/1	192.168.1.21	255.255.255.252
		S1/3	no set	no set
R2	LSR	Loopback	192.168.1.202	255.255.255.255
		S1/0	192.168.1.33	255.255.255.252
		S1/1	192.168.1.2	255.255.255.252
		S1/2	192.168.1.5	255.255.255.252
		S1/3	192.168.1.25	255.255.255.252
R3	LSR	Loopback	192.168.1.203	255.255.255.255
		S1/0	192.168.1.9	255.255.255.252
		S1/1	192.168.1.37	255.255.255.252
		S1/2	192.168.1.30	255.255.255.252
		S1/3	192.168.1.6	255.255.255.252
R4	LSR	Loopback	192.168.1.204	255.255.255.255
		S1/0	192.168.1.22	255.255.255.252
		S1/1	192.168.1.34	255.255.255.252
		S1/2	192.168.1.29	255.255.255.252
		S1/3	192.168.1.17	255.255.255.252
R5	LSR	Loopback	192.168.1.205	255.255.255.255
		S1/0	192.168.1.38	255.255.255.252
		S1/1	192.168.1.13	255.255.255.252
		S1/2	192.168.1.26	255.255.255.252
		S1/3	192.168.1.18	255.255.255.252
R6	LER	Loopback	192.168.1.206	255.255.255.255
		S1/0	192.168.1.14	255.255.255.252
		S1/1	192.168.1.10	255.255.255.252
		S1/3	no set	no set
R11	CE	FastEth0/0	192.168.100.1	255.255.255.0
		S1/3.1	192.168.2.1	255.255.255.0
R12	CE	FastEth0/0	192.168.137.1	255.255.255.0
		S1/3.1	192.168.2.2	255.255.255.0

4.9.3. Configuración

4.9.3.1. R1

Este es un LER que permite en ingreso y la salida del tráfico FR en el dominio MPLS a través de la tecnología AToM. La configuración que se ha realizado en este dispositivo es la siguiente:

```
!
ip cef
!
multilink bundle-name authenticated
FR switching
mpls traffic-eng tunnels
mpls ldp loop-detection
!
interface Loopback0
 ip address 192.168.1.201 255.255.255.255
 ip flow ingress
!
interface Tunnel0
 ip unnumbered Loopback0
 ip flow ingress
 tunnel destination 192.168.1.206
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 2 2
 tunnel mpls traffic-eng bandwidth 100
 tunnel mpls traffic-eng path-option 1 explicit name ruta1
 no routing dynamic
!
interface Serial1/0
 description intMPLS
 ip address 192.168.1.1 255.255.255.252
 ip flow ingress
 mpls traffic-eng tunnels
 mpls ip
 serial restart-delay 0
 clock rate 252000
 ip rsvp bandwidth 256 256
!
interface Serial1/1
 description intMPLS
 ip address 192.168.1.21 255.255.255.252
 ip flow ingress
```

```
 mpls ip
 serial restart-delay 0
 clock rate 252000
!
interface Serial1/3
 no ip address
 ip flow ingress
 encapsulation FR IETF
 serial restart-delay 0
 dce-terminal-timing-enable
 FR intf-type dce
!
router ospf 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 log-adjacency-changes
 network 192.168.1.0 0.0.0.3 area 0
 network 192.168.1.20 0.0.0.3 area 0
 network 192.168.1.40 0.0.0.3 area 0
 network 192.168.1.201 0.0.0.0 area 0
!
router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.1.42 remote-as 65000
 neighbor 192.168.1.202 remote-as 65000
 neighbor 192.168.1.202 update-source Loopback0
 neighbor 192.168.1.203 remote-as 65000
 neighbor 192.168.1.203 update-source Loopback0
 neighbor 192.168.1.204 remote-as 65000
 neighbor 192.168.1.204 update-source Loopback0
 neighbor 192.168.1.205 remote-as 65000
 neighbor 192.168.1.205 update-source Loopback0
 neighbor 192.168.1.206 remote-as 65000
 neighbor 192.168.1.206 update-source Loopback0
 no auto-summary
!
ip flow-cache mpls label-positions mpls-length
ip flow-export version 5
ip flow-export destination 192.168.1.42 9996
!
!
ip explicit-path name ruta1 enable
 next-address 192.168.1.2
 next-address 192.168.1.26
 next-address 192.168.1.14
!
connect tunel Serial1/3 102 l2transport
```

```
 xconnect 192.168.1.206 20 encapsulation mpls
 !
mpls ldp router-id Loopback0 force
```

4.9.3.2. R2

Este es LSR que conmuta el tráfico de capa dos encapsulado en función del protocolo RSVP.

```
!
ip cef
!
mpls traffic-eng tunnels
!
interface Loopback0
 description Loop202
 ip address 192.168.1.202 255.255.255.255
!
interface Serial1/0
 description intMPLS
 ip address 192.168.1.33 255.255.255.252
 mpls ip
 serial restart-delay 0
 clock rate 252000
 no dce-terminal-timing-enable
!
interface Serial1/1
 description intMPLS
 ip address 192.168.1.2 255.255.255.252
 mpls ip
 mpls traffic-eng tunnels
 serial restart-delay 0
 no dce-terminal-timing-enable
 ip rsvp bandwidth 256 256
!
interface Serial1/2
 description intMPLSclk
 ip address 192.168.1.5 255.255.255.252
 mpls ip
 serial restart-delay 0
 clock rate 252000
 no dce-terminal-timing-enable
!
interface Serial1/3
 description intMPLSclk
 ip address 192.168.1.25 255.255.255.252
```

```
 mpls ip
 mpls traffic-eng tunnels
 serial restart-delay 0
 clock rate 252000
 no dce-terminal-timing-enable
 ip rsvp bandwidth 256 256
!
router ospf 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 log-adjacency-changes
 network 192.168.1.0 0.0.0.3 area 0
 network 192.168.1.4 0.0.0.3 area 0
 network 192.168.1.24 0.0.0.3 area 0
 network 192.168.1.32 0.0.0.3 area 0
 network 192.168.1.202 0.0.0.0 area 0
!
router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.1.41 remote-as 65000
 neighbor 192.168.1.41 update-source Loopback0
 neighbor 192.168.1.42 remote-as 65000
 neighbor 192.168.1.42 update-source Loopback0
 neighbor 192.168.1.201 remote-as 65000
 neighbor 192.168.1.201 update-source Loopback0
 neighbor 192.168.1.203 remote-as 65000
 neighbor 192.168.1.203 update-source Loopback0
 neighbor 192.168.1.204 remote-as 65000
 neighbor 192.168.1.204 update-source Loopback0
 neighbor 192.168.1.205 remote-as 65000
 neighbor 192.168.1.205 update-source Loopback0
 neighbor 192.168.1.206 remote-as 65000
 neighbor 192.168.1.206 update-source Loopback0
 no auto-summary
!
```

4.9.3.3. R3

Este es un LER que conmuta los paquetes del tráfico de capa 2 encapsulado en función RSVP.

```
ip cef
!
multilink bundle-name authenticated
!
```

```
interface Loopback0
 description Loop203
 ip address 192.168.1.203 255.255.255.255
 ip flow ingress
!
interface Serial1/0
 description intMPLSclk
 ip address 192.168.1.9 255.255.255.252
 ip flow ingress
 mpls ip
 serial restart-delay 0
 clock rate 252000
!
interface Serial1/1
 description intMPLS clk
 ip address 192.168.1.37 255.255.255.252
 ip flow ingress
 mpls ip
 serial restart-delay 0
 clock rate 252000
!
interface Serial1/2
 description intMPLS
 ip address 192.168.1.30 255.255.255.252
 ip flow ingress
 mpls ip
 serial restart-delay 0
!
interface Serial1/3
 description intMPLS
 ip address 192.168.1.6 255.255.255.252
 ip flow ingress
 mpls ip
 serial restart-delay 0
!
router ospf 100
 log-adjacency-changes
 network 192.168.1.4 0.0.0.3 area 0
 network 192.168.1.8 0.0.0.3 area 0
 network 192.168.1.28 0.0.0.3 area 0
 network 192.168.1.36 0.0.0.3 area 0
 network 192.168.1.203 0.0.0.0 area 0
!
router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.1.41 remote-as 65000
 neighbor 192.168.1.41 update-source Loopback0
```

```
 neighbor 192.168.1.42 remote-as 65000
 neighbor 192.168.1.42 update-source Loopback0
 neighbor 192.168.1.201 remote-as 65000
 neighbor 192.168.1.201 update-source Loopback0
 neighbor 192.168.1.202 remote-as 65000
 neighbor 192.168.1.202 update-source Loopback0
 neighbor 192.168.1.204 remote-as 65000
 neighbor 192.168.1.204 update-source Loopback0
 neighbor 192.168.1.205 remote-as 65000
 neighbor 192.168.1.205 update-source Loopback0
 neighbor 192.168.1.206 remote-as 65000
 neighbor 192.168.1.206 update-source Loopback0
 no auto-summary
!
ip flow-export version 5
ip flow-export destination 192.168.1.42 9996
!
control-plane
```

4.9.3.4. R4

Este es un LSR que conmuta el tráfico de capa 2 encapsulado en función del protocolo RSVP. En su interfaz ETH se conecta la nube que permite conectar la estación de monitoreo NetFlow.

```
!
ip cef
!
multilink bundle-name authenticated
!
interface Loopback0
 description loop204
 ip address 192.168.1.204 255.255.255.255
 ip flow ingress
!
interface FastEthernet0/0
 ip address 192.168.1.41 255.255.255.252
 duplex half
 speed auto
!
interface Serial1/0
 description intMPLS
 ip address 192.168.1.22 255.255.255.252
 ip flow ingress
```

```
 mpls ip
 serial restart-delay 0
!
interface Serial1/1
 description intMPLS
 ip address 192.168.1.34 255.255.255.252
 ip flow ingress
 mpls ip
 serial restart-delay 0
!
interface Serial1/2
 description intMPLSclk
 ip address 192.168.1.29 255.255.255.252
 ip flow ingress
 mpls ip
 serial restart-delay 0
 clock rate 252000
!
interface Serial1/3
 description intMPLSclk
 ip address 192.168.1.17 255.255.255.252
 ip flow ingress
 mpls ip
 serial restart-delay 0
 clock rate 252000
!
router ospf 100
 log-adjacency-changes
 network 192.168.1.16 0.0.0.3 area 0
 network 192.168.1.20 0.0.0.3 area 0
 network 192.168.1.28 0.0.0.3 area 0
 network 192.168.1.32 0.0.0.3 area 0
 network 192.168.1.40 0.0.0.3 area 0
 network 192.168.1.204 0.0.0.0 area 0
!
router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.1.41 remote-as 65000
 neighbor 192.168.1.41 update-source Loopback0
 neighbor 192.168.1.42 remote-as 65000
 neighbor 192.168.1.42 update-source Loopback0
 neighbor 192.168.1.201 remote-as 65000
 neighbor 192.168.1.201 update-source Loopback0
 neighbor 192.168.1.202 remote-as 65000
 neighbor 192.168.1.202 update-source Loopback0
 neighbor 192.168.1.203 remote-as 65000
 neighbor 192.168.1.203 update-source Loopback0
```

```
 neighbor 192.168.1.205 remote-as 65000
 neighbor 192.168.1.205 update-source Loopback0
 neighbor 192.168.1.206 remote-as 65000
 neighbor 192.168.1.206 update-source Loopback0
 no auto-summary
!
ip flow-export version 5
ip flow-export destination 192.168.1.42 9996
!
control-plane
```

4.9.3.5. R5

Este es un LSR que conmuta el tráfico de capa 2 encapsulado en función del protocolo RSVP.

```
!
multilink bundle-name authenticated
mpls traffic-eng tunnels
!
interface Loopback0
 description loop205
 ip address 192.168.1.205 255.255.255.255
 ip flow ingress
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Serial1/0
 description intMPLS
 ip address 192.168.1.38 255.255.255.252
 ip flow ingress
 mpls ip
 serial restart-delay 0
!
interface Serial1/1
 description intMPLSclk
 ip address 192.168.1.13 255.255.255.252
 ip flow ingress
 mpls traffic-eng tunnels
 mpls ip
 serial restart-delay 0
 clock rate 252000
```

```
 ip rsvp bandwidth 256 256
!
interface Serial1/2
 description intMPLS
 ip address 192.168.1.26 255.255.255.252
 ip flow ingress
 mpls traffic-eng tunnels
 mpls ip
 serial restart-delay 0
 ip rsvp bandwidth 256 256
!
interface Serial1/3
 description intMPLS
 ip address 192.168.1.18 255.255.255.252
 ip flow ingress
 mpls ip
 serial restart-delay 0
!
router ospf 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 log-adjacency-changes
 network 192.168.1.12 0.0.0.3 area 0
 network 192.168.1.16 0.0.0.3 area 0
 network 192.168.1.24 0.0.0.3 area 0
 network 192.168.1.36 0.0.0.3 area 0
 network 192.168.1.205 0.0.0.0 area 0
!
router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.1.41 remote-as 65000
 neighbor 192.168.1.41 update-source Loopback0
 neighbor 192.168.1.42 remote-as 65000
 neighbor 192.168.1.42 update-source Loopback0
 neighbor 192.168.1.201 remote-as 65000
 neighbor 192.168.1.201 update-source Loopback0
 neighbor 192.168.1.202 remote-as 65000
 neighbor 192.168.1.202 update-source Loopback0
 neighbor 192.168.1.203 remote-as 65000
 neighbor 192.168.1.203 update-source Loopback0
 neighbor 192.168.1.204 remote-as 65000
 neighbor 192.168.1.204 update-source Loopback0
 neighbor 192.168.1.206 remote-as 65000
 neighbor 192.168.1.206 update-source Loopback0
 no auto-summary
!
ip flow-export version 5
```

```
ip flow-export destination 192.168.1.42 9996
!
control-plane
```

4.9.3.6. R6

Este es un LER que permite la entrada y salida del tráfico de FR al dominio MPLS.

```
!
ip cef
!
multilink bundle-name authenticated
FR switching
mpls traffic-eng tunnels
mpls label protocol ldp
!
interface Loopback0
 description loop206
 ip address 192.168.1.206 255.255.255.255
 ip flow ingress
!
interface Tunnel0
 ip unnumbered Loopback0
 ip flow ingress
 tunnel destination 192.168.1.201
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 2 2
 tunnel mpls traffic-eng bandwidth 100
 tunnel mpls traffic-eng path-option 1 explicit name ruta1
 no routing dynamic
!
interface Serial1/0
 description intMPLS
 ip address 192.168.1.14 255.255.255.252
 ip flow ingress
 mpls traffic-eng tunnels
 mpls ip
 serial restart-delay 0
 ip rsvp bandwidth 256 256
!
interface Serial1/1
 description intMPLS
 ip address 192.168.1.10 255.255.255.252
```

```
 ip flow ingress
 mpls ip
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 ip flow ingress
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 ip flow ingress
 encapsulation FR IETF
 serial restart-delay 0
 FR intf-type dce
!
router ospf 100
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 log-adjacency-changes
 network 192.168.1.8 0.0.0.3 area 0
 network 192.168.1.12 0.0.0.3 area 0
 network 192.168.1.40 0.0.0.3 area 0
 network 192.168.1.206 0.0.0.0 area 0
!
router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 neighbor 192.168.1.41 remote-as 65000
 neighbor 192.168.1.201 remote-as 65000
 neighbor 192.168.1.201 update-source Loopback0
 neighbor 192.168.1.202 remote-as 65000
 neighbor 192.168.1.202 update-source Loopback0
 neighbor 192.168.1.203 remote-as 65000
 neighbor 192.168.1.203 update-source Loopback0
 neighbor 192.168.1.204 remote-as 65000
 neighbor 192.168.1.204 update-source Loopback0
 neighbor 192.168.1.205 remote-as 65000
 neighbor 192.168.1.205 update-source Loopback0
 no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip flow-cache mpls label-positions mpls-length
ip flow-export version 5
```

```
ip flow-export destination 192.168.1.42 9996
!
!
ip explicit-path name ruta1 enable
 next-address 192.168.1.13
 next-address 192.168.1.25
 next-address 192.168.1.1
!
logging alarm informational
connect tunel Serial1/3 201 l2transport
 xconnect 192.168.1.201 20 encapsulation mpls
 !
mpls ldp router-id Loopback0 force
!
control-plane
!
```

4.9.3.7. R11

Es un CE que permite la conexión de las LAN a cruzar a través del dominio MPLS. Cumple también la función de CME.

```
!
ip source-route
ip cef
!
multilink bundle-name authenticated
!
interface FastEthernet0/0
 ip address 192.168.100.1 255.255.255.0
 ip flow ingress
 duplex half
!
interface Serial1/3
 no ip address
 encapsulation FR IETF
 serial restart-delay 0
 FR congestion-management
!
interface Serial1/3.1 point-to-point
 ip address 192.168.2.1 255.255.255.0
 FR interface-dlci 102
!
router ospf 200
 log-adjacency-changes
```

```
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.100.0 0.0.0.255 area 0
!
ip flow-export source FastEthernet0/0
ip flow-export version 5
ip flow-export destination 192.168.200.3 9996
!
snmp-server ifindex persist
!
control-plane
!
telephony-service
 video
 max-ephones 200
 max-dn 200
 ip source-address 192.168.100.1 port 2000
 auto assign 100 to 200
 system message VoIP
 voicemail 999
 max-conferences 4 gain -6
 transfer-system full-consult
 create cnf-files version-stamp Jan 01 2002 00:00:00
!
ephone-dn  1
 number 100
 name 100
!
ephone-dn  2
 number 200
 name 200
!
ephone  1
 mac-address 0200.4C4F.4F50
 type CIPC
 button  1:1
!
ephone  2
 mac-address 0019.D178.0BCC
 type CIPC
 button  1:2
!
```

4.9.3.8. R12

Es un CE que permite la conexión de las LAN a cruzar a través del dominio MPLS.

```
!
ip source-route
ip cef
!
multilink bundle-name authenticated
!
interface FastEthernet0/0
 ip address 192.168.200.1 255.255.255.0
 ip flow ingress
!
interface Serial1/3
 no ip address
 encapsulation FR IETF
 serial restart-delay 0
!
interface Serial1/3.1 point-to-point
 ip address 192.168.2.2 255.255.255.0
 FR interface-dlci 201
!
router ospf 200
 log-adjacency-changes
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.200.0 0.0.0.255 area 0
!
ip flow-export source FastEthernet0/0
ip flow-export version 5
ip flow-export destination 192.168.200.3 9996
!
snmp-server ifindex persist
!
control-plane
!
```

CONCLUSIONES

Luego de un estudio minucioso de las distintas tecnologías involucradas en la realización de este proyecto (Ethernet, Frame Relay, LDP, RSVP y MPLS), se ha podido concluir que cada una de ellas presenta sus respectivas fortalezas y debilidades que deben ser consideradas al momento del diseño, para de esta manera obtener una red escalable pero, sobre todo, de alto rendimiento.

Se ha comprobado que MPLS puede integrar distintos dominios de red independientemente de su protocolo de capa 2 a través de distintas técnicas de encapsulamiento gracias a la gestión multi-etiquetas y de tunelizado que presenta este protocolo de capa 2.5. Haciendo uso de la tecnología AToM de Cisco se realizó la simulación respectiva para cada escenario por separado, de las cuales, luego del respectivo análisis de los resultados, se pudo comprobar que la hipótesis planteada al inicio de la investigación, es real.

El indicador 1 (transmisiones RT), relacionado con el tráfico de tiempo real, es el más influyente en el proceso de decisión representado el 80% del resultado final; en este indicador constan el Jitter y la pérdida de paquetes, que son aquellos índices que contribuyen con el 30 % cada uno, debido a su mayor influencia en las comunicaciones y su directa relación con el indicador 2 (transmisiones NRT) el cual, representa solo el 20% del resultado final.

El protocolo de señalización LDP junto con la tecnología de acceso Ethernet presenta un rendimiento del 76.83 % frente a Frame Relay que tiene un 41.49 %, superándolo de esta manera en aproximadamente un 35%, en cambio con el protocolo RSVP, el rendimiento de Ethernet sobrepasa a Frame Relay por un 38%, de esta manera se concluye que el protocolo RSVP

proporciona un mejor rendimiento independientemente de la tecnología de acceso estudiada en esta investigación.

Así, la tecnología ETH debido a su mayor capacidad de transmisión ha superado a Frame Relay, y esta ventaja se acentúa aún más si el enrutamiento es explícito. De esta forma, sobre un 100%, ETH + RSVP presenta un 85,78%, en relación a FR + RSVP que tan solo alcanzo el 48.12 % de su rendimiento, superándolo así en un 38%, demostrando de esta forma que Ethernet es la tecnología de acceso que presenta un mejor rendimiento sobre una arquitectura MPLS.

RECOMENDACIONES

Es necesario investigar a fondo las características de los dispositivos que van a intervenir en el diseño de una red, ya que en nuestro caso, para implementar el soporte multiprotocolo de MPLS fue necesario hacer uso de AToM, el mismo que es soportado solo por equipos de gama media y con las últimas actualizaciones de sus sistemas operativos.

Al momento de hacer mediciones del rendimiento de una red es necesario elegir parámetros que sean medibles con las herramientas que se tenga a disposición; estas mediciones deben ser realizadas siguiendo las recomendaciones sugeridas por la ITU-T por ejemplo, con la finalidad de que el procedimiento sea estandarizado y no haya lugar a dudas.

Para realizar las simulaciones con GNS3 es necesario contar con el hardware lo suficientemente potente como procesar la información de muchos enrutadores simultáneamente. Siendo necesario tener como mínimo 2 GB de memoria RAM, una velocidad de procesador de al menos 2 GHz, entre otras características citadas en el capítulo 3.

Se debe tener muy cuenta la configuración de direcciones con mascara de 32 bits para que sirvan como direcciones de referencia para LDP y los túneles creados por AToM. De no ser así, estas interfaces podrían ser inestables y no se podrían crear los LSP necesarios.

Se recomienda hacer uso de Ethernet como tecnología de acceso, ya que de acuerdo a esta investigación, es la que presenta las mejores condiciones para un flujo intensivo de tráfico a través de un dominio MPLS y, que junto a un protocolo de señalización RSVP, hacen un uso eficiente de los recursos disponibles.

RESUMEN

El análisis del rendimiento de Frame Relay vs Ethernet sobre una arquitectura MPLS, desarrollada por estudiantes de la Escuela de Ingeniería en Electrónica, Telecomunicaciones y Redes, perteneciente a la Escuela Superior Politécnica de Chimborazo proporcionan un amplio conocimiento acerca del rendimiento de las redes de acceso y su integración a las redes de siguiente generación.

Usando el método de investigación deductivo se consideraron criterios para la medición del rendimiento, propuestos por estándares existentes en el campo de las telecomunicaciones, seleccionando así, solo cierto grupo de parámetros que afectan al rendimiento de una red de telecomunicaciones. Mientras que con el método experimental se realizaron ambientes de prueba que permitieron establecer las diferencias existentes entre las tecnologías de estudio, las cuales determinaron la que ofrece mejor rendimiento, para esto se utilizó las herramientas software: GNS3, NetTools, VQManager y Cisco IP Communicator y como Hardware 3 computadoras.

Se compararon los siguientes parámetros: Jitter, Retardo, Pérdida de Paquetes, Latencia y Velocidad de Transmisión, dando como resultado que Ethernet tiene el 85.78% de rendimiento y Frame Relay un 48.12% estableciéndose una diferencia de aproximadamente el 37% entre las tecnologías de acceso.

Con la tecnología de acceso Ethernet se tiene un mejor nivel de rendimiento sobre una arquitectura MPLS, por lo cual facilita la integración de las comunicaciones de voz, video y datos.

Se recomienda hacer uso de Ethernet como tecnología de acceso, ya que junto con el protocolo RSVP (Resource Reservation Protocol), es la que presenta mejores condiciones para un flujo intensivo de tráfico.

SUMMARY

The analysis of the performance of Frame Relay vs Ethernet about MPLS Architecture, developed by the students from School of Telecommunication and Networks Engineering from Escuela Superior Politécnica de Chimborazo, provides a huge knowledge about performance of Net Access and it's integration to next generations nets.

Using the deductive research approach it was considered criteria for the measuring of performance, proposed by standards-setting for global telecommunications, selecting the, only a group of parameters that affect the performance of a net of telecommunication.

With the experimental research approach was realized the test environment the permitted established the existing differences between the two researches approach, to determine which one offers the best performance. For this purpose it was used the software tools: GNS3, NetTools, VQManager and Cisco Communicator, which was processed in 3 computers.

The follow parameters were bough: Jitter, Delay, Packet loss, Latency and Transmission speed, giving as result: Ethernet with the 85.78% of performance and Frame Relay with 48.12%, establishing a difference of approximately a 37% between this two Access technologies.

With the Access technology Ethernet the performance is better over the MPLS Architecture, and this simplifies the integration of voice, video & data communications.

It is recommended to use the Ethernet like and Access Technology, because combined with RSVP protocol (Resource Reservation Protocol), it shows better conditions for an intensive flow.

BIBLIOGRAFÍA

1. **ALVEZ, R.,** Fundamentos de MPLS., Buenos Aires-Argentina., Tiagora., 2009., Pp. 27.

2. **ALWAYN, V.,** Advanced MPLS Design and Implementation., Washington-USA., Cisco Press., 2002., Pp. 123.

3. **BLACK, U.,** MPLS and Label Switching Networks., Washington-USA., Prentice Hall., 2002., Pp. 336.

4. **GHEIN, L.,** MPLS Fundamentals., Washington-USA., Cisco Press., 2006., Pp. 93.

5. **GEROMETTA, O.,** MPLS Frame-Mode Basic., 1a Ed., Buenos Aires-Argentina., EduBooks., 2004., Pp. 26.

6. **PEPELNJAK, I.; GUICHARD J.,** MPLS and VPN Architectures., Washington-USA., Cisco Press., 2003., Pp. 504.

7. **PHEBY, L.,** Methodology And Economics., Londres-Inglaterra., MacMillan Press., 1997., Pp. 290.

8. **TOMSU, P.; WIESER, G.,** MPLS-Based VPN´s., Washington-USA., Pearson Education., 2001., Pp. 224.

INTERNET

9. A FRAMEWORK FOR QOS-BASED ROUTING IN THE INTERNET

http://tools.ietf.org/html/rfc2386

2013-04-11

10. AToM

http://www.cisco.com/warp/public/cc/so/neso/vpn/unvpnst/atomf_ov.htm

20213-03-20

11. AXCENCE NETTOOLS HELP DOCUMENTATION

http://www.axencesoftware.com/es/nettools

2013-01-12

12. EoMPLS

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SY/configuration/guide/eompls.html

2013-03-14

13. GNS3 GRAPHICAL NETWORK SIMULATOR

http://www.gns3.net/

2012-11-28

14. LDP SPECIFICATION

http://tools.ietf.org/html/rfc5036

2013-03-21

15. MULTIPROTOCOL LABEL SWITCHING ARCHITECTURE

http://www.ietf.org/rfc/rfc3031.txt

2013-03-08

16. MPLS LABEL STACK ENCODING

http://www.ietf.org/rfc/rfc3032.txt

2013-02-27

17. UNDERSTANDING DELAY IN PACKET VOICE NETWORKS

http://www.cisco.com/en/US/tech/tk652/tk698/technologies_tech_note09186a00800945df.shtml

2013-02-12

ANEXOS

ANEXO 1

RESULTADOS DE LAS MEDICIONES PARA LA TECNOLOGIA DE ACCESO ETHERNET

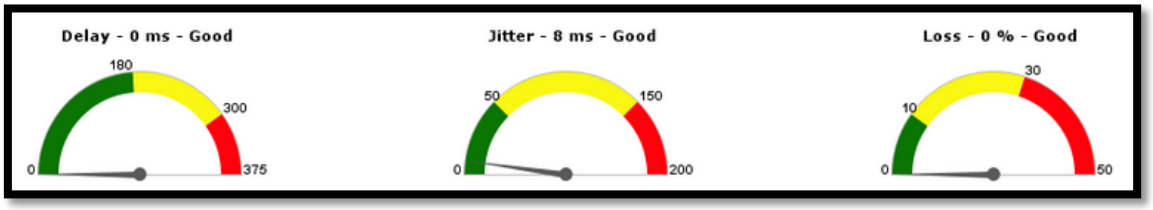
Las mediciones mostradas en este apartado son las que se extrajeron de una red Ethernet con señalización RSVP, ya que éste protocolo proporcionó un mayor nivel de rendimiento, las mediciones se las realizó con las herramientas NetTools y VQManager.

A continuación se presentan los resultados de 10 pruebas realizadas al escenario de simulación, donde se obtuvieron valores para cada uno de los parámetros que definieron el rendimiento dentro de este tema de estudio, como son: jitter, latencia, pérdida de paquetes, retardo y velocidad de transmisión.

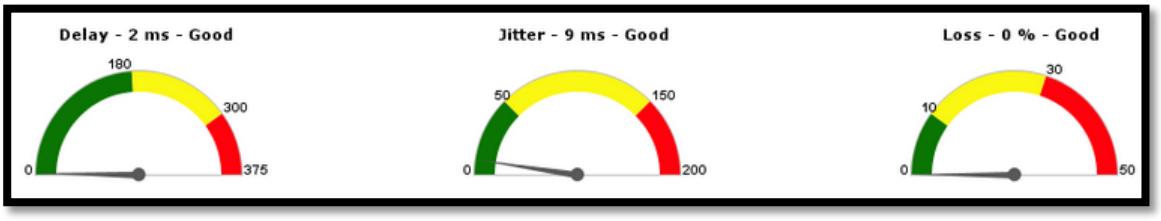
Mediciones realizadas con VQManager

Con la herramienta VQManager se midieron los parámetros: jitter, retardo y érdida de paquetes y sus valores se los puede observar en las siguientes figuras:

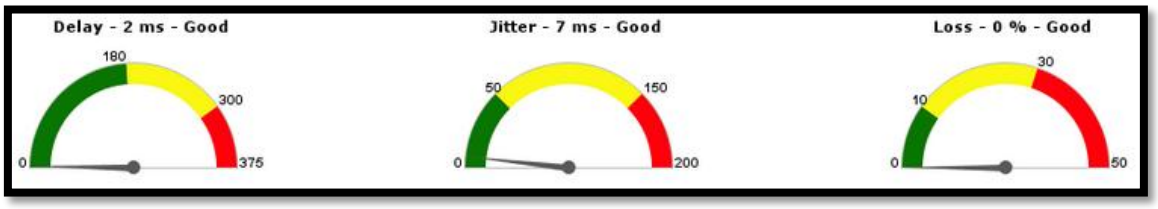
Prueba 1



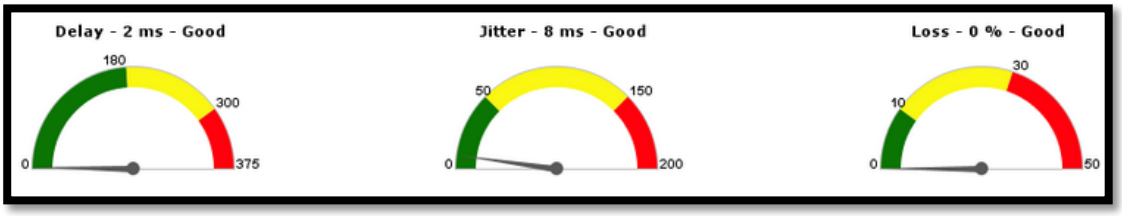
Prueba 2



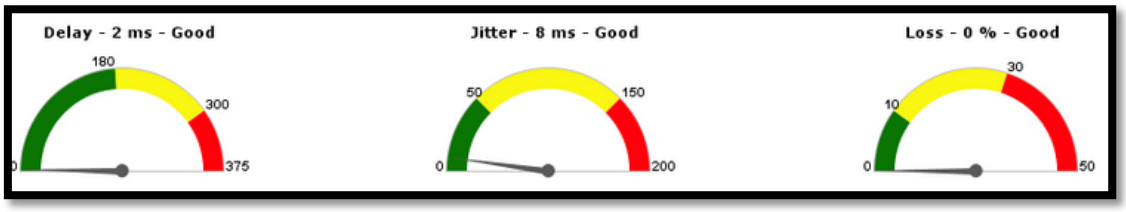
Prueba 3



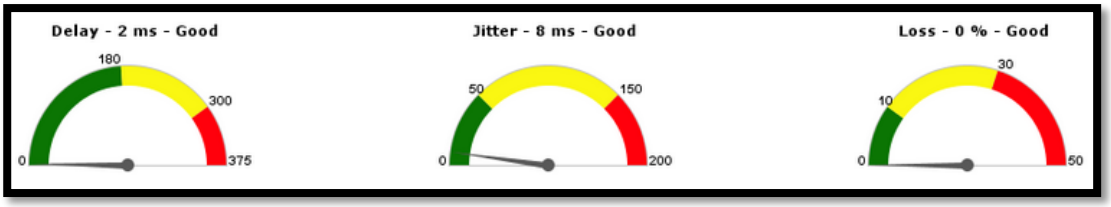
Prueba 4



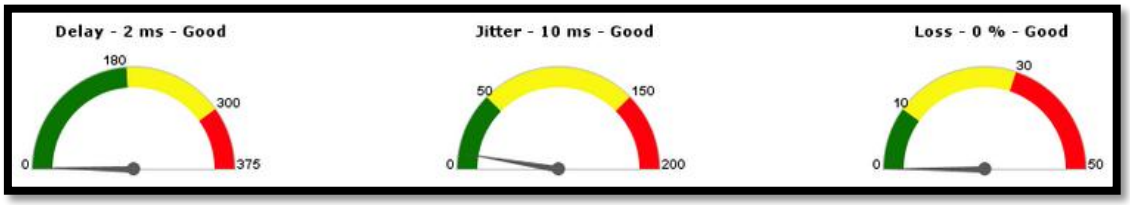
Prueba 5



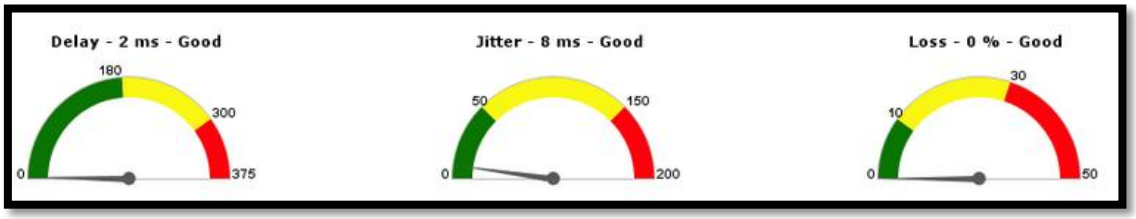
Prueba 6



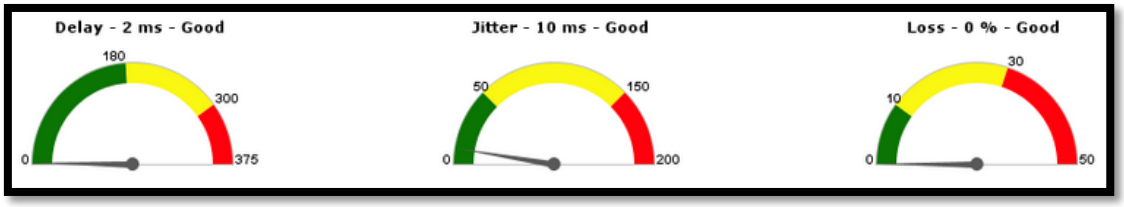
Prueba 7



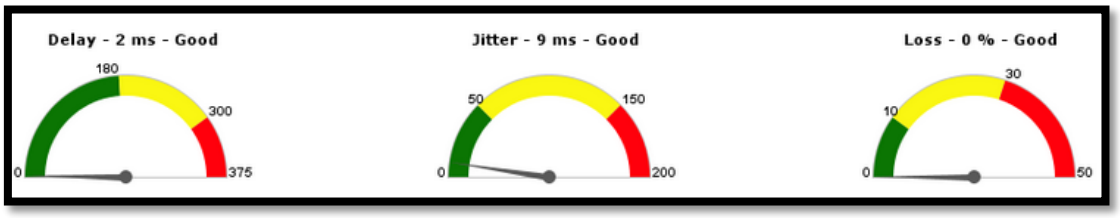
Prueba 8



Prueba 9



Prueba 10

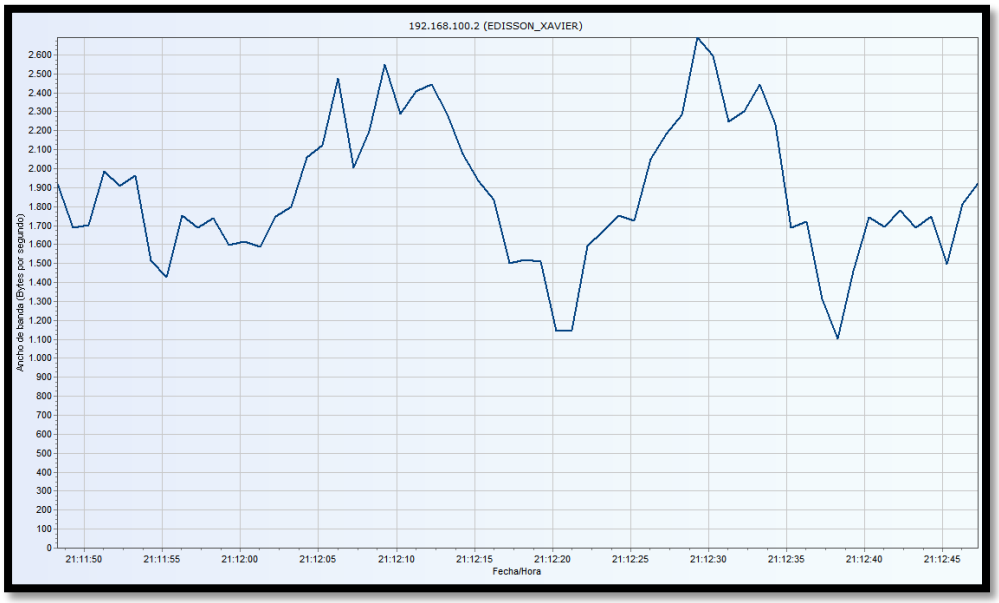


Mediciones realizadas con NetTools

Con herramienta NetTools se midieron los parámetros: BW y latencia; valores que se muestran en las siguientes figuras:

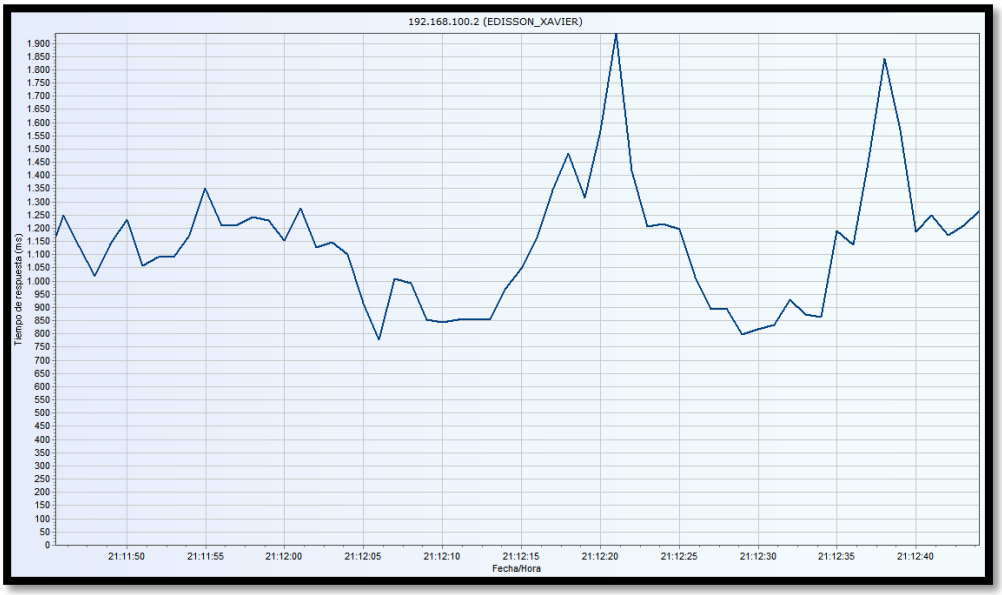
Prueba 1

- BW



- Latencia

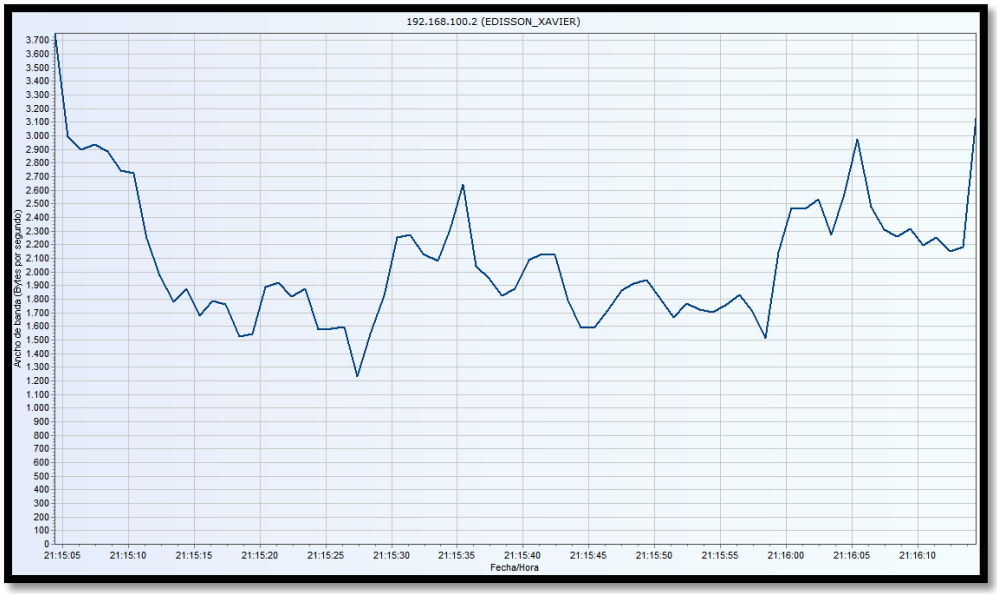
Paquetes:		
Enviados:	60	
Recibidos:	60	(100 %)
Perdidos:	0	(0 %)
Tiempo de respuesta (ms):		
Promedio:	1141	
Mínimo:	777	
Máximo:	1938	



Prueba 2

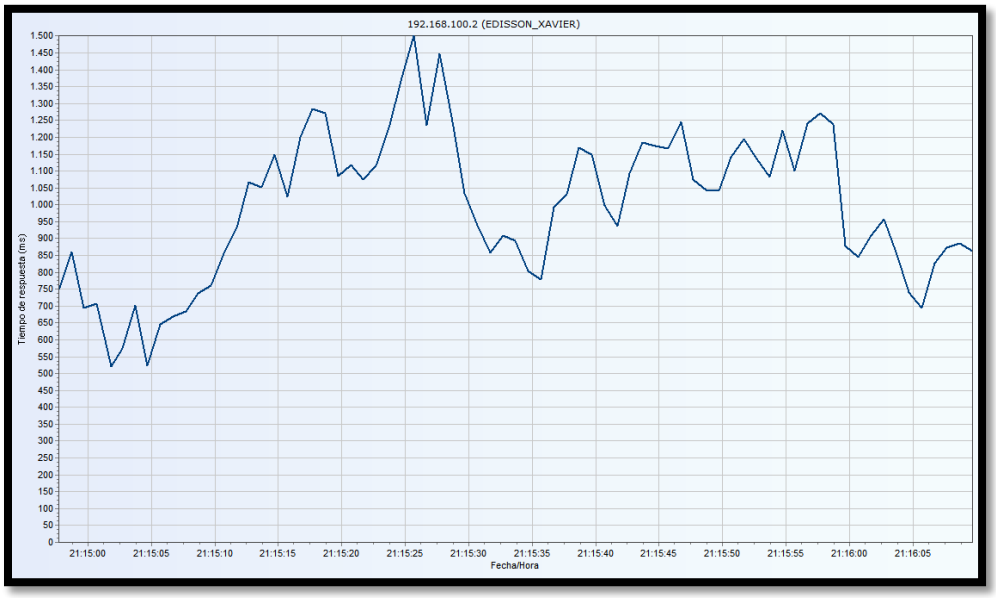
- BW

Paquetes:		
Enviados:	73	
Recibidos:	73	(100 %)
Perdidos:	0	(0 %)
Tiempo de respuesta (ms):		
Promedio:	994	
Mínimo:	520	
Máximo:	1501	



- Latencia

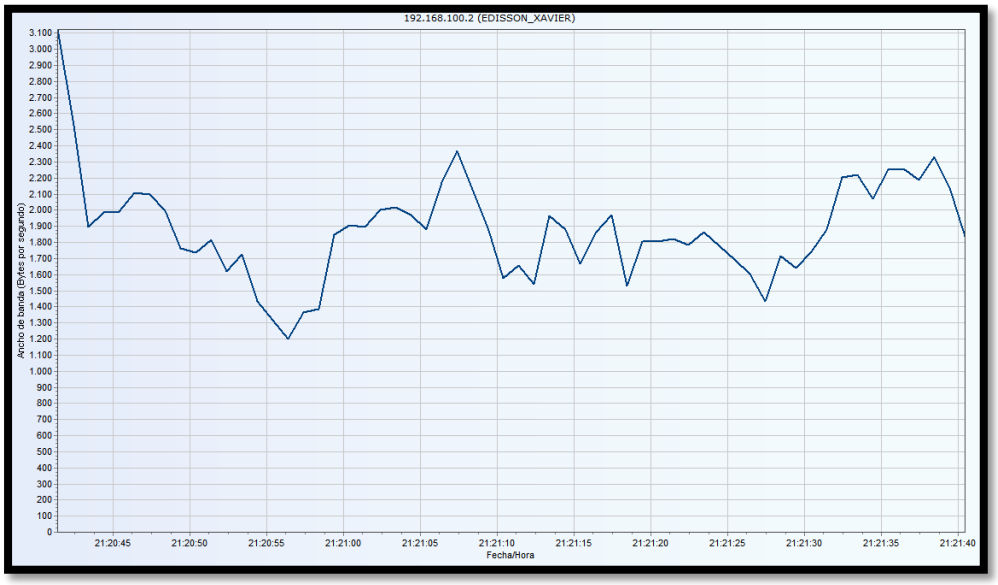
Paquetes:		
Enviados:	73	
Recibidos:	73	(100 %)
Perdidos:	0	(0 %)
Tiempo de respuesta (ms):		
Promedio:	994	
Mínimo:	520	
Máximo:	1501	


192.168.100.2 (EDISSON_XAVIER)
Tiempo de respuesta (ms)
Fecha/Hora

Prueba 3

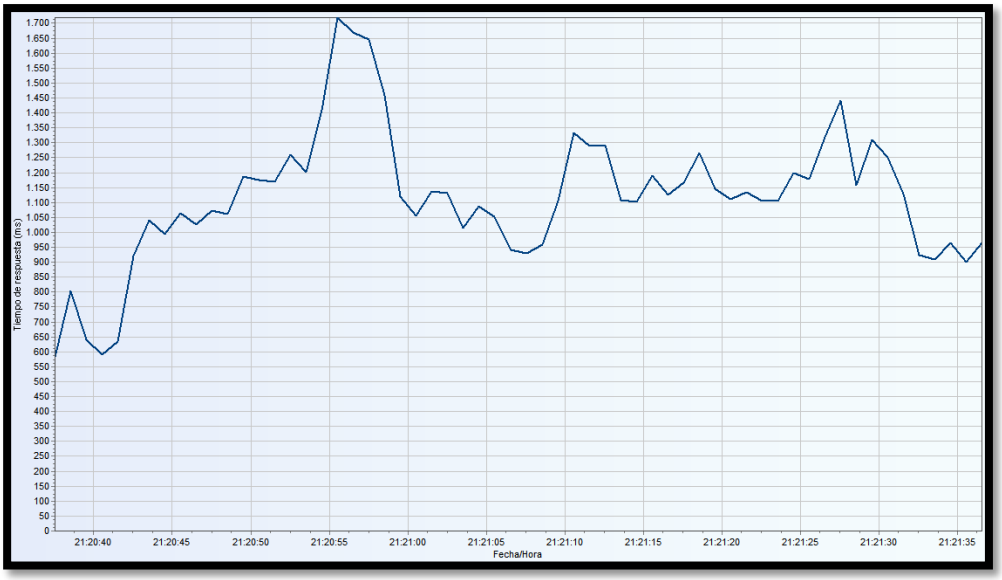
- BW


Ancho de banda:
Promedio 15 057
Mínimo 9 592
Máximo 24 984
Paquetes:
Enviados 60
Recibidos 60
Perdidos 0


192.168.100.2 (EDISSON_XAVIER)
Ancho de banda (Bytes por segundo)
Fecha/Hora

- Latencia

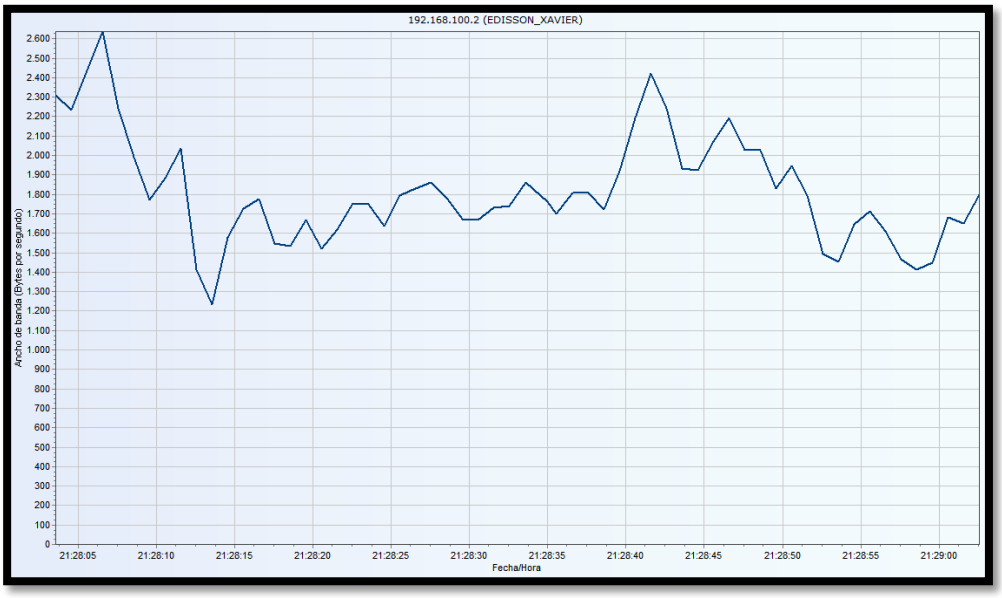
Paquetes:		
Enviados:	60	
Recibidos:	60	(100 %)
Perdidos:	0	(0 %)
Tiempo de respuesta (ms):		
Promedio:	1117	
Mínimo:	583	
Máximo:	1719	



Prueba 4

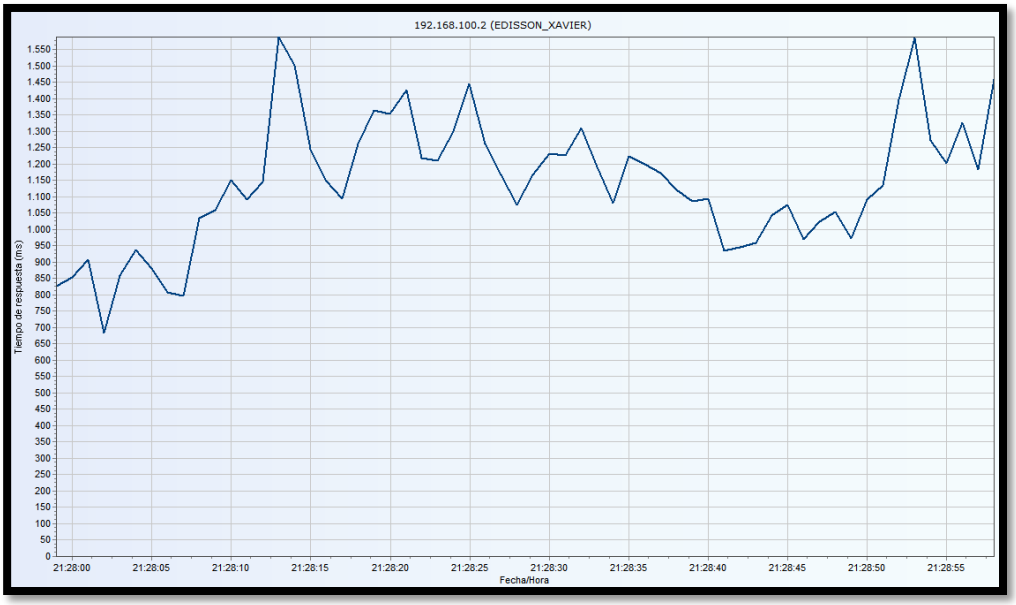
- BW

Ancho de banda:	
Promedio	14 523
Mínimo	9 864
Máximo	21 096
Paquetes:	
Enviados	60
Recibidos	60 (10
Perdidos	0 (



- Latencia

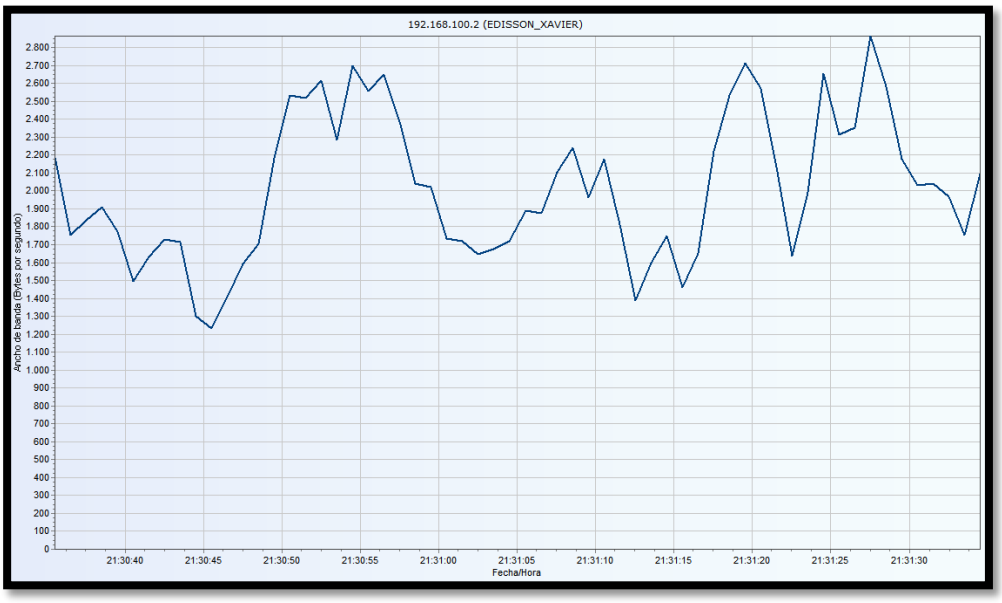
Paquetes:		
Enviados:	60	
Recibidos:	60	(100 %)
Perdidos:	0	(0 %)
Tiempo de respuesta (ms):		
Promedio:	1141	
Mínimo:	683	
Máximo:	1589	



Prueba 5

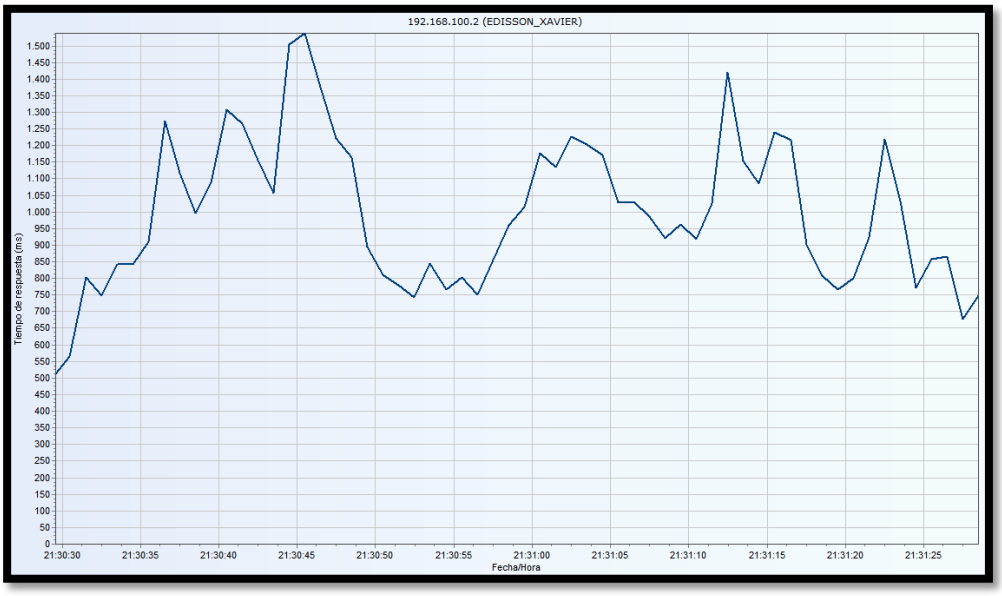
- BW

Ancho de banda:	
Promedio	16 109 I
Mínimo	9 872 I
Máximo	22 912 I
Paquetes:	
Enviados	60
Recibidos	60 (10
Perdidos	0 (



- Latencia

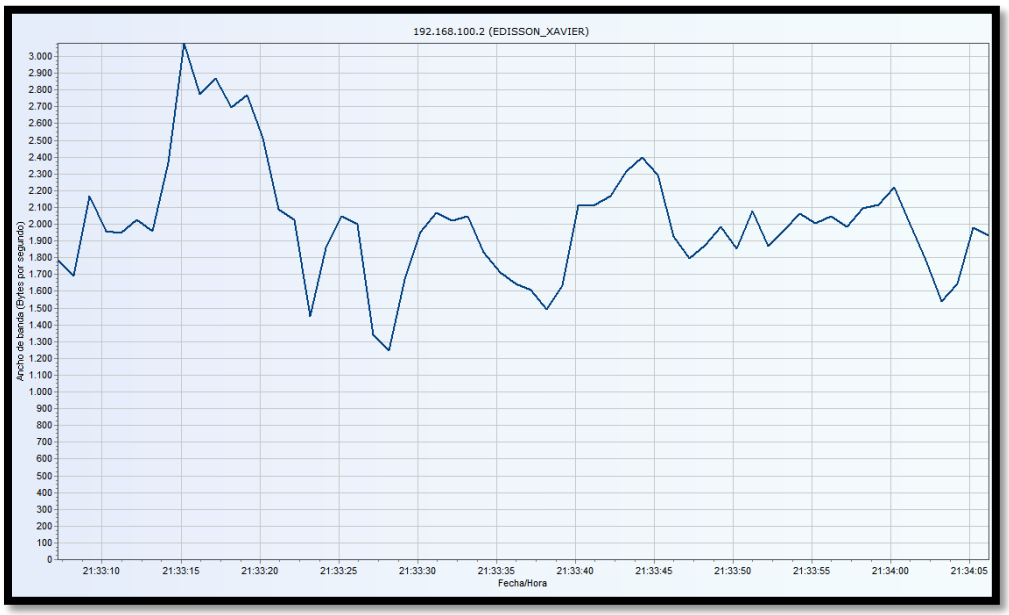
Paquetes:		
Enviados:	60	
Recibidos:	60	(100 %)
Perdidos:	0	(0 %)
Tiempo de respuesta (ms):		
Promedio:	997	
Mínimo:	512	
Máximo:	1538	



Prueba 6

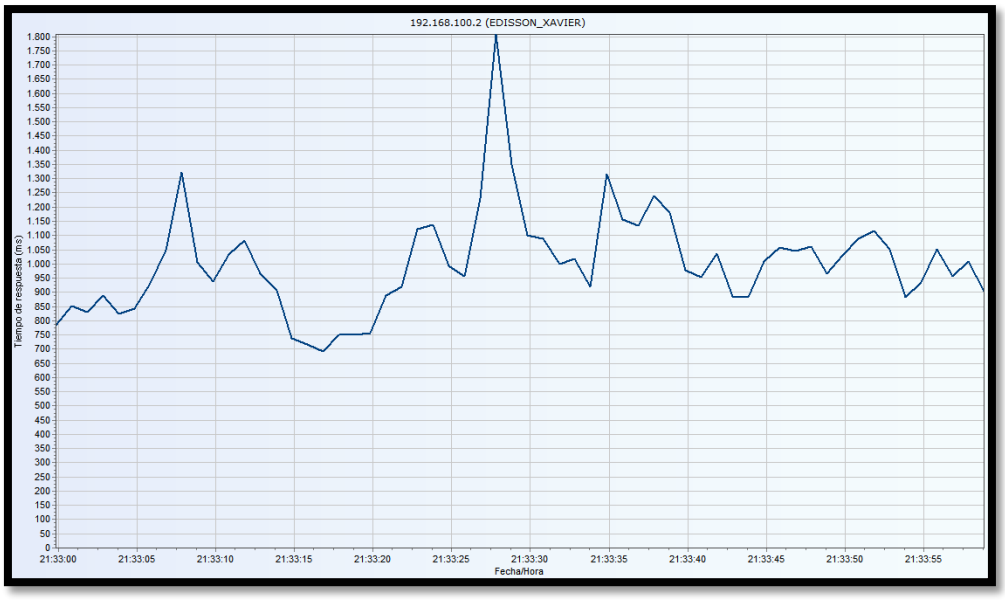
- BW

Ancho de banda:	
Promedio	16 066 l
Mínimo	9 952 l
Máximo	24 632 l
Paquetes:	
Enviados	60
Recibidos	60 (10
Perdidos	0 (



- Latencia

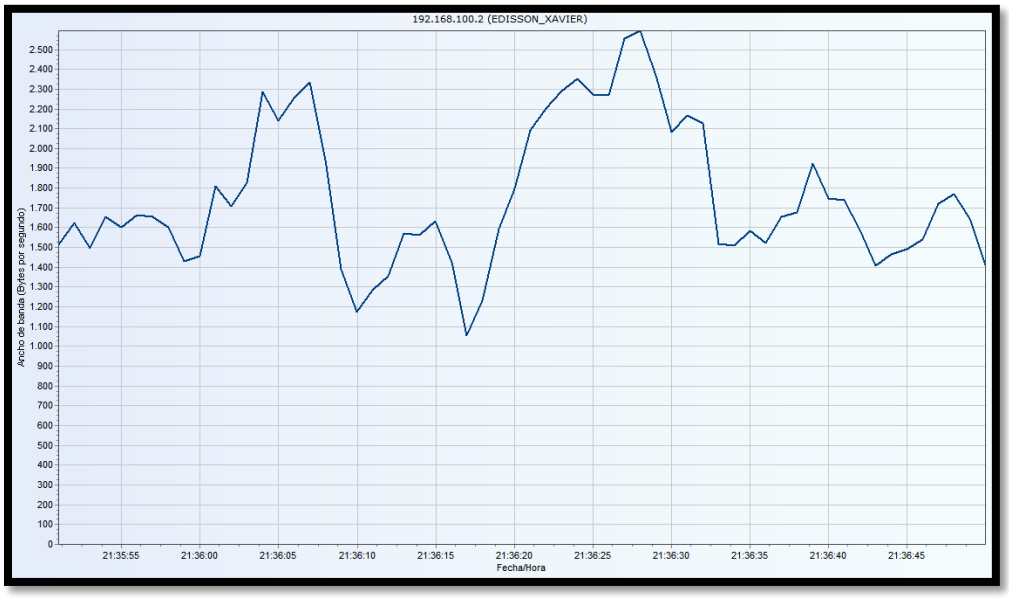
Paquetes:		
Enviados:	60	
Recibidos:	60	(100 %)
Perdidos:	0	(0 %)
Tiempo de respuesta (ms):		
Promedio:	1002	
Mínimo:	693	
Máximo:	1808	



Prueba 7

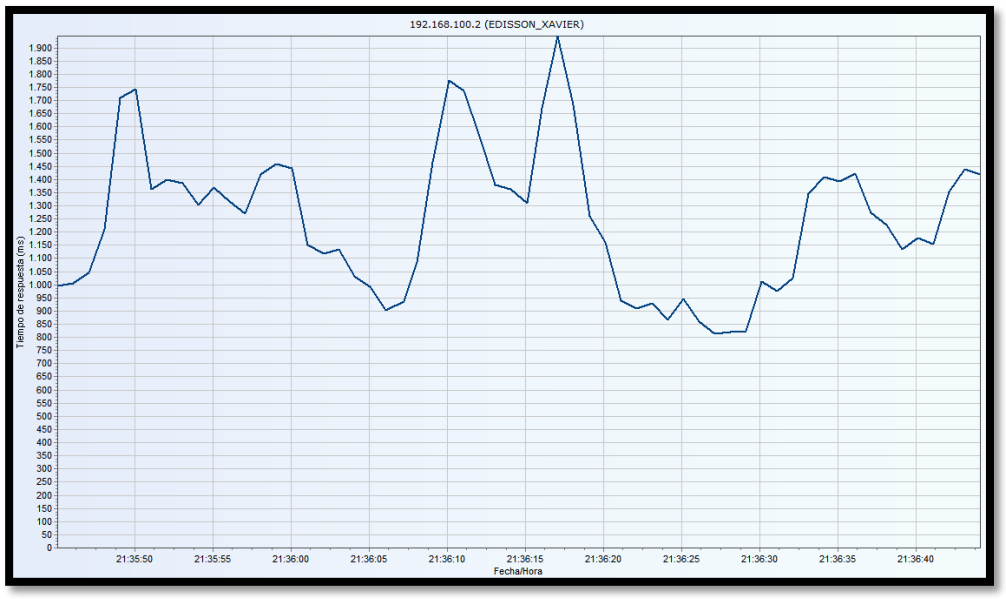
- BW

Ancho de banda:	
Promedio	14 047 I
Mínimo	8 424 I
Máximo	20 760 I
Paquetes:	
Enviados	60
Recibidos	60 (10
Perdidos	0 (



- Latencia

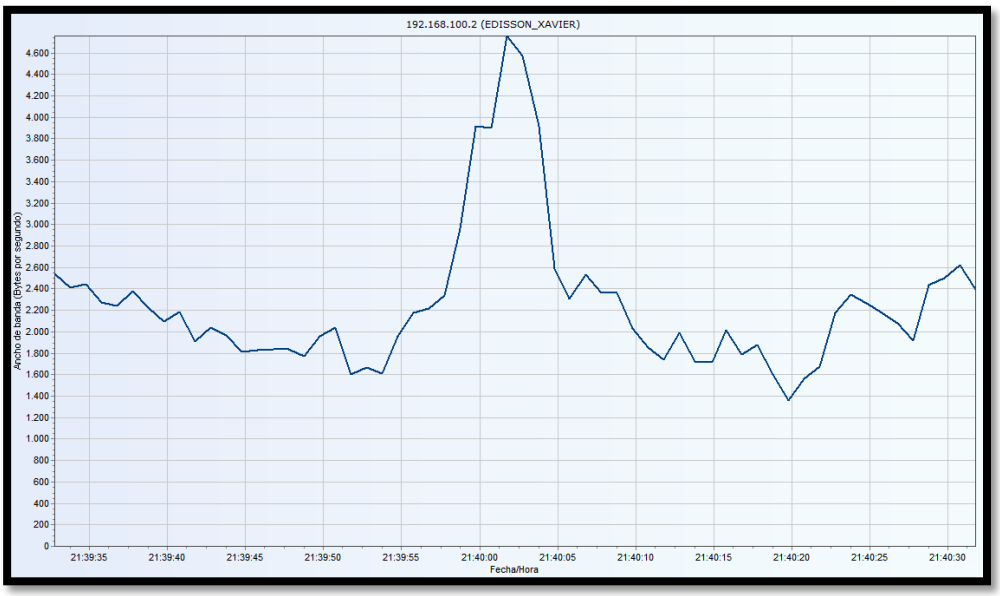
Paquetes:		
Enviados:	60	
Recibidos:	60	(100 %)
Perdidos:	0	(0 %)
Tiempo de respuesta (ms):		
Promedio:	1247	
Mínimo:	814	
Máximo:	1945	



Prueba 8

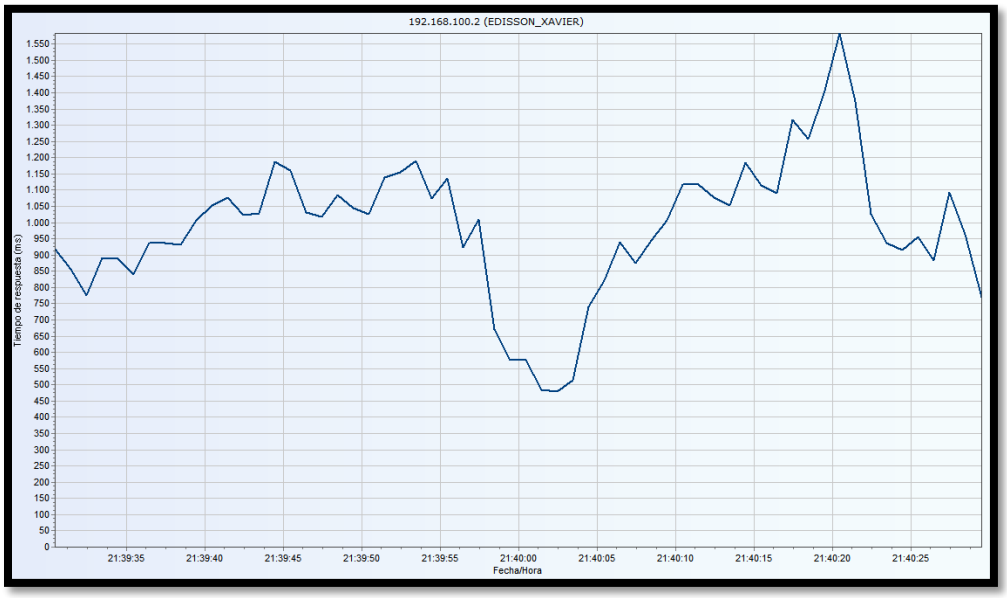
- BW

Ancho de banda:	
Promedio	18 054
Mínimo	10 848
Máximo	38 064
Paquetes:	
Enviados	60
Recibidos	60 (10
Perdidos	0 (



- Latencia

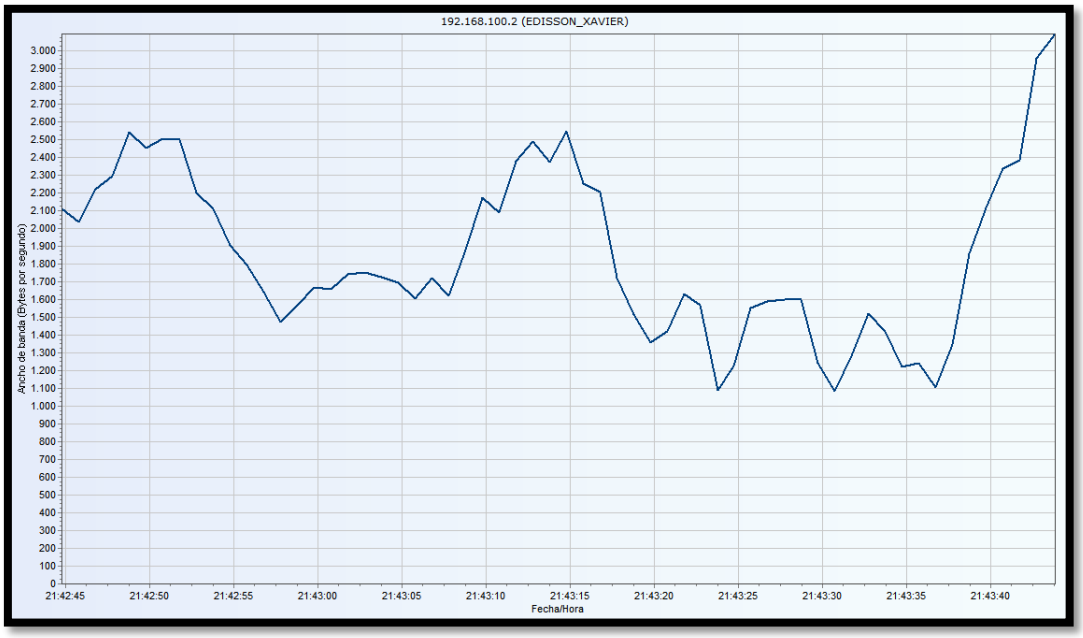
Paquetes:		
Enviados:	60	
Recibidos:	60	(100 %)
Perdidos:	0	(0 %)
Tiempo de respuesta (ms):		
Promedio:	987	
Mínimo:	480	
Máximo:	1583	



Prueba 9

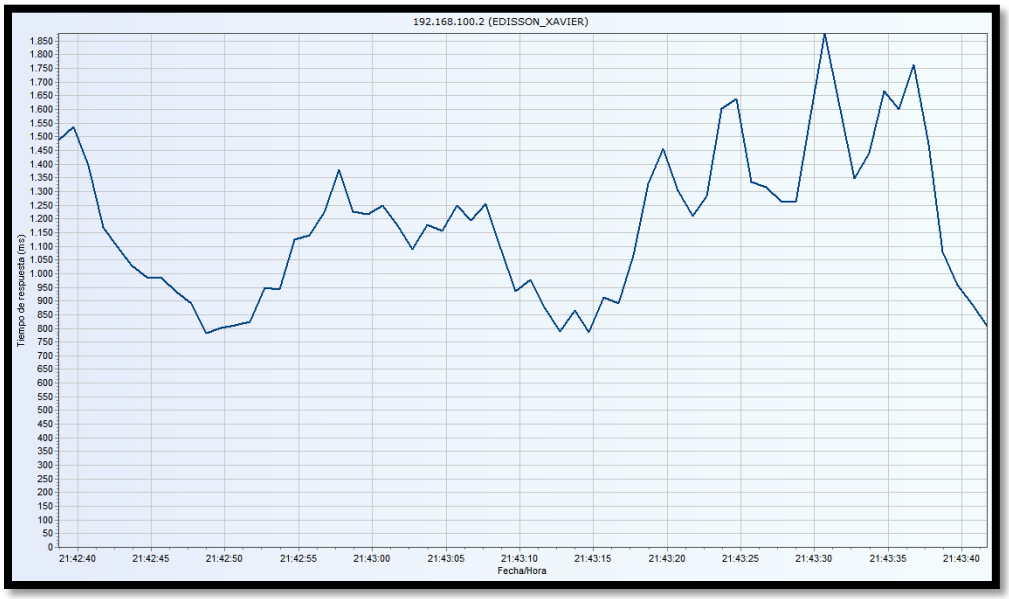
- BW

Ancho de banda:	
Promedio	14 804 I
Mínimo	8 672 I
Máximo	24 752 I
Paquetes:	
Enviados	60
Recibidos	60 (10
Perdidos	0 (



- Latencia

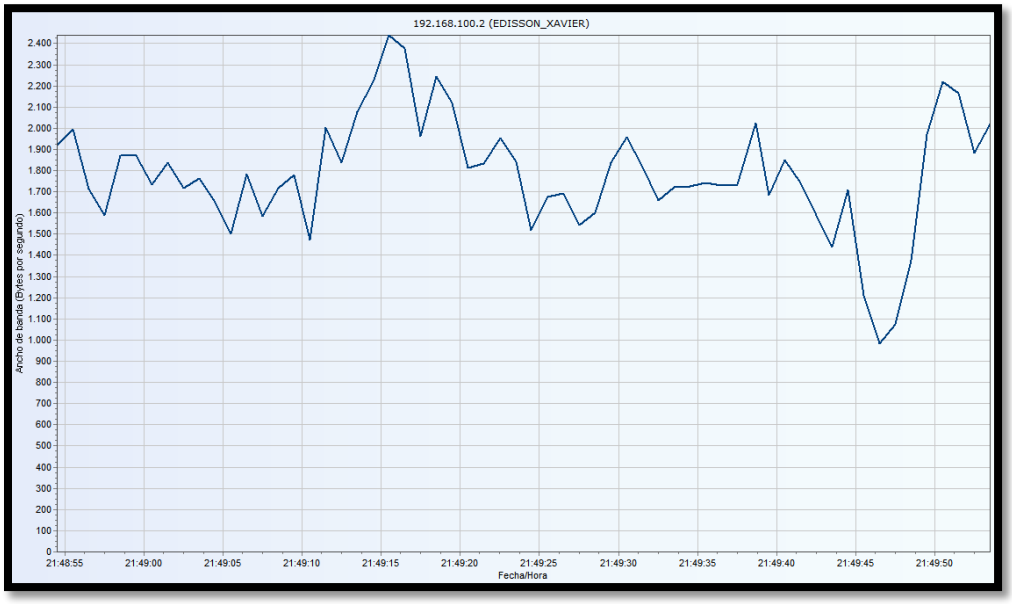
Paquetes:		
Enviados:	64	
Recibidos:	64	(100 %)
Perdidos:	0	(0 %)
Tiempo de respuesta (ms):		
Promedio:	1184	
Mínimo:	783	
Máximo:	1878	



Prueba 10

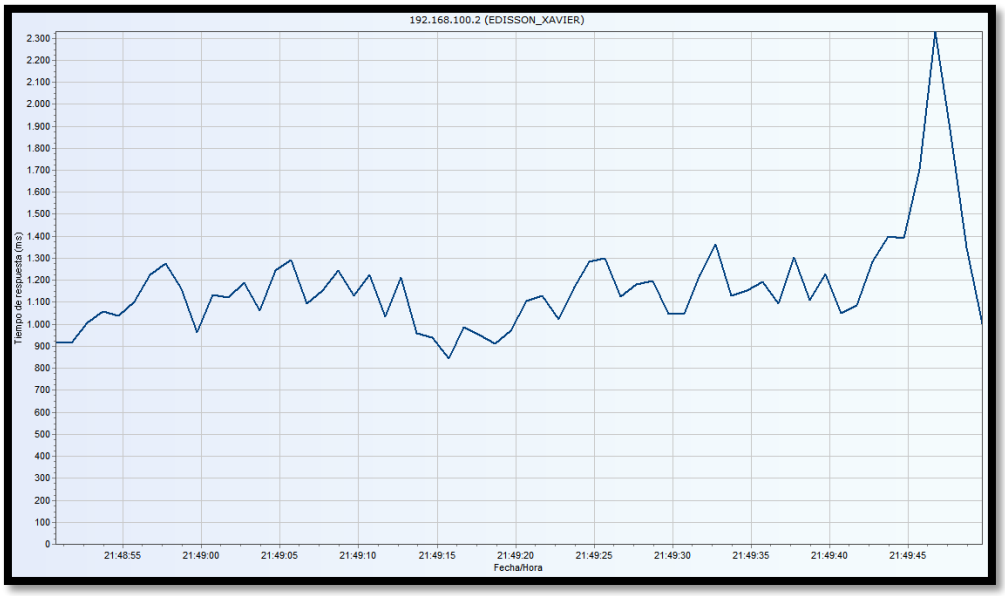
- BW

Ancho de banda:	
Promedio	14 283
Mínimo	7 864
Máximo	19 512
Paquetes:	
Enviados	60
Recibidos	60 (10
Perdidos	0 (



- Latencia

Paquetes:		
Enviados:	60	
Recibidos:	60	(100 %)
Perdidos:	0	(0 %)
Tiempo de respuesta (ms):		
Promedio:	1171	
Mínimo:	845	
Máximo:	2330	


192.168.100.2 (EDISSON_XAVIER)
Tiempo de respuesta (ms)
2.300
2.200
2.100
2.000
1.900
1.800
1.700
1.600
1.500
1.400
1.300
1.200
1.100
1.000
900
800
700
600
500
400
300
200
100
0
21:48:55
21:49:00
21:49:05
21:49:10
21:49:15
21:49:20
21:49:25
21:49:30
21:49:35
21:49:40
21:49:45
Fecha/Hora

ANEXO 2

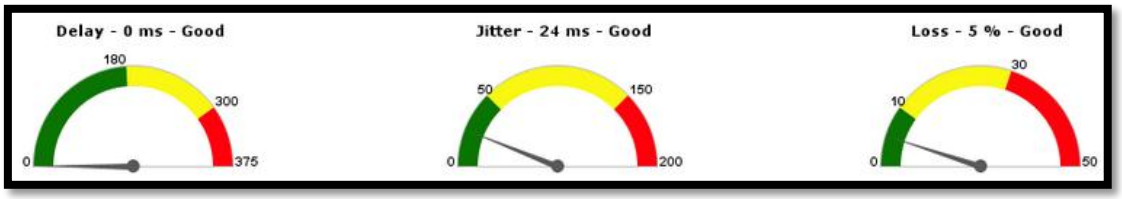
RESULTADOS DE LAS MEDICIONES PARA LA TECNOLOGIA DE ACCESO FRAME RELAY

Las mediciones mostradas fueron obtenidas de una red Frame Relay con señalización RSVP, que como ya se explico es el protocolo de distribución de etiquetas que proporcionó un mejor rendimiento del tráfico que fluye atravesó de un backbone MPLS.

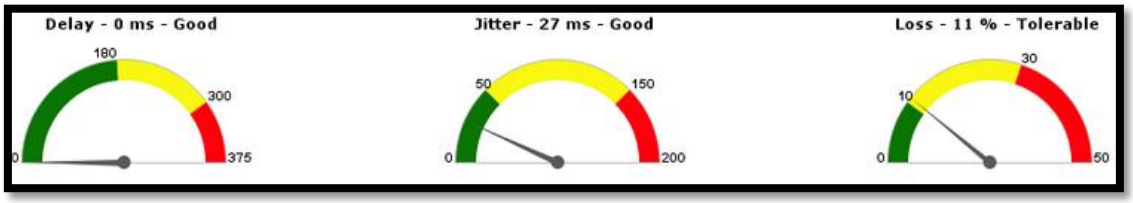
Mediciones Realizadas con VQManager

Los parámetros medidos con esta herramienta son: jitter, pérdida de paquetes, retardo; valores que se los puede ver claramente en las siguientes figuras:

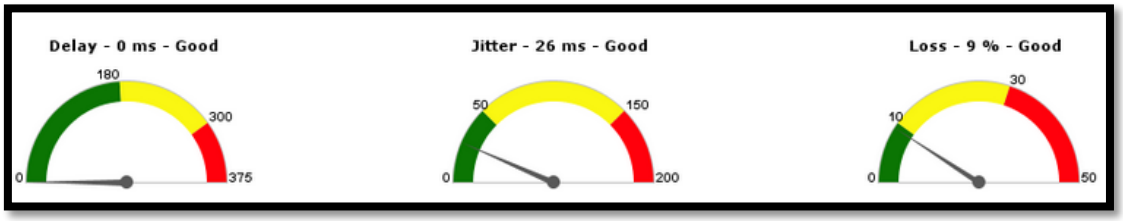
Prueba 1



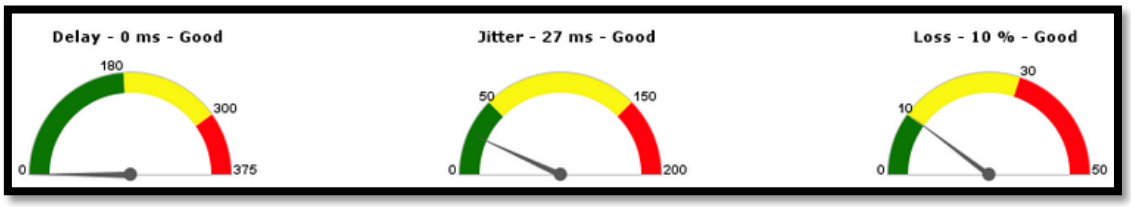
Prueba 2



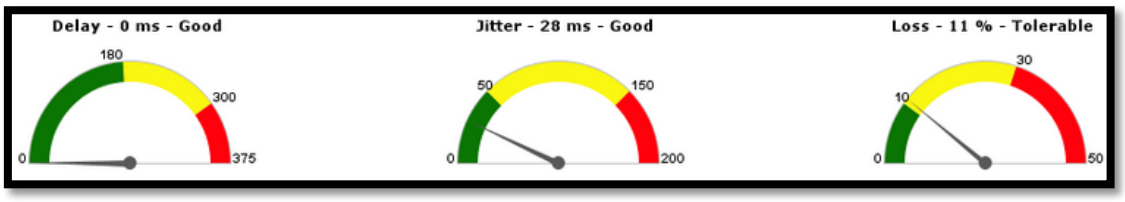
Prueba 3



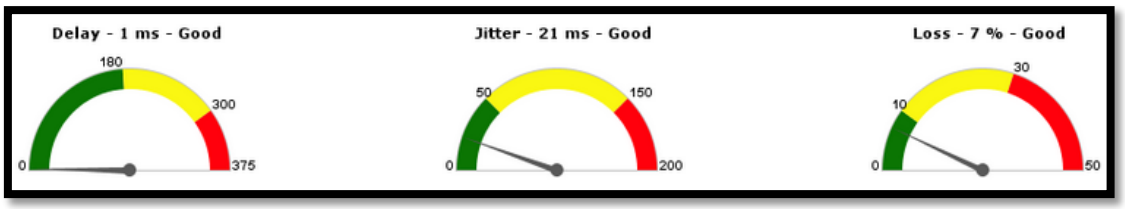
Prueba 4



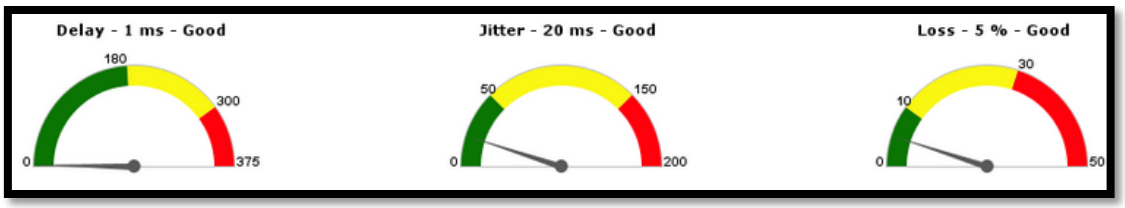
Prueba 5



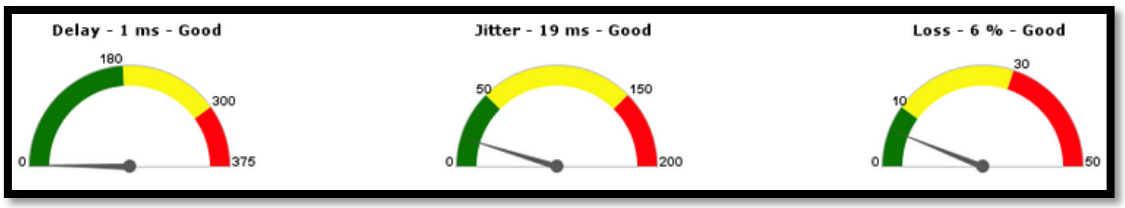
Prueba 6



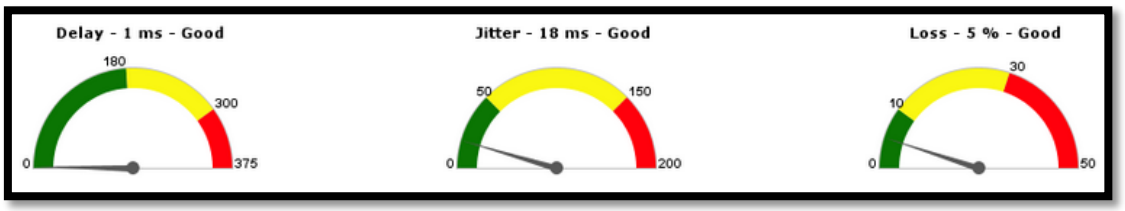
Prueba 7



Prueba 8



Prueba 9



Prueba 10

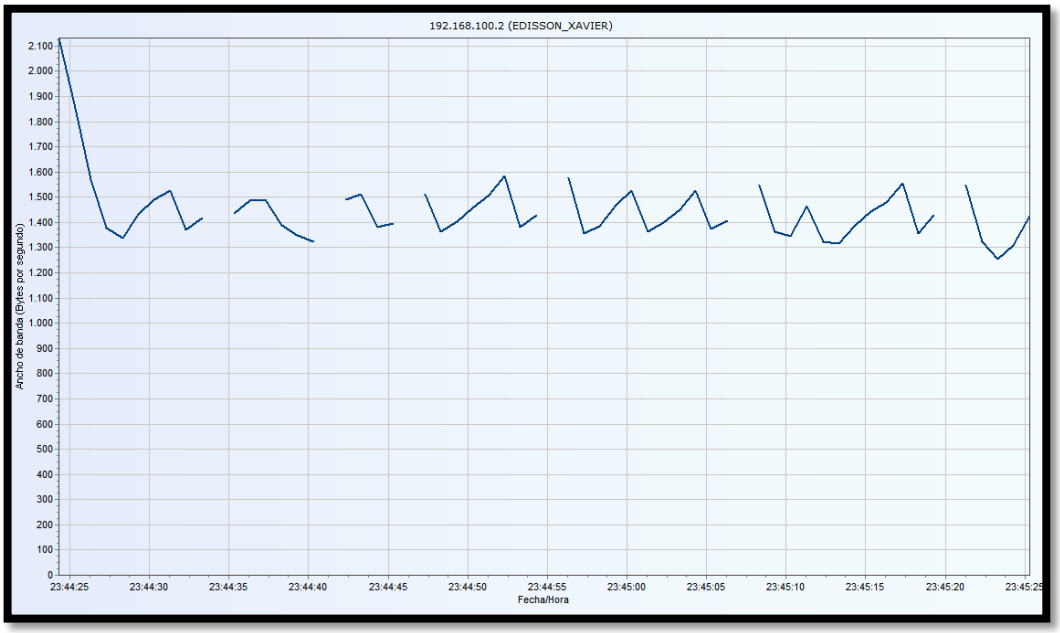
Mediciones Realizadas con NetTools

Los parámetros medidos con esta herramienta fueron BW y latencia, resultados que se las observa en las figuras siguientes:

Prueba 1

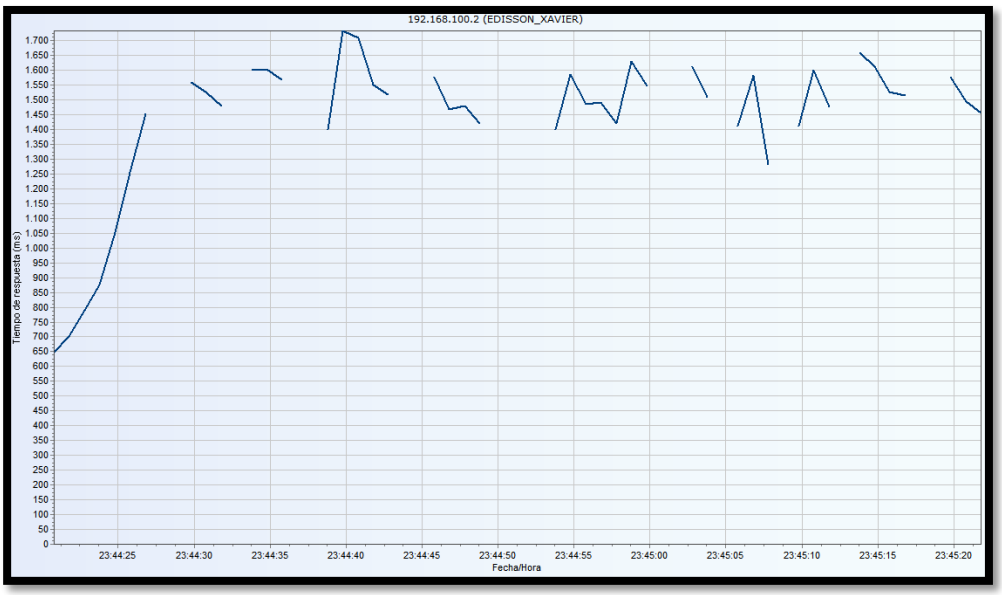
- BW

Ancho de banda:		
Promedio	11 587 l	
Mínimo	10 040 l	
Máximo	17 056 l	
Paquetes:		
Enviados	62	
Recibidos	56	(9
Perdidos	6	(1



- Latencia

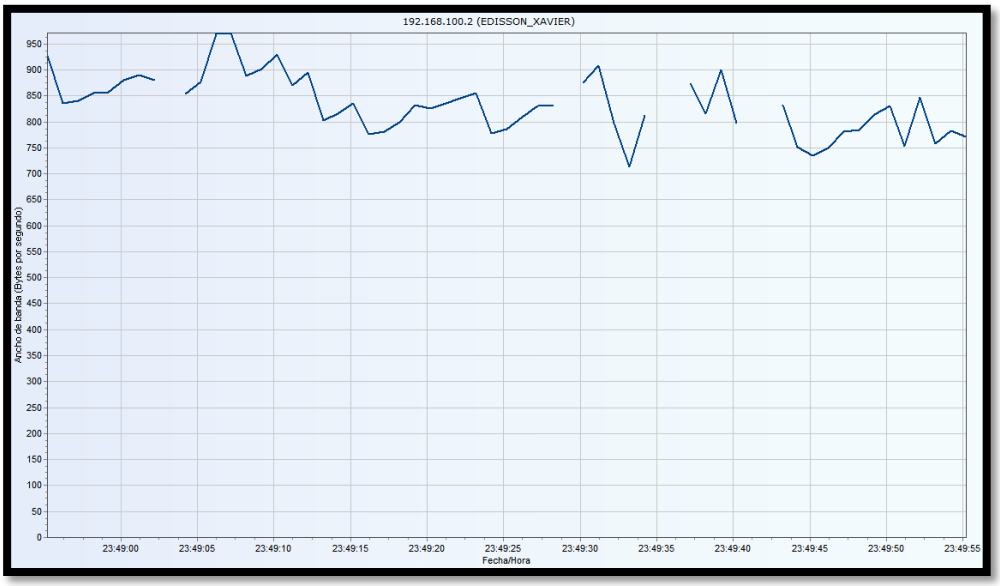
Paquetes:		
Enviados:	62	
Recibidos:	45	(73 %)
Perdidos:	17	(27 %)
Tiempo de respuesta (ms):		
Promedio:	1440	
Mínimo:	648	
Máximo:	1733	



Prueba 2

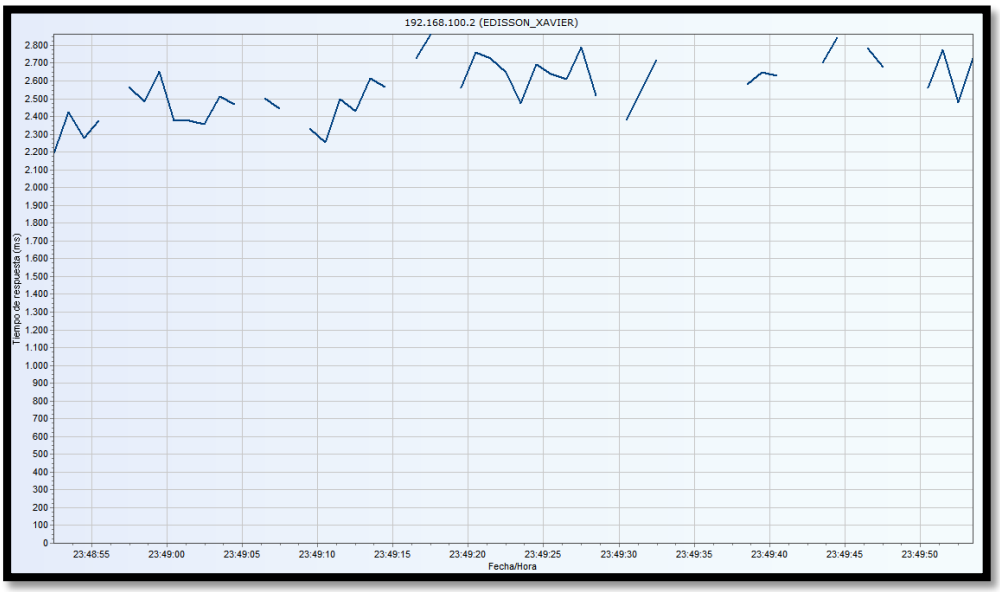
- BW

Ancho de banda:	
Promedio	6 669
Mínimo	5 712
Máximo	7 768
Paquetes:	
Enviados	61
Recibidos	55 (9
Perdidos	6 (1



- Latencia

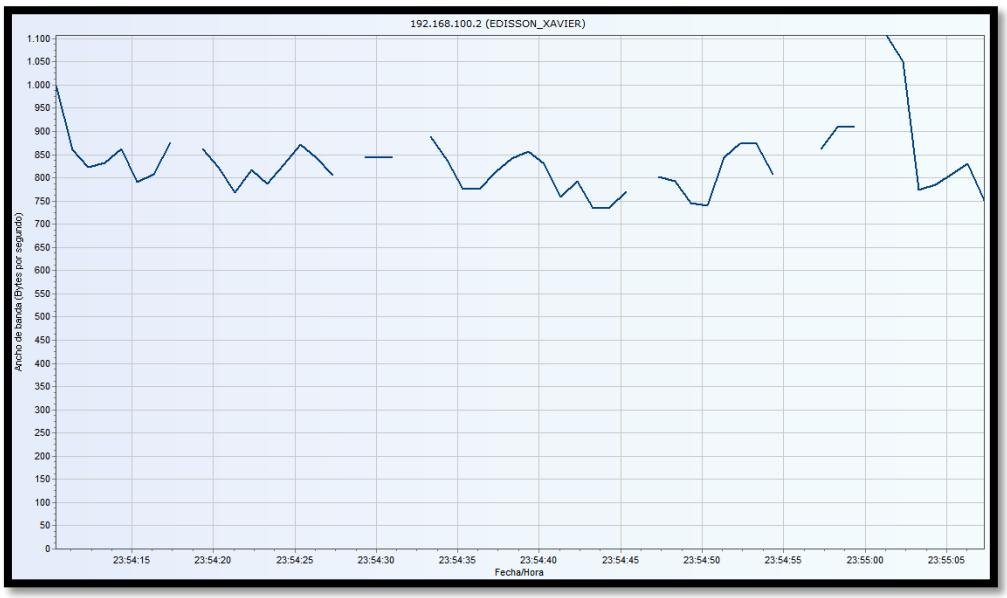
Paquetes:		
Enviados:	62	
Recibidos:	47	(76 %)
Perdidos:	15	(24 %)
Tiempo de respuesta (ms):		
Promedio:	2567	
Mínimo:	2192	
Máximo:	2863	



Prueba 3

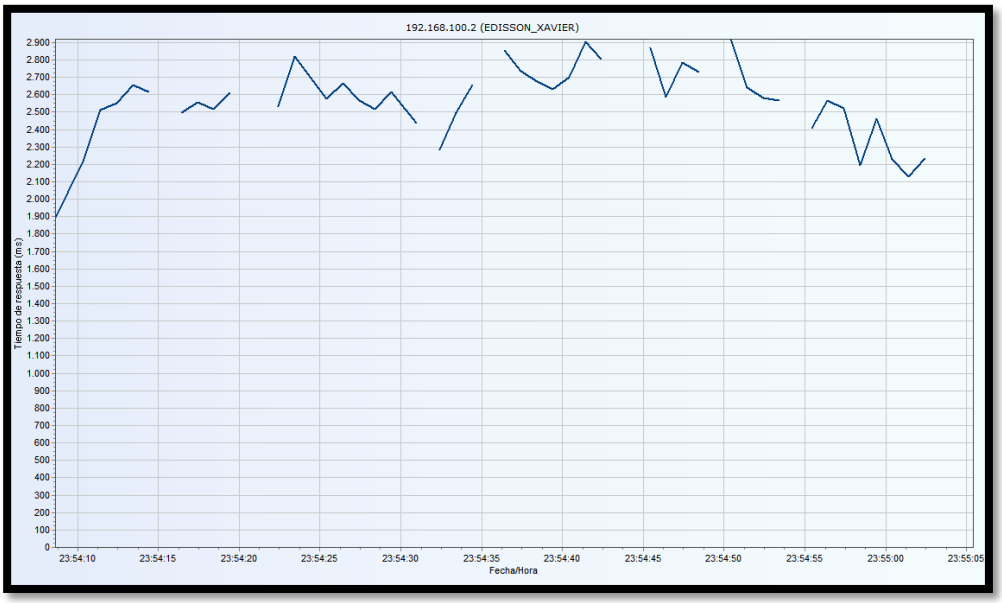
- BW

Ancho de banda:	
Promedio	6 661 I
Mínimo	5 880 I
Máximo	8 856 I
Paquetes:	
Enviados	58
Recibidos	50 (8
Perdidos	8 (1



- Latencia

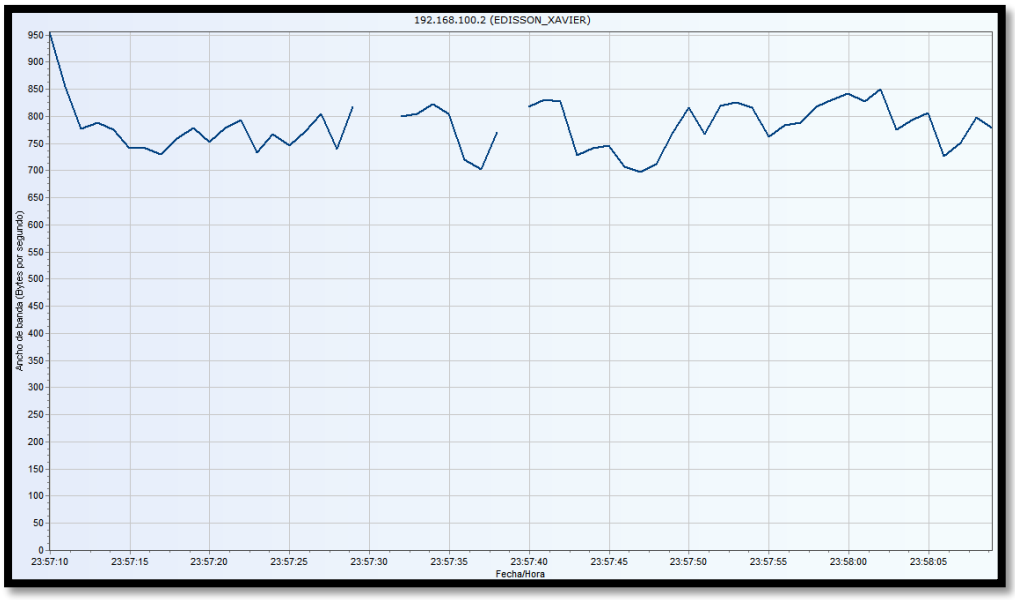
Paquetes:		
Enviados:	58	
Recibidos:	47	(81 %)
Perdidos:	11	(19 %)
Tiempo de respuesta (ms):		
Promedio:	2549	
Mínimo:	1890	
Máximo:	2919	



Prueba 4

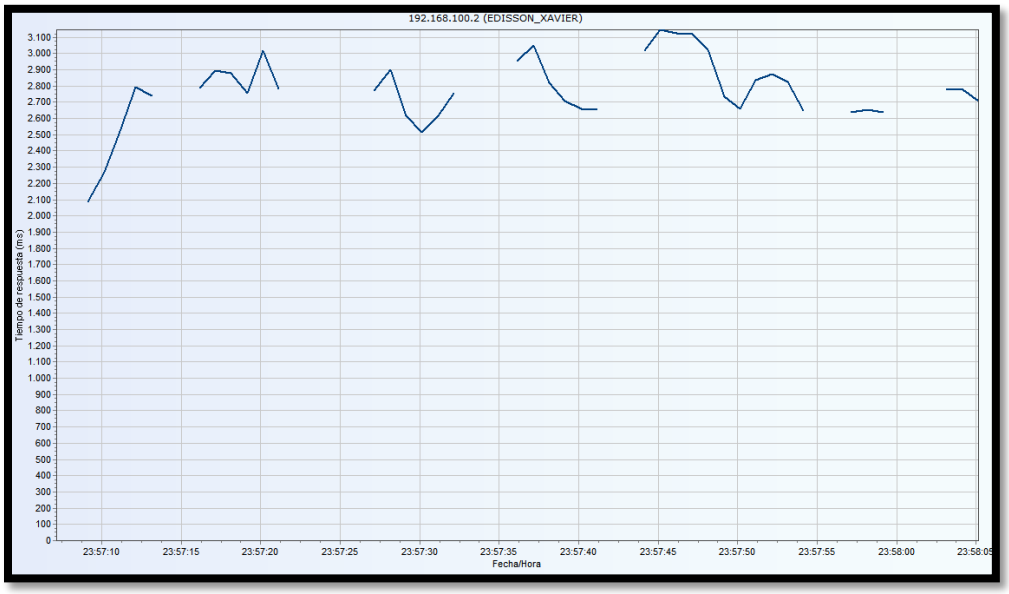
- BW

Ancho de banda:		
Promedio	6 258 l	
Mínimo	5 576 l	
Máximo	7 648 l	
Paquetes:		
Enviados	60	
Recibidos	57	(9
Perdidos	3	(



- Latencia

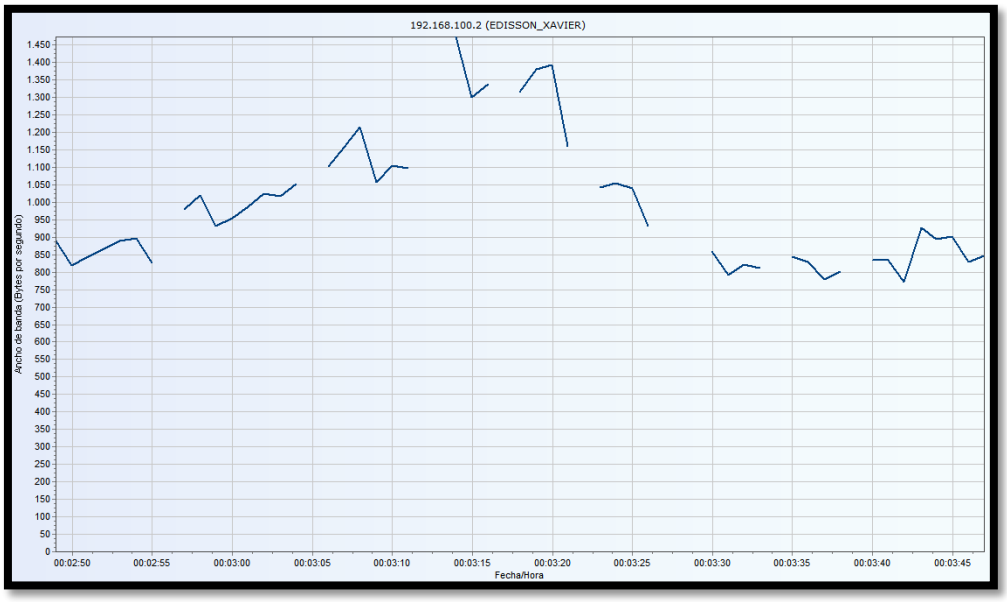
Paquetes:		
Enviados:	59	
Recibidos:	43	(73 %)
Perdidos:	16	(27 %)
Tiempo de respuesta (ms):		
Promedio:	2749	
Mínimo:	1816	
Máximo:	3146	



Prueba 5

- BW

Ancho de banda:	
Promedio	7 904
Mínimo	6 176
Máximo	11 784
Paquetes:	
Enviados	59
Recibidos	49
Perdidos	10



- Latencia

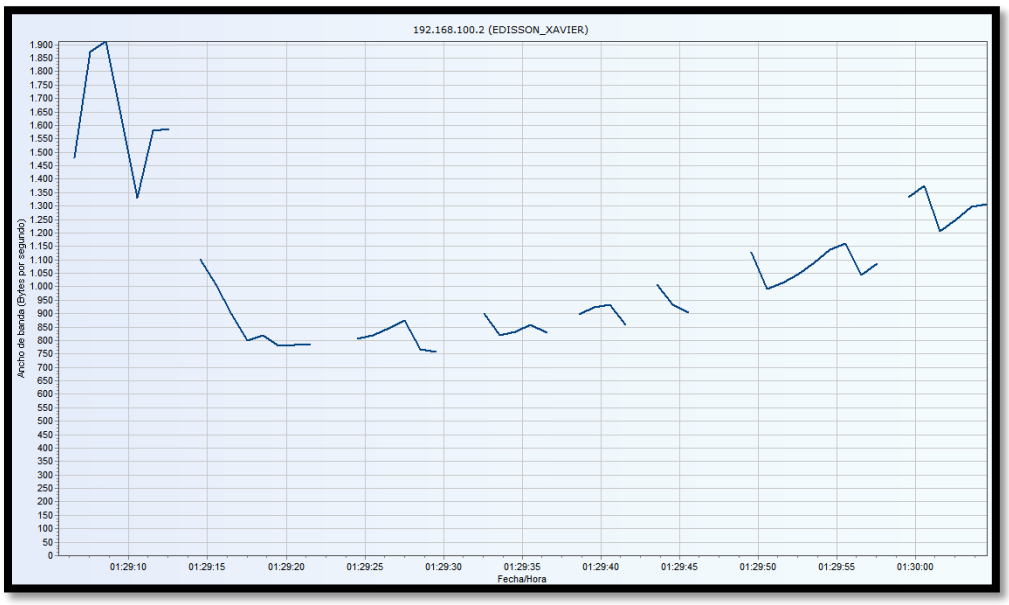
Paquetes:		
Enviados:	60	
Recibidos:	54	(90 %)
Perdidos:	6	(10 %)
Tiempo de respuesta (ms):		
Promedio:	2157	
Mínimo:	1404	
Máximo:	2744	

-

Prueba 6

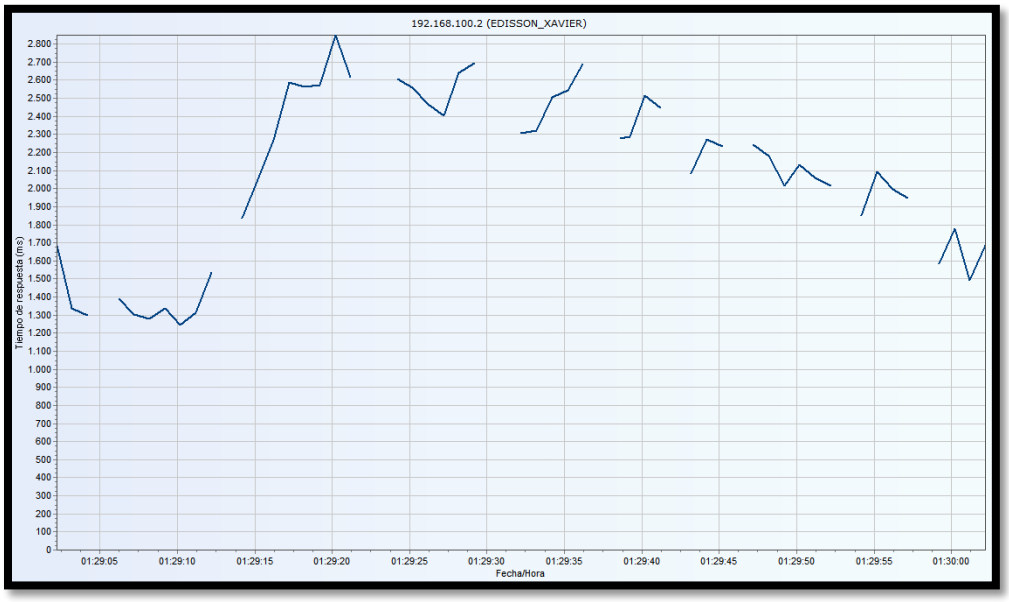
- BW

Ancho de banda:	
Promedio	8 548
Mínimo	6 056
Máximo	15 296
Paquetes:	
Enviados	60
Recibidos	49 (8
Perdidos	11 (1



- Latencia

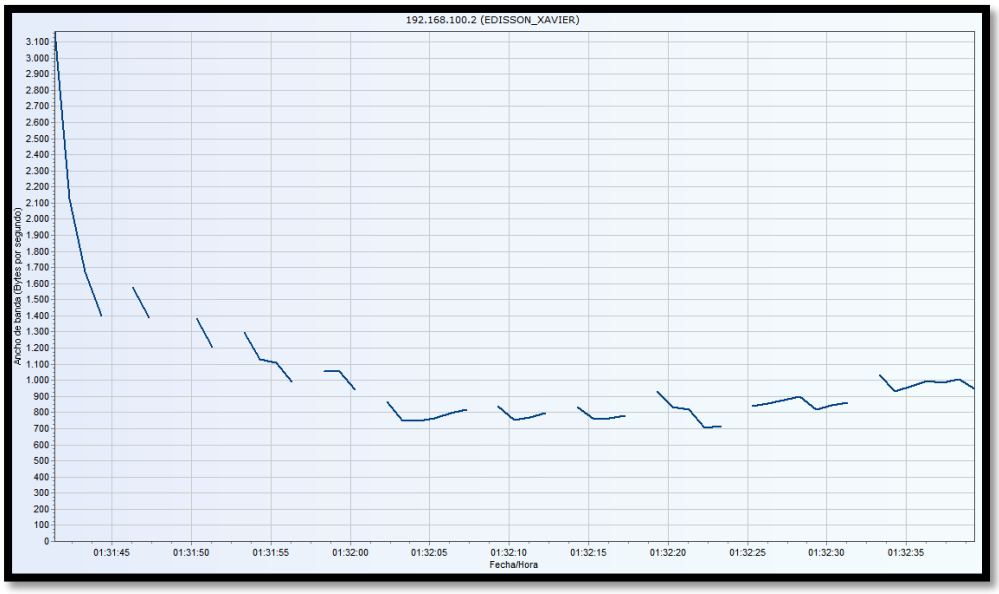
Paquetes:		
Enviados:	61	
Recibidos:	50	(82 %)
Perdidos:	11	(18 %)
Tiempo de respuesta (ms):		
Promedio:	2080	
Mínimo:	1246	
Máximo:	2849	



Prueba 7

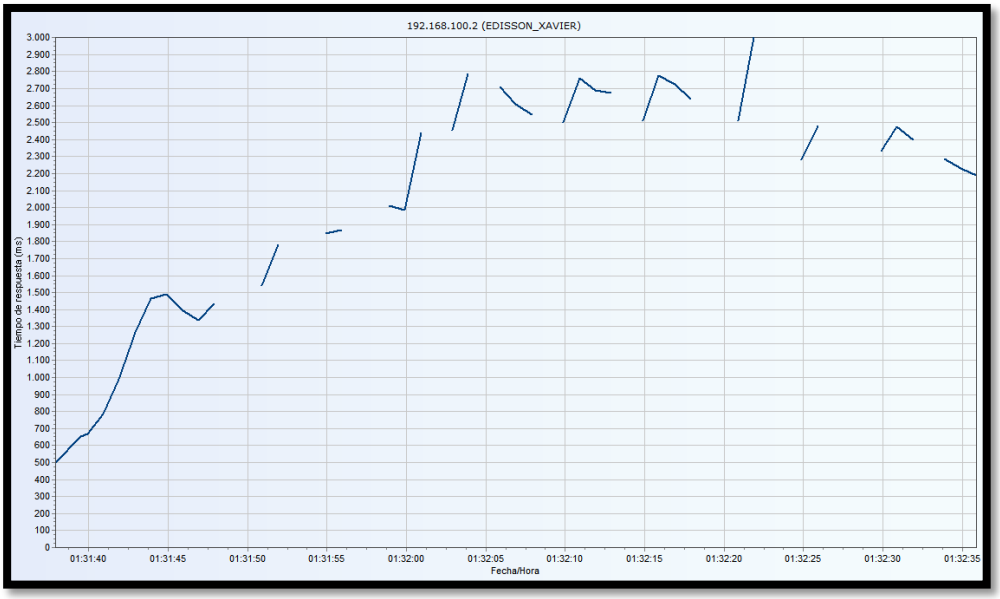
- BW

Ancho de banda:		
Promedio	8 233	
Mínimo	5 640	
Máximo	25 320	
Paquetes:		
Enviados	59	
Recibidos	48	(8
Perdidos	11	(1



- Latencia

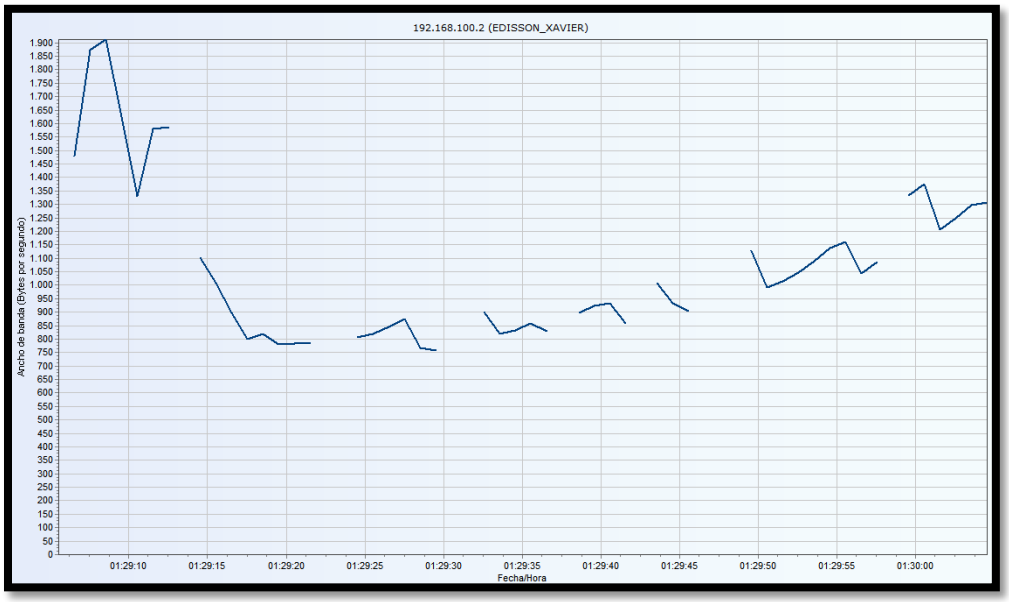
Paquetes:		
Enviados:	59	
Recibidos:	41	(70 %)
Perdidos:	18	(31 %)
Tiempo de respuesta (ms):		
Promedio:	2050	
Mínimo:	498	
Máximo:	3001	



Prueba 8

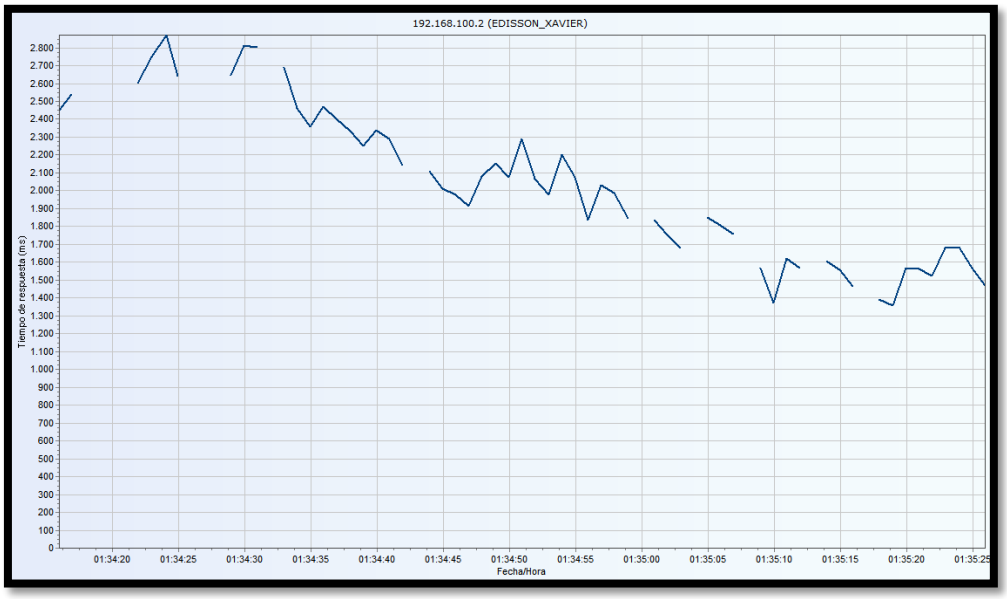
- BW

Ancho de banda:	
Promedio	8 548
Mínimo	6 056
Máximo	15 296
Paquetes:	
Enviados	60
Recibidos	49
Perdidos	11



- Latencia

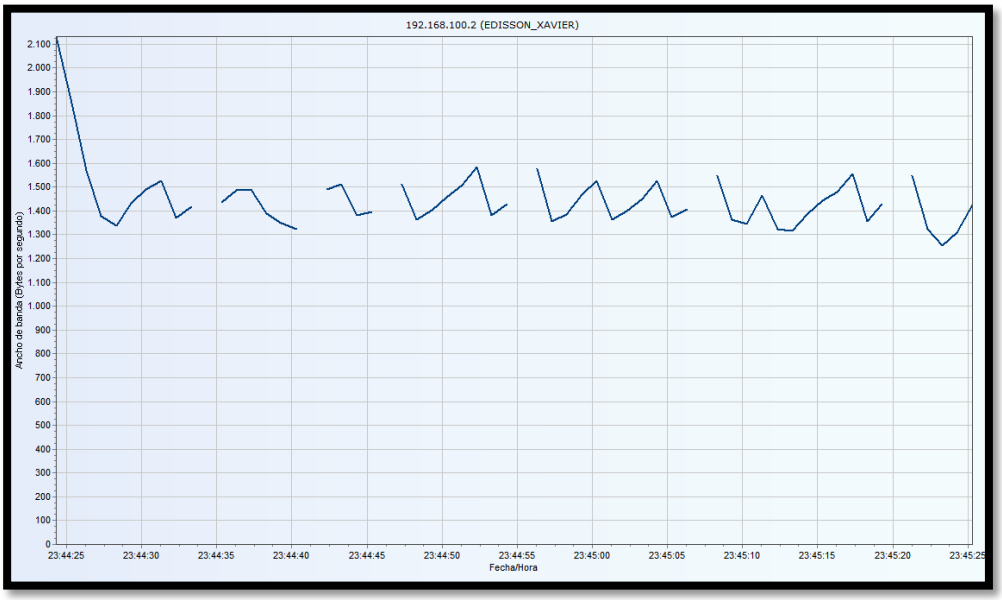
Paquetes:		
Enviados:	71	
Recibidos:	59	(83 %)
Perdidos:	12	(17 %)
Tiempo de respuesta (ms):		
Promedio:	2057	
Mínimo:	1356	
Máximo:	2871	



Prueba 9

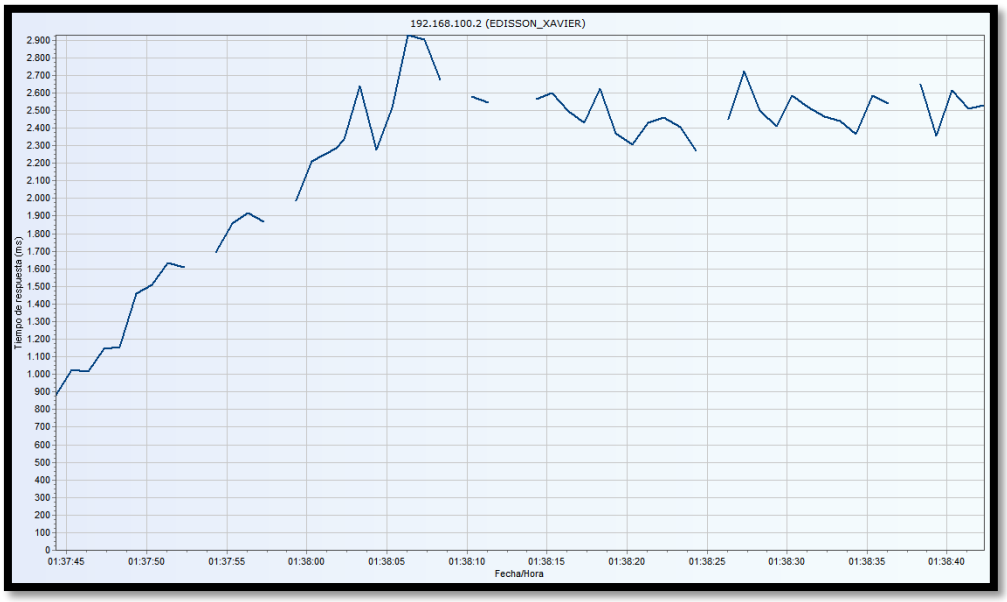
- BW

Ancho de banda:	
Promedio	11 587 l
Mínimo	10 040 l
Máximo	17 056 l
Paquetes:	
Enviados	62
Recibidos	56 (9
Perdidos	6 (1



- Latencia

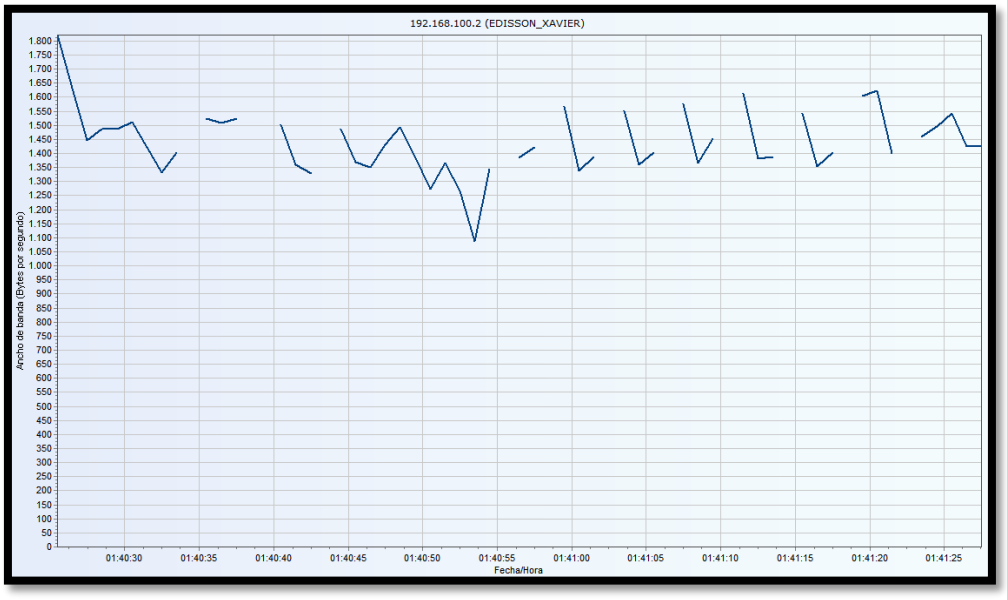
Paquetes:		
Enviados:	59	
Recibidos:	52	(88 %)
Perdidos:	7	(12 %)
Tiempo de respuesta (ms):		
Promedio:	2228	
Mínimo:	883	
Máximo:	2928	



Prueba 10

- BW

Ancho de banda:		
Promedio	11 547	
Mínimo	8 704	
Máximo	14 568	
Paquetes:		
Enviados	63	
Recibidos	51	(8
Perdidos	12	(1



- Latencia

Paquetes:		
Enviados:	59	
Recibidos:	53	(90 %)
Perdidos:	6	(10 %)
Tiempo de respuesta (ms):		
Promedio:	1389	
Mínimo:	632	
Máximo:	1753