UNIVERSIDAD CATÓLICA ANDRÉS BELLO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

IMPLEMENTACIÓN DE UN MODELO DE RED, PARA ACCESO Y TRANSPORTE MULTIPROPÓSITO Y MULTIFORMATO DESTINADO A MODERNIZAR LAS REDES DE SERVICIOS DE CANTV

TRABAJO ESPECIAL DE GRADO

presentado ante la

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

Como parte de los requisitos para optar al título de

INGENIERO EN TELECOMUNICACIONES

REALIZADO POR *Ricardo Anda Iturralde.*
Fernando García Rosell Foronda.

PROFESOR GUÍA *Ing. Pedro Fariña*

FECHA *Caracas, 24 de Septiembre de 2007.*

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

IMPLEMENTACIÓN DE UN MODELO DE RED, PARA ACCESO Y TRANSPORTE MULTIPROPÓSITO Y MULTIFORMATO DESTINADO A MODERNIZAR LAS REDES DE SERVICIOS DE CANTV

TRABAJO ESPECIAL DE GRADO

presentado ante la

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

Como parte de los requisitos para optar al título de

INGENIERO EN TELECOMUNICACIONES

REALIZADO POR *Ricardo Anda Iturralde.*
Fernando García Rosell Foronda.

PROFESOR GUÍA *Ing. Pedro Fariña*

FECHA *Caracas, 24 de Septiembre de 2007.*

UNIVERSIDAD CATÓLICA ANDRÉS BELLO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE TELECOMUNICACIONES

IMPLEMENTACIÓN DE UN MODELO DE RED, PARA ACCESO Y TRANSPORTE MULTIPROPÓSITO Y MULTIFORMATO DESTINADO A MODERNIZAR LAS REDES DE SERVICIOS DE CANTV

Este jurado; una vez realizado el examen del presente trabajo ha evaluado su contenido con el resultado: 20 (veinte)

J U R A D O E X A M I N A D O R

Firma:	Firma:	Firma:
Nombre: José Roldán	Nombre: Miguel Contreras	Nombre: Pedro Fariña

REALIZADO POR	*Ricardo Anda Iturralde.* *Fernando García Rosell Foronda.*
PROFESOR GUÍA	*Ing. Pedro Fariña*
FECHA	*Caracas, 24 de Septiembre de 2007.*

IMPLEMENTACIÓN DE UN MODELO DE RED, PARA ACCESO Y TRANSPORTE MULTIPROPÓSITO Y MULTIFORMATO DESTINADO A MODERNIZAR LAS REDES DE SERVICIOS DE CANTV

Anda, Ricardo

anda.iturralde@gmail.com

García Rosell, Fernando

fernandogrf@gmail.com

La serie Tellabs 8800 es una familia de enrutadores multi-servicio, con tecnología de próxima generación, desarrollados para trabajar con un alto desempeño cubriendo los requerimientos a nivel de proveedores de servicios. Los 8800 representan un camino para la migración hacia la convergencia de redes IP a través de las capacidades de Ingeniería de Tráfico del protocolo MPLS, valiéndose de características de las redes orientadas a la conexión como la Calidad de Servicio y seguridad, manteniendo las propiedades de escalabilidad y flexibilidad de las redes IP. Este Trabajo Especial de Grado demuestra y evalúa la funcionalidad de estos equipos como proveedores de una solución multiservicio para las redes de CANTV, con el fin de considerar su posterior implementación a nivel nacional. Esto se logró a través de la instalación de un modelo de red y la ejecución un protocolo de pruebas como parte de un proceso de homologación.

Palabras Claves: MPLS, Enrutadores Multi Servicio, Tellabs 8800, Homologación.

Dedicatoria

A mis padres,

a mi hermano,

a Andreína

y a la Amá.

Ricardo Anda

A mi papá y a mi mamá,

a Alejandro y Rafucho,

y a mi familia.

Fernando García Rosell

Agradecimientos

Queremos ofrecer nuestros agradecimientos a la empresa Eprotel, C.A y a toda su gente por permitirnos comenzar nuestro desarrollo profesional a través de la ejecución de este Trabajo Especial de Grado.

En especial queremos agradecer al Ingeniero Pedro Fariña por el apoyo brindado y por la confianza depositada en nosotros. Igualmente al Ingeniero Jonathan Polly por toda la ayuda y soporte ofrecido durante el desarrollo del proyecto.

Además, a la gente del laboratorio de CANTV por su cooperación, y a todos nuestros amigos de la universidad.

Índice General

Dedicatoria iv

Agradecimientos v

Índice General vi

Índice de Figuras y Tablas viii

Introducción 1

Capítulo I 3

Planteamiento del Proyecto 3
- I.1 Planteamiento del Problema 2
- I.2 Objetivos 2
  - I.2.1 Objetivo General 6
  - I.2.2 Objetivos Específicos 6
- I.3 Limitaciones y Alcances 7

Capítulo II 8

Marco Teórico 8
- II.1 Servicios Capa 2 9
  - II.1.1 ATM 9
  - II.1.2 Ethernet 12
  - II.1.3 Frame Relay 15
- II.2 Servicios Capa 3 16
  - II.2.1 OSPF 18
  - II.2.2 BGP 20
- II.3 Calidad de Servicio (QoS) y Clases de Servicio (CoS) 21
- II.4 Protocolo MPLS 22
  - II.4.1 Ingeniería de Tráfico en MPLS 26
  - II.4.2 Señalización y enrutamiento 29
- II.5 Redes VPN 32
  - II.5.1 Pseudowires y Service Interworking 34
  - II.5.2 Servicios de Red Privada Local (VPLS) 35
  - II.5.3 IP VPNs 36

Capítulo III 38

Metodología y Desarrollo 38
III.1 Investigación Preliminar 38
III.2 Ingeniería de Detalles 39
III.3 Desarrollo de Pruebas 40
III.3.1 Herramientas de Prueba 40
III.3.2 Configuración Inicial de Equipos 41
III.3.3 Configuraciones Básicas de las red MPLS 42
III.3.4 Servicios Capa 2 44
III.3.5 Servicios Capa 3 49
III.3.6 Interoperabilidad de Servicios 50
III.3.7 Calidad de Servicio (Qos) 52
III.3.8 Confiabilidad y Rendimiento 53

Capítulo IV 56

Resultados 56
IV.1 Configuración Inicial de Equipos 57
IV.2 Configuraciones Básicas de las red MPLS 61
IV.3 Servicios Capa 2 62
IV.4 Servicios Capa 3 67
IV.5 Interoperabilidad de Servicios 68
IV.6 Confiabilidad y Rendimiento 70

Capítulo V 72

Conclusiones y Recomendaciones 72
V.1 Conclusiones 72
V.2 Recomendaciones 73

Lista de Acrónimos 74

Bibliografía 76

Apéndice A 78

Ingeniería de Detalles 78

Índice de Figuras y Tablas

Figura 1. Red de Telecomunicaciones 4
Figura 2. Red de Telecomunicaciones propuesta 5
Figura 3. Formato de una celda ATM 10
Figura 4. Interfaces de red ATM 11
Figura 5. Agregación de cabecera MPLS 24
Figura 6. LSR's 25
Figura 7. Intercambio de Etiquetas en MPLS 25
Figura 8. Label Switch Path 26
Figura 9. Ejemplo de Ingeniería de Tráfico MPLS 28
Figura 10. Concepto General de Pseudowire 34
Figura 11. Modelo de Referencia Básico de VPLS 35
Figura 12. Servicio IP VPN 37
Figura 13. Red de gestión del modelo de red 42
Figura 14. Red MPLS y OSPF 43
Figura 15. Topología Servicio VPLS 45
Figura 16. Pseudowire Ethernet 46
Figura 17. Pseudowire ATM o Frame Relay 48
Figura 18. Red IP VPN 49
Figura 19. ATM / Ethernet Interworking propuesta 50
Figura 20. ATM / Ethernet Interworking 51
Figura 21. Red Ethernet / Frame Relay 52
Figura 22. Topología Prueba Throughput 55
Figura 23. Pantalla Inicial de Bienvenida Tellabs 8800 57
Figura 24. Versión de Software 8820 58
Figura 25. Versión de Software 8830 58
Figura 26. Estado de la tarjeta SCC en 8830 58
Figura 27. Estado ULCs en 8830 59
Figura 28. Estado PLMs en 8830 59
Figura 29. Alarmas en 8820 60
Figura 30. Alarmas en 8830 60
Figura 31. Tabla de nodos vecinos OSPF 61
Figura 32. MPLS habilitado en interfaz 8830 61
Figura 33. MPLS habilitado en interfaz 8820 61
Figura 34. Tabla de nodos vecinos RSVP 62
Figura 35. Ancho de banda disponible en el enlace troncal 62
Figura 36. LSPs configurados 62

Introducción

En la actualidad se ofrecen un gran número de servicios de telecomunicaciones que tienden a viajar sobre distintas plataformas y tecnologías; esto tiende a generar redes de telecomunicaciones complejas, como es el caso de CANTV. Este hecho motivó a la empresa EPROTEL, C.A. a ofrecer una solución que permitiera unificar la red de dicha compañía. Como etapa inicial de esta solución se encuentra la homologación de los equipos Tellabs 8800 en la red de CANTV, que representa el tema principal del trabajo especial de grado que se le invita a conocer.

Dicho trabajo está estructurado en 5 capítulos principales, los cuales se apoyan en apéndices para otorgarle mayor robustez.

El primer capítulo explica de forma concreta el problema que se presenta, seguido por los objetivos generales y específicos a buscar. A su vez hace referencia al alcance y limitaciones bajo los cuales está enmarcado este trabajo.

El segundo capítulo ofrece los conceptos y protocolos necesarios para entender el proyecto, aquí se le da mayor importancia al protocolo MPLS así como a redes VPN.

En el tercer capítulo; denominado metodología y desarrollo, se explican todos los pasos necesarios para ejecutar el trabajo especial de grado, así como se expone detalladamente lo que fue el desarrollo en sí. Aquí se especifican principalmente tres fases; la primera investigación preliminar, seguida por la ingeniería de detalles para terminar con la ejecución de las pruebas.

En el cuarto capítulo se muestran los resultados obtenidos después de haber realizado un conjunto de pruebas a un modelo de red propuesto. Estos resultados se exponen principalmente utilizando diferentes herramientas de la interfaz de línea de comando.

El último capítulo está constituido por las conclusiones a las que se llegó, las cuales están referidas a las funcionalidades de los equipos, así como a las ventajas que se pueden ofrecer a los proveedores de servicios de telecomunicaciones con el uso de los enrutadores multi-servicios Tellabs.

El principal apéndice presentado es el que muestra la ingeniería de detalles utilizada para desarrollar el proyecto.

Finalmente se presentaron todas las fuentes bibliográficas consultadas que sirvieron como base para soportar el proyecto. Adicionalmente se expone un glosario con los acrónimos utilizados donde se expone cada uno de sus significados.

Capítulo I

Planteamiento del Proyecto

I.1 Planteamiento del Problema

La velocidad de los cambios tecnológicos y la aceleración del fenómeno de Internet en los últimos años han afectado de manera significativa la industria de las telecomunicaciones, al punto que han surgido las llamadas redes de nueva generación o New Generation Networking (del inglés NGN), las cuales se basan en los principios y estándares fundamentales que dieron pie al fenómeno de Internet; es decir, el empaquetamiento asociado a los protocolos.

Internet ha cambiado al mercado así como al cliente, quien ahora tiene nuevas expectativas de comunicación debido a que la estandarización de la tecnología Internet Protocol (IP) ha impactado la oferta de servicios y reducido los costos de infraestructura. A su vez, los adelantos en electrónica y tecnología inalámbrica están transformando al negocio tradicional de las empresas de telecomunicaciones.

Entre las principales características de las NGN está su mayor capacidad para transportar datos, contrariamente a la red telefónica tradicional diseñada sólo para transmitir voz. Por otra parte, la red actual de banda ancha funciona hasta 1Mbps soportando muchos más servicios, pero aún así su capacidad es insuficiente.

En Agosto del año 2006 EPROTEL identificó en las redes de CANTV una necesidad importante para sus clientes. Se determinó que los mismos no solicitaban mayores velocidades en sus servicios de telecomunicaciones, bien por limitaciones en las tecnologías disponibles o bien por los altos costos que implicaban el uso de las aplicaciones existentes como Frame Relay o ATM. Como consecuencia de varias visitas de expertos de otras operadoras de telefonía fija e inalámbrica, se concluyó

que CANTV requería equipos que permitieran operar en distintas tecnologías, y que facilitaran productos y servicios a bajo costo para los usuarios finales.

En la actualidad, CANTV ofrece múltiples servicios sobre distintas plataformas y tecnologías, pero podría hacerlo de una moderna y mejor forma. La figura a continuación muestra un ejemplo del funcionamiento actual de las redes de Telecomunicaciones de CANTV.

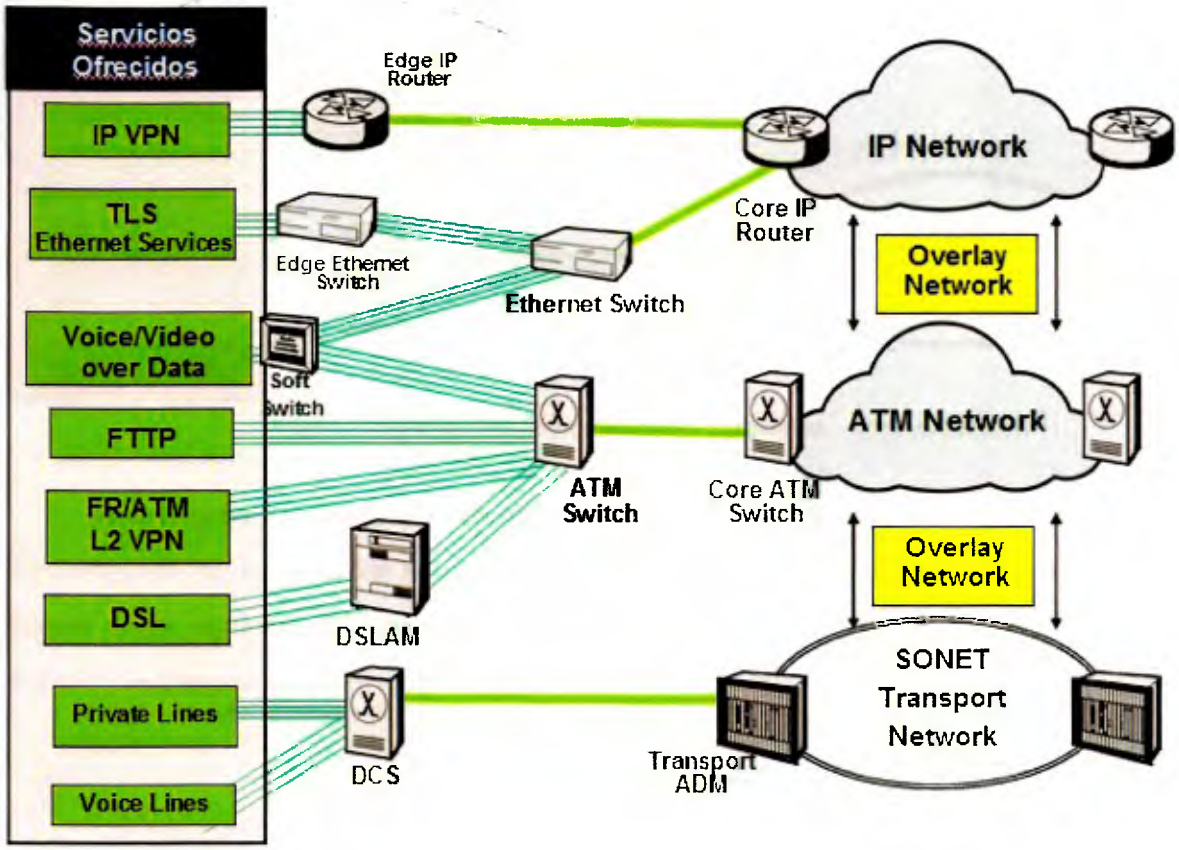


Figura 1. Red de Telecomunicaciones

En respuesta a esto se propuso presentar un modelo simulado de red que comprobara, en laboratorio de homologación y luego en la red operativa, sus ventajas con respecto a las redes existentes. La siguiente figura expone el modelo de red propuesto para mejorar las redes de telecomunicaciones de CANTV.

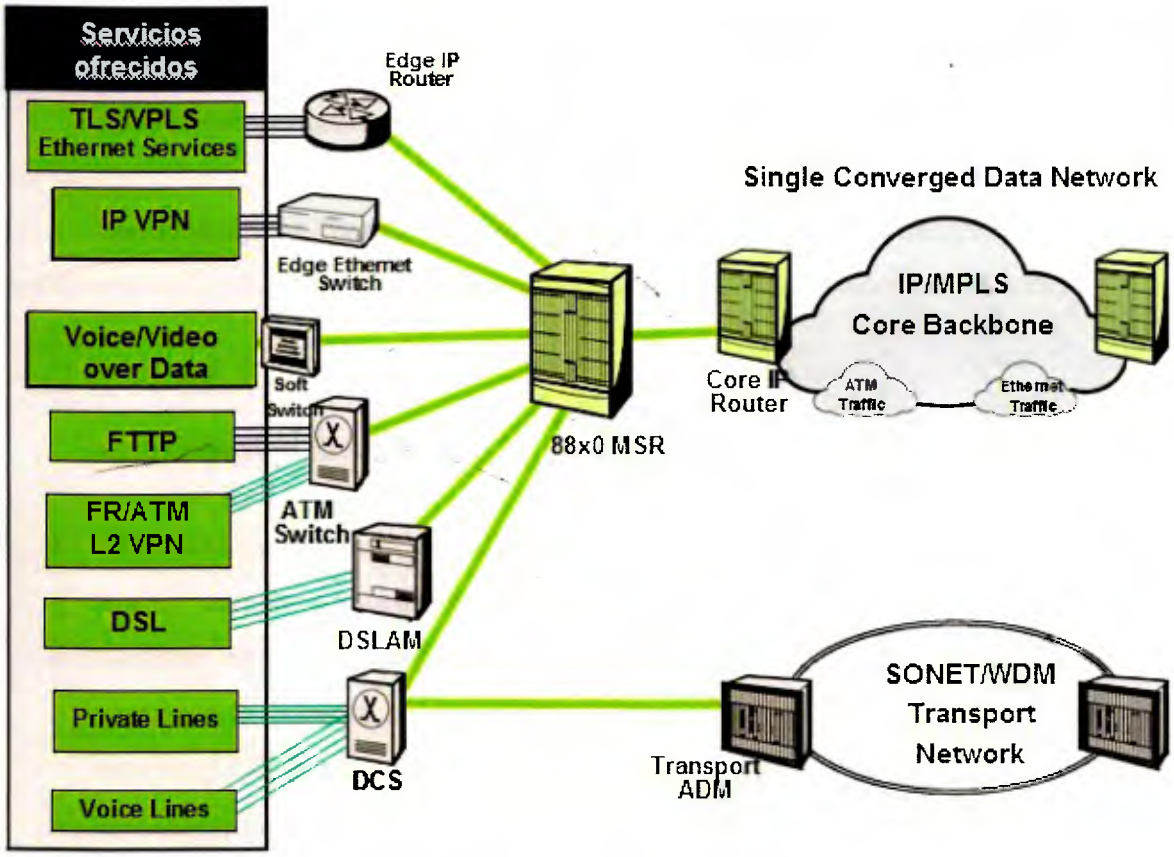


Figura 2. Red de Telecomunicaciones propuesta

En los actuales momentos se propone un proyecto cuyo inicio parte de la determinación de las pruebas de aceptación de este proceso de homologación, la procura de los equipos, su configuración en un sistema, el desarrollo práctico de las pruebas y la integración final en la red operativa de CANTV.

I.2 Objetivos

I.2.1 Objetivo General

Implementar un modelo de red, para acceso y transporte multipropósito y multiformato destinado a modernizar las redes de servicios de telecomunicaciones de CANTV.

I.2.2 Objetivos Específicos

- Determinar la topología, arquitectura de la red y protocolo de prueba
- Instalar equipos y accesorios necesarios para la interconexión del sistema.
- Realizar pruebas de configuración de los equipos, la red y los servicios mediante la interfaz de comandos de línea (CLI) y la interfaz gráfica de usuario (GUI) del sistema de gestión de red y servicios Tellabs 8000.
- Realizar pruebas de MPLS relacionadas con señalización (RSVP-TE), CAC, implementación de E-LSP y L-LSP.
- Realizar pruebas de funcionalidad y servicios de capa 2 y capa 3 que se pueden implementar con los equipos Tellabs 8800, tales como FR, ATM, Ethernet; creación de circuitos Pseudowires, IP VPN, VPLS y "Service Interworking" entre otros.
- Realizar pruebas de disponibilidad de los servicios y confiabilidad de los equipos, acordes con las facilidades de la solución "carrier-class" en cuanto a calidad de servicio (QoS) y las diferentes protecciones soportadas.

I.3 Limitaciones y Alcance

La implementación de la red de nueva generación se estima será colocada en una primera fase localmente en la sede principal de CANTV en Caracas. Para ello se emplearán equipos MPLS 8800 de la familia Tellabs.

Luego de verificar los resultados en función de las pruebas realizadas a nivel local y evaluando el desempeño del sistema, se estima implementar a nivel nacional. Cabe destacar que la implementación a nivel nacional está fuera del alcance de este Trabajo Especial de Grado.

Capítulo II

Marco Teórico

El comienzo de las transmisiones de datos representó un papel relevante en las comunicaciones del mundo informático. Desde entonces, la idea de una red única para los servicios de voz y datos ha sido uno de los principales objetivos dentro del área de las telecomunicaciones. En algunos países como Alemania, se realizó un primer intento por adaptar la transmisión de datos a la red tradicional de conmutación de circuitos, pero fracasó, dando paso a la tecnología de conmutación de paquetes.

Desde ese momento surgen protocolos como el X.25, luego Frame Relay, ATM, los cuales perseguían la integración de servicios sobre una única red de conmutación, como ya se había logrado para los medios de transmisión. Luego, "el mundo informático se vio convulsionado por la aparición del protocolo TCP/IP y por la utilización masiva de la red pública a escala mundial, Internet, basada en dicho protocolo" (Vidaurrazaga, 2004).

Hoy en día, la orientación en la industria apunta hacia la integración de servicios sobre las redes IP, utilizando el Multi Protocol Label Switching (MPLS), definido por Enrique Vázquez como "una tecnología flexible capaz de transportar voz, IPv4, IPv6, servicios capa-2 como Frame Relay, ATM, Ehternet e incluso PDH y circuitos SDH/SONET, sobre una infraestructura única de paquetes" (2004).

A continuación se explicarán algunos protocolos pertenecientes a la capa 2 y 3 del modelo OSI, seguidos por el tema principal de este trabajo especial de grado, el protocolo MPLS, finalizando con redes VPN y los diferentes tipos que existen.

II.1 Servicios Capa 2

La capa 2 o capa de enlace de datos se encarga principalmente de desplazar los datos por el enlace físico de comunicación hasta el nodo receptor, e identifica cada dispositivo ubicada en la red de acuerdo a su dirección de Hardware, que viene codificada en la tarjeta de red y es denomina dirección MAC (del inglés Media Access Control).

Diversos protocolos se caracterizan como pertenecientes a esta capa del modelo OSI (del inglés Open System Interconnection) y se diferencian por los servicios que ofrecen. Para este trabajo de grado fue necesario manejar los protocolos ATM y Ethernet principalmente así como Frame Relay; los cuales son explicados a continuación.

II.1.1 ATM

Según se describe en el artículo *What is ATM?* (Kerzhaw, 2001), ATM (del inglés Asynchronous Transfer Mode) es una tecnología desarrollada específicamente para permitir múltiples y diversos servicios con distintos requerimientos, transportados sobre una misma red de manera eficiente y efectiva. Es un protocolo de red, orientado a la conexión y basado en la conmutación de paquetes.

Esta tecnología ha permitido el desarrollo e integración de diferentes servicios como voz, datos y video, debido a las ventajas que ofrece frente a otros sistemas. Sin embargo, presenta algunas limitaciones que serán cubiertas por nuevas tecnologías, como MPLS, la cual ofrece una nueva ingeniería de tráfico combinando redes existentes, como la red ATM con la red de datagramas IP.

Algunas de las principales ventajas de ATM son:

- Integración de voz, datos y video.
- Provee ancho de banda por demanda.

- Por su escalabilidad, trabaja a distintas velocidades, por distintos medios, dejando abierta las posibilidades para desarrollar mejoras.

Sin embargo, presenta algunas desventajas como los complicados mecanismos necesarios para alcanzar Calidad de Servicio (QoS), ya que la infraestructura de ATM requiere de grandes desarrollos en software.

En el modelo de referencia OSI, el protocolo ATM se encuentra dentro de la capa 2. Debido a que es orientado a la conexión, requiere establecer un enlace punto a punto, o un canal virtual, antes de la transmisión. Los paquetes utilizados para el envió de información son denominados celdas *(cells)*, con un tamaño fijo de 53 octetos donde 5 pertenecen a la cabecera y 48 a la carga útil, como se muestra en la siguiente figura, tomada del texto *Redes ATM* (Mendillo, 2005).

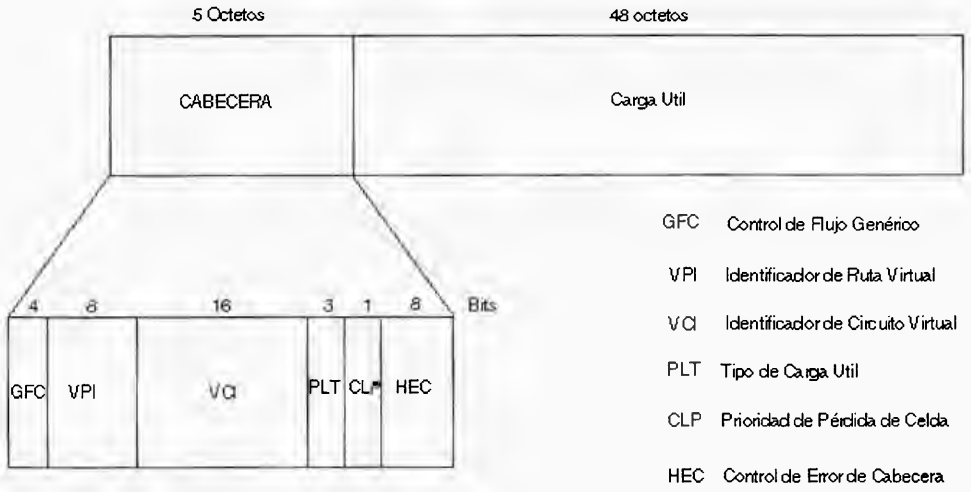


Figura 3. Formato de una celda ATM.

En el artículo *ATM Internetworking*, Anthony Alles describe el funcionamiento de una red ATM, el cual se expone a continuación.

Una red ATM consiste básicamente en un conjunto de conmutadores conectados a través de enlaces o interfaces ATM, de los cuales existen dos tipos: UNI (user-network interface) y NNI (network-node interface). Una interfaz UNI comprende nodos finales del sistema, como usuarios, enrutadores, mientras una

interfaz NNI representa cualquier enlace físico o lógico que conecta dos conmutadores ATM. En la siguiente figura se presenta el esquema de una red ATM.

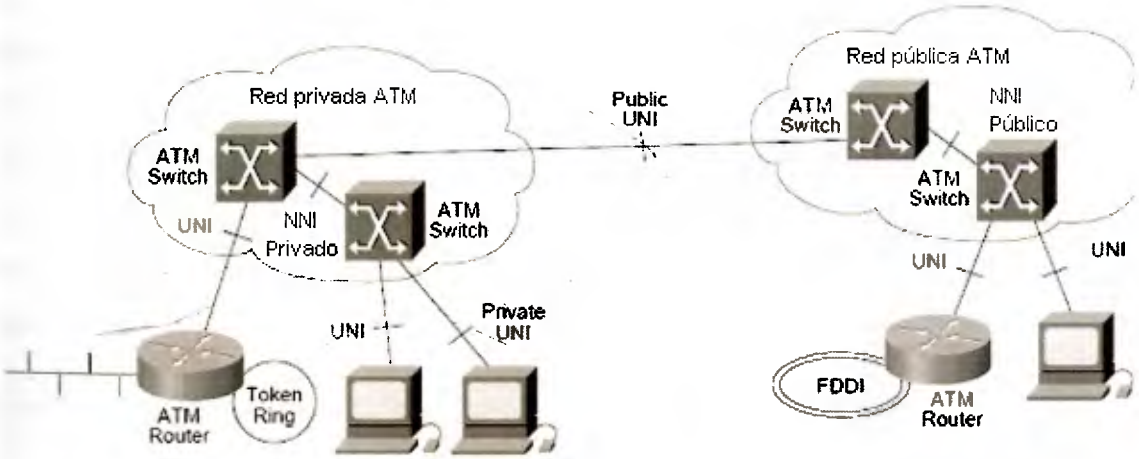


Figura 4. Interfaces de red ATM.

En ATM, se definen dos tipos de circuitos: los *virtual paths* o enlaces virtuales, identificados por los VPI (virtual path identifiers) y los *virtual channels* o canales virtuales, identificados por los VCI (virtual channel identifier). Básicamente, un switch ATM recibe una celda a través de un enlace con un VCI o VPI válido, busca en las tablas de conexión el puerto de salida y su correspondiente valor VCI/VPI y finalmente retransmite la celda. El sencillo funcionamiento del switch se debe a que las tablas de enrutamiento son preestablecidas por mecanismos externos, los cuales determinan dos tipos de conexiones ATM:

- *Permanent Virtual Connections* (PVC): establecidas por mecanismos externos, como administradores de red, en los que se preestablecen los valores VPI/VCI de los nodos fuente y destino conectados a la red. Este tipo de conexión siempre requiere configuración manual.

- *Switched Virtual Connections* (SVC): son determinadas de manera automática mediante protocolos de señalización. No requieren configuración manual, por lo que son más utilizadas que las PVC por los protocolos de las capas más altas.

Para optimizar el desempeño de ATM este puede ser mapeado sobre la jerarquía de sincronía digital o SDH (del inglés Synchronous digital Hierarchy). SDH viene a representar un conjunto de estándares que rigen las transmisiones sobre fibra óptica de forma tal de permitir la interoperabilidad entre fabricantes, así como de reforzar la estructura de la señal. La trama básica de SDH es el STM-1 (del inglés Synchronous Transport Module level 1), con una velocidad de 155Mbps. Cada trama va encapsulada en un tipo especial de estructura denominado contenedor. Una vez encapsulados se añaden cabeceras de control que identifican el contenido de la estructura.

II.1.2 Ethernet

Ethernet es una especificación inventada en los años 1970 por el centro de investigación de Xerox en Palo Alto; en la cual se utilizaba originalmente un canal compartido para transmitir información digital entre computadoras pertenecientes a una misma red de área local o LAN (del inglés Local Area Network). Posteriormente el canal se compartía a través de concentradores o Hubs, los cuales permitían que cada computador estuviera conectado a un puerto.

Como se describe en la guía de de Charles E. Spurgeon *Ethernet: The Definitive guide* (2000), Ethernet está compuesto por 4 elementos principales:

- El marco o frame: que es un conjunto de bits estandarizados usados para transportar información a través del sistema.
- El protocolo MAC: Consiste en conjunto de reglas en cada interfaz Ethernet, permitiendo que múltiples computadoras accedan al canal Ethernet para compartir información de una manera justa.
- Los componentes de Señalización: Son un conjunto de equipos electrónicos que envían y reciben señales sobre un canal Ethernet.

- El medio Físico: Todos aquellos cables y otros elementos de Hardware usados para transportar las señales digitales Ethernet entre los usuarios pertenecientes a la red.

De estos 4 elementos se hará referencia especial al protocolo de Control MAC, el cual es un conjunto de reglas utilizadas para controlar el acceso de un conjunto de estaciones al canal compartido. La forma en que trabaja este protocolo de acceso es relativamente sencilla. Cada computadora equipada con Ethernet opera independientemente de las demás estaciones de la red, donde no hay ningún controlador central. Todas las estaciones unidas al medio Ethernet half-duplex están conectadas a un canal de señalización, conocido como señal de bus.

Ethernet utiliza un mecanismo de transmisión en difusión en el cual cada paquete que es transmitido es escuchado por cada estación; a pesar que esto parezca ineficiente, simplifica el medio físico donde cada usuario es capaz de tomar los paquetes que le pertenecen a través de un proceso de comparación de direcciones, a pesar de esta simplicidad existe un potencial riesgo de seguridad debido a que muchas veces la data es enviada dentro de una la LAN sin ser encriptada. En una LAN Ethernet, todo lo que la señalización física debe hacer, es ver los bits transmitiéndose correctamente a cada estación, mientras las interfaces Ethernet se encargan de lo demás.

Las señales Ethernet son transmitidas desde la interfaz y son enviadas a través del canal compartido de señalización a cada estación conectada. Para enviar información una estación primero debe escuchar el canal y si el canal está desocupado la estación transmite su data en forma de un paquete Ethernet. A medida que los paquetes Ethernet son enviados a través del canal compartido todas las interfaces Ethernet conectadas al medio leen los bits de la señal y buscan la dirección MAC de destino, las interfaces comparan esta dirección con su propia dirección MAC unicast de 48 bits. La interfaz Ethernet para la cual las direcciones concuerdan

continuará leyendo el paquete y lo distribuirá al software de red que esté corriendo en esa computadora. Los demás usuarios dejarán de leer el paquete.

Después de cada transmisión de paquete, todas las estaciones en la red con tráfico por enviar deben competir de manera igual para la próxima oportunidad de transmisión. Esto asegura que el acceso al canal de la red sea justo. Un acceso justo al canal compartido se logra a través del uso del protocolo MAC existente en la interfaz Ethernet de cada estación.

El protocolo MAC usa otro protocolo denominado Carrier Sense Multiple Access with Collision Detection o CSMA/CD el cual es explicado en el libro *Catalyst LAN Switching* (Cisco, 2000) de la siguiente forma:

Aquel equipo que quiera transmitir sobre una red Ethernet primero deberá monitorear el canal para ver si está ocupado. Si el medio está libre transmite su información, en caso contrario tendrá que esperar que el nodo que ocupa el canal termine de enviar su data para comenzar su envío.

Si dos estaciones comienzan a transmitir al mismo tiempo se dice que ocurrió una colisión. Las colisiones pueden ser detectadas por todos los nodos porque reciben un voltaje superior al típico. Inmediatamente después de una colisión las estaciones involucradas transmiten una señal de congestión o jam para asegurar que todas las estaciones se enteren de la colisión de tal forma que no circule tráfico por la red. Los nodos que no estaban implicados en la colisión no transmitirán hasta que cese la colisión. Una vez que los nodos implicados terminan de transmitir la señal de congestión, establecen un tiempo aleatorio y comienzan una cuenta decreciente hasta cero. La primera estación en llegar a cero escucha el medio y detecta que está libre por lo cual comienza a transmitir. Cuando el contador de la segunda estación llega a 0 este equipo escucha el canal y detecta que la primera estación está transmitiendo por lo cual deberá esperar para enviar su información.

En el libro de Gilbert Held *Ethernet Networks* (2003) se explica que a pesar que cada tipo de red de área local presenta características diferentes referentes a su topología, método de acceso, método de señalización, medio de transmisión, entre otras; Ethernet representa una de las mejores soluciones al momento de implementar redes locales. Esto se debe entre otras cosas a que presenta una mezcla de diversas características de diferentes tecnologías las cuales se pueden implementar por una fracción del costo de cualquier otra red local. Otra de las características de Ethernet que la hace tan favorable es su escalabilidad y el constante esfuerzo de las empresas por desarrollarlo. Refiriéndose a la escalabilidad se pueden obtener equipos Ethernet que permiten operar una red originalmente a 10 Mbps y tener la opción de mejorar tu red hasta 100 Mbps e incluso 1 o 10 Gbps . Con respecto al esfuerzo de las empresas en los últimos años han surgido una gran cantidad de productos que les han permitido a los usuarios Ethernet mejorar su desempeño en la red así como el control de esta. Probablemente el producto más versátil es el conmutador Ethernet que permite múltiples conexiones entre estaciones y servidores, donde existirá interacción simultánea entre estos elementos, obteniéndose conexiones full duplex para cada dispositivo conectado al conmutador. Además el conmutador Ethernet presenta características muy importantes para manejar la red.

II.1.3 Frame Relay

En la guía de AT&T *Frame Relay Service in Today's Enterprise Network Environment* (1998) se denomina a Frame Relay como un protocolo que opera en la capa física y en la capa de enlace de datos del modelo OSI, capaz de proveer interconexión entre redes de área local (LAN) y redes de área amplia (WAN), a una alta velocidad, con confiabilidad y de forma económica.

Frame Relay utiliza conmutación por paquetes en donde se envían paquetes entre los distintos elementos de red utilizando técnicas estadísticas de multiplexación de paquetes para controlar el acceso a la red, esto otorga flexibilidad y un mejor uso del ancho de banda disponible.

En la guía de Cisco *Internetworking Technology Overview* (1999) se diferencian varios equipos Frame Relay los cuales entran en 2 categorías generales.

- Los equipos de terminación de data o DTE (del inglés Data Terminal Equipment), los cuales son equipos de terminación para determinadas redes y por lo general están ubicados en el cliente o cerca de él. Ejemplos de estos equipos son computadores personales, enrutadores, puentes, etc.

- Los equipos de terminación de circuitos de data o DCE (del inglés Data Circuit-Terminating Equipment), los cuales son propiedad de los proveedores de servicios y son los equipos que en realidad transportan la información a través de la WAN. Los DCE son los encargados de proveer los servicios de sincronización y conmutación en la red.

Para el funcionamiento de Frame Relay es necesaria la existencia de circuitos virtuales los cuales representan una conexión lógica creada entre dos equipos DTE a través de una red Frame Relay de conmutación de paquetes PSN (del inglés Packet-Switched Network).

Frame Relay ofrece una comunicación de enlace de datos orientada a la conexión, lo cual significa que una conexión existe entre cada par de dispositivos y que estas conexiones son asociadas con un identificador de conexión de enlace de datos o DLCI (del inglés Data Link Connection Identifier). Los valores de DLCI generalmente son asignados por el proveedor de servicios y tienen un significado local, lo que quiere decir que estos valores no son únicos en una WAN de Frame Relay.

II.2 Servicios Capa 3

La capa 3 o de red, según la normalización OSI, es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas.

En el programa de la Academia de Networking de Cisco *CCNA2: Principios básicos de routers y enrutamiento v3.1.1* se describe el enrutamiento como el proceso usado por los enrutadores para enviar paquetes a la red de destino. Durante este proceso un enrutador toma decisiones en función de la dirección IP destino de los paquetes de datos. Todos los dispositivos intermedios usan la dirección de IP de destino para guiar el paquete hacia la dirección correcta, de modo que llegue finalmente a su destino.

Para que los enrutadores tomen decisiones correctas estos deben aprender la ruta hacia las redes remotas, esto se puede lograr de dos formas:

- Utilizando enrutamiento estático: donde el administrador de la red configura manualmente la información acerca de las redes remotas, ó
- Utilizando enrutamiento dinámico: Donde las rutas se obtienen de otros enrutadores. Para obtener esta información es necesario utilizar protocolos de enrutamiento

Los protocolos de enrutamiento representan un esquema de comunicación entre enrutadores. Un protocolo de enrutamiento permite que un enrutador comparta información con otros enrutadores, acerca de las redes que conoce así como de su proximidad a otros enrutadores. La información que un enrutador obtiene de otro, mediante el protocolo de enrutamiento, es usada para crear y mantener las tablas de enrutamiento. Algunos ejemplos de protocolos de enrutamiento son:

- Protocolo de información de enrutamiento (RIP)
- Protocolo "Primero la ruta más corta" (OSPF)
- Protocolo de borde (BGP)

Otros tipos de protocolos importantes que se deben entender y diferenciar de los de enrutamiento son los enrutados; los cuales se usan para dirigir el tráfico

generado por los usuarios. Un protocolo enrutado proporciona información suficiente en su dirección de la capa de red, para permitir que un paquete pueda ser enviado desde un usuario a otro, basado en el esquema de direcciones. Algunos ejemplos de protocolos enrutados son:

- Protocolo Internet (IP)
- Intercambio de paquetes de internetwork (IPX)

Para el desarrollo de este trabajo de Grado se utilizaran principalmente los protocolos de enrutamiento OSPF y BGP, los cuales se explicarán a detalle a continuación; pero antes de estudiar estos protocolos se debe manejar el concepto de sistema autónomo o A.S (Autonomous System). el cual se define en el RFC 1930 como aquel conjunto de enrutadores que se encuentran bajo una única administración técnica y que utilizan un protocolo interno o IGP (del inglés Interior Gateway Protocol) para enrutar paquetes dentro de un mismo sistema autónomo y un protocolo externo o EGP (del inglés Exterior Gateway Protocol) para enrutar paquetes hacia otros sistemas autónomos.

II.2.1 OSPF

En el artículo de la IXIA *Open Shortest Path First (OSPF) Conformance and Performance Testing* (2004) se explica que OSPF surge con la finalidad de manejar tareas de enrutamiento dentro de un sistema autónomo, donde exista una convergencia rápida, un control mínimo del tráfico de enrutamiento y mejor seguridad.

OSPF es un protocolo de estado de enlace, lo cual quiere decir que se crea, se mantiene y se distribuye una base de datos de estados de enlace. Esta base de datos describe la información de los enrutadores dentro de un área OSPF. Dentro de esta información se encuentra las interfaces activas, como están interconectadas, y el costo de usar dicha interfaz. El costo representa la métrica utilizada para describir la

eficiencia relativa de varias rutas hacia un mismo destino. Cada enrutador es responsable por la creación de su propio trozo de topología a través de notificaciones de estado de enlace o LSA´s (del inglés Link State Advertisements), las cuales poseen información describiendo los enrutadores, rutas alcanzables, métricas, entre otros. Los LSA´s son distribuidos de forma confiable a los demás enrutadores dentro del área OSPF, lo que permite sincronizar la topología de bases de datos. Cuando todos los enrutadores tienen la misma base de datos de topología, cada enrutador puede calcular el camino más corto hacia los destinos utilizando el algoritmo de Dijkstra también llamado primero la ruta más corta, SPF (del inglés Shortest Path First).

Para lograr la sincronización de las bases de datos es necesario inundar toda la red con LSA´s, para disminuir este evidente problema OSPF maneja dos mecanismos.

- El primero es la utilización del enrutador designado o DR (del ingés Designated Router), este principio se basa en la elección de un enrutador al cual se le enviarán todos los LSA´s y este se encargará de distribuirlos por toda la red. Esto disminuye notablemente el tráfico de LSA´s pero a su vez crea un punto único de falla, lo cual se soluciona con la elección de un enrutador designado de respaldo o BDR (del ingés Backup Designated Router), el cual recibe todos los LSA´s pero se mantiene pasivo y solo entra en operación si el enrutador designado falla.

- El segundo mecanismos es la creación de las áreas OSPF mencionadas anteriormente, las cuales limitan la base de datos de topología únicamente a los enrutadores que se encuentran dentro de una misma área. Es decir los LSA´s generado por un enrutador sólo se difundirán a los enrutadores que pertenezcan a la misma área, por lo tanto existirá un enrutador designado y uno de respaldo para cada área OSPF. En OSPF siempre debe existir un área núcleo o de backbone la cual se denomina área 0 y es la encargada de interconectar todas las áreas, los enrutadores que interconectan áreas se

denominar enrutadores de borde de área o ABR (del inglés Area Border Router) y pertenecen a más de un área.

II.2.2 BGP

En el volumen 1 de la guía del estudiante de Juniper Networks, *Configuring Juniper Networks Routers* (2006), se clasifica al protocolo de entrada de borde o BGP (del ingés Border Gateway Protocol) como un protocolo de enrutamiento que trabaja entre varios sistemas autónomos. BGP intercambia información de enrutamiento entre diferentes sistemas autónomos, buscando crear una base de datos que permita mantener la conectividad entre diferentes redes.

Las rutas en BGP consisten en redes destino y al igual que en otro protocolos de enrutamiento en atributos asociados con esas rutas. Existe una diversidad de estos atributos los cuales deben ser aplicados en un determinado orden y a los cuales se les pueden aplicar varias reglas.

Una característica importante de BGP es que usa TCP (Transmission Control Protocol) como su protocolo de transporte, el cual le ofrece un proceso orientado a conexión y confiable. BGP considera una conexión entre dos entes como ociosa mientras no se establezca una conexión TCP.

BGP soporta dos tipos diferentes de intercambio de información .de enrutamiento EBGP e IBGP

- BGP externo o EBGP; en el cual la información es intercambiada entre sistemas autónomos. La conexión entre los dos sistemas autónomos consiste en una conexión física y en una BGP. La conexión física es un medio compartido en el cual cada uno de los sistemas autónomos tiene por lo menos un enrutador de borde. La conexión EBGP es establecida entre dispositivos directamente conectados debido a que el tiempo de vida de los

paquetes EBGP es de uno. La conexión BGP existe entre los enrutadores que hablen BGP en cada uno de los sistemas autónomos.

- BGP interno o IBGP, la información es intercambiada dentro del mismo sistema autónomo y por lo general la conexión es establecida entre direcciones loopbacks por razones de estabilidad. Las conexiones IBGP existen entre enrutadores remotos pertenecientes al mismo S.A que no necesariamente estén conectados directamente; por lo tanto es necesario la existencia de un protocolo interno de enrutamiento con el cual se pueda establecer la sesión BGP TCP.

II.3 Calidad de servicio (Qos) y Clases de Servicio (CoS)

Muchas veces los términos calidad de servicio o QoS (del inglés Quality of Service) y clases de servicio o CoS (del inglés Class of Service) no son usados de la mejor manera lo cual lleva a confundirlos, intercambiarlos y hasta a ser vistos como iguales. Por esto es importante definirlos de forma clara y concreta.

En el manual de Tellabs *TMOS QoS Application Manual* (2006) se describe QoS como el mecanismo capaz de describir los diferentes procesos implementados para entregar la información de una forma confiable. En general QoS provee los mecanismos para manejar la perdida de información, los retardos y la latencia.

Por otro lado CoS es el encargado de diferenciar el flujo de tráfico y los tipos de servicios para proveer el servicio requerido. En los equipos Tellabs 8800 existen 4 grupos principales de CoS, los cuales son:

- Tasa constante de bit o CBR (del inglés Constant Bit Rate); el cual es usado para el tráfico que requiere una cantidad de ancho de banda estático, continuamente disponible durante toda la conexión. Este tipo de tráfico soporta muy poco los retrasos

- Tasa Variable de Bit en Tiempo Real o VBR-rt (del inglés Real Time Variable Bit Rate); es usado para tráfico sensible al tiempo que tiene restricciones de retraso y se transmite a una tasa constante. Una aplicación típica de este tipo de CoS es video

- Tasa Variable de Bit en Tiempo No Real o VBR-nrt (del ingés Non Real Time Variable Bit Rate); es usado para el tráfico con tasas variables de transmisión y picos, pero que no tiene requerimientos de retraso. Ejemplos de este tipo de CoS son transferencias de archivos y sesiones de terminal

- Tasa de Bit no especificada, mejor esfuerzo o UBR (Unspecified Bit Rate); es usada para el tráfico que no requiere ninguna garantía de rendimiento de la red. Por lo tanto el tráfico está en riesgo en términos de QoS. Un ejemplo típico de UBR es el Internet.

En resumen QoS se diferencia de CoS en que QoS provee los mecanismos usados para que se haga cumplir el CoS asignado por la red. QoS es una de las principales virtudes que otorga el protocolo MPLS el cual es explicado en el siguiente punto

II.4 Protocolo MPLS

En la actualidad existe una gran demanda de ancho de banda debido a la transmisión de novedosos servicios. Esto ha generado un crecimiento exponencial en el tamaño de Internet el cual según el padre de Internet Larry Roberts se duplica cada dos meses. Por lo tanto los proveedores de servicios deben luchar para adaptar su infraestructura a los nuevos requerimientos del mercado para lo cual es necesario adoptar protocolos de conmutación y enrutamiento de alto desempeño.

En el artículo *MPLS - An Introduction to Multiprotocol Label Switching* (Nortel Networks, 2001) se explica que a pesar que la mayoría de los proveedores de servicios poseen núcleos bastante buenos basados en ATM, la conexión a estos proveedores continua siendo bastante lenta a través de enlaces Frame Relay y punto a

punto, agregando latencia y muchas veces cuellos de botella. Los enrutadores de la capa de núcleo también contribuyen a la latencia, debido al tiempo que tardan en tomar decisiones de envío para cada paquete que reciben.

IP ha estado enrutando utilizando métodos como IP sobre ATM y multiprotocolo sobre ATM los cuales han demostrado ser muy complicados. Por lo tanto es necesario un método más sencillo el cual abarque las características de control de tráfico de los conmutadores tradicionales combinado con la inteligencia de envío de un enrutador. Todas estas necesidades se pueden cubrir con MPLS.

MPLS es un mecanismo de transporte que fue estandarizado de forma abierta por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI por esto también es conocido como un protocolo de capa 2.5. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes, puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

En la guía de entrenamiento de Rick Gallagher *Building* Multiprotocol Label Swiching Networks (2003) se explica el funcionamiento del protocolo MPLS de la siguiente manera.

Primero es importante saber que el funcionamiento de MPLS está basado en agregar etiquetas a los paquetes de forma tal de poder designar diferentes clases de servicios o prioridades de servicios.

Para lograr esto es necesario un enrutador de borde LER (de las siglas en inglés Label Edge Router). El LER de forma muy general convierte los paquetes IP en paquetes MPLS y viceversa. Cuando los paquetes ingresan al LER este examina si los paquetes deben ser etiquetados, si la respuesta es afirmativa el LER se encarga de clasificar el tráfico entrante y lo relaciona con la etiqueta correcta, este proceso de clasificación se conoce por sus siglas FEC (del inglés Forward Equivalence Class) y

se basa en la dirección destino del paquete así como otros datos relevantes que contenga el paquete.

Para entender mejor como se agrega la cabecera, se presenta la figura 5, en la cual se muestran las capas del modelo OSI.

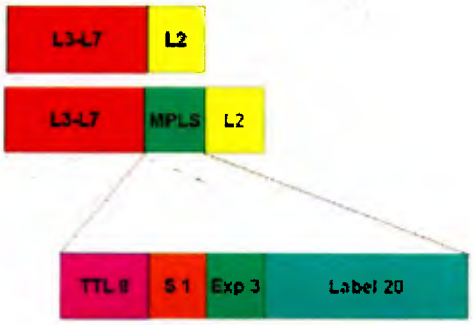


Figura 5. Agregación de cabecera MPLS

Cuando un paquete se presenta ante el LER, este coloca la cabecera MPLS entre las capas 2 y 3; por lo tanto no pertenece ni a la capa 2 ni a la 3 y de esta forma se presenta una forma a través de la cual se puede relacionar la información de capa 2 y 3.

Una vez que los paquetes abandonan el LER son dirigidos hacia los LSR (de las siglas en ingles label switch routers), los cuales son enrutadores que examinan los paquetes buscando etiquetas; el LSR busca en su tabla de envío conocida por sus siglas LIB (del inglés label information base) para obtener instrucciones. El LSR intercambia etiquetas de acuerdo a la información de la LIB. En la figura 6 se muestra como intervienen los LSR en una topología de red.

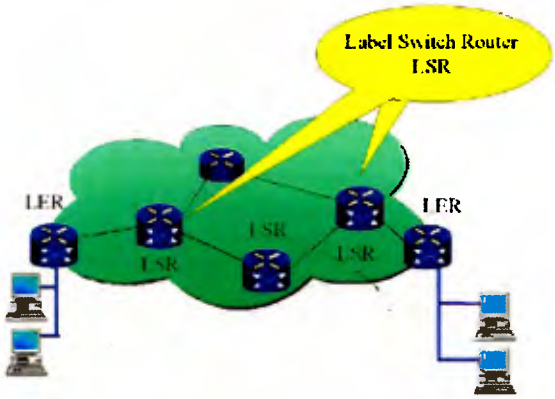


Figura 6 LSR´s

La función de los LSR es examinar los paquetes entrantes, verificar que una etiqueta está presente y enviar el paquete cumpliendo con las instrucciones que este contenga. En general los LSR realizan una función de intercambio de etiquetas, el cual está basado en la información que contiene el paquete, esto se puede observar en la figura 7.

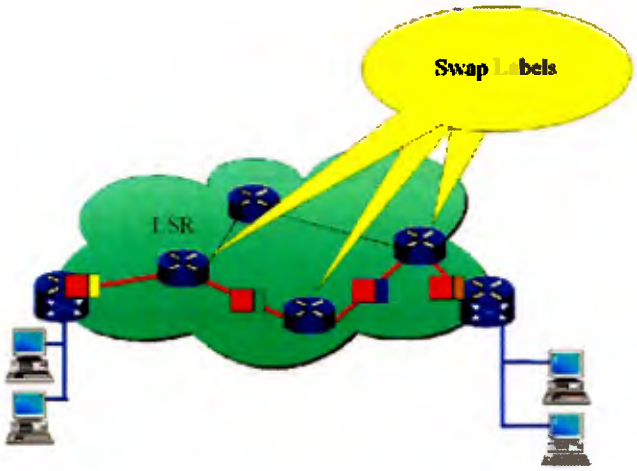


Figura 7. Intercambio de Etiquetas en MPLS

Entre los LER y los LSR se crean caminos, estos caminos se llaman LSPs (del inglés Label Switch paths) los cuales se muestran en la figura 8. Estos caminos son diseñados para características de tráfico, esto es muy parecido a la ingeniería de caminos de ATM. La capacidad de manejo de tráfico de cada camino es calculada.

Estas características incluyen carga, cálculo de porcentaje de paquetes perdidos, variación dentro de los paquetes; entre otros.

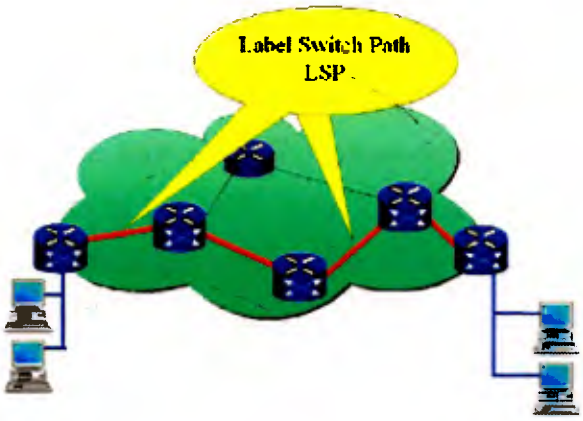


Figura 8. Label Switch Path

En el artículo de Asha Rahul Sawant y Jihad Qaddour *MPLS Diffserv: A combined approach* (2003) se explica la existencia de dos tipos de LSP's, el primero que se menciona es el E-LSP (EXP-LSP) en el cual los nodos deducen el tratamiento de Qos exclusivamente de la parte EXP de la cabecera MPLS, esto permite que diferentes tipos de tráfico puedan viajar dentro de una misma LSP permitiéndose hasta un máximo de 8 tipos de tráfico, debido a que el tramo EXP está compuesto por 3 bits. Luego se menciona L-LSP los cuales permiten sólo un tipo de tráfico o CoS.

Finalmente cuando los paquetes están saliendo de la red el LER le remueve al paquete la cabecera MPLS y envía el paquete hacia la red IP.

II.4.1 Ingeniería de tráfico en MPLS

En el artículo *Traffic Engineering with MPLS in the Internet* (Xiao, Hannan, & Bailey, 2000) se define Ingeniería de tráfico como el proceso que controla como el tráfico fluye a través de una red, de manera tal que se optimice la utilización de recursos y el desempeño de la red.

Para entender mejor cómo funciona la ingeniería de tráfico en redes basadas en MPLS el artículo *MPLS- An Introduction to Multiprotocol Label Switching* (Nortel Networks, 2001) primero explica los principios básicos del enrutamiento tradicional, enunciados a continuación.

En los ambientes con enrutamiento tradicional los paquetes son enviados a través de una red utilizando IGP´s o EGP´s basándose en un sistema salto a salto. Esto se logra comparando la dirección capa 3 con una tabla de enrutamiento de manera tal de obtener información para realizar el próximo salto. Posteriormente la dirección destino de capa 2 es reemplazada con la dirección de capa 2 del próximo salto y la dirección origen de capa 2 es sustituida con la dirección de capa 2 del enrutador actual; dejando la dirección capa 3 origen y destino igual, de forma tal que el próximo enrutador pueda determinar la ruta a seguir para alcanzar el próximo salto. Este proceso se repite cada salto hasta que el paquete alcance su destino final.

Para que un enrutador escoja cual es la mejor ruta para enviar un paquete tomará una decisión basándose en los atributos de selección que especifique ese determinado IGP. Esto ha proporcionado buenas soluciones cuando se trabaja dentro de un mismo sistema autónomo, pero cuando es necesario trabajar entre diferentes sistemas autónomos ha tenido ciertas limitaciones de enrutamiento, administración de red, ingeniería de tráfico y servicios IP escalables.

Por otra parte MPLS utiliza un método de envío de paquetes basado en intercambio de etiquetas. La idea más importante es que al LSR añadir etiquetas se puede enviar un paquete a través de una red de una forma mucho más eficiente debido a un simple elemento de envío a diferencia del enrutamiento tradicional que tiene una estructura más compleja basada en saltos.

La verdadera fortaleza del algoritmo de envío de MPLS es que el análisis de la cabecera IP sólo necesita hacerse una vez por el LER en el momento que el paquete ingresa al dominio MPLS. Una vez que el paquete completa el proceso de

FEC, el envío del paquete puede hacerse simplemente con las etiquetas usadas para un determinado LSP.

Para entender mejor estos principios el artículo *MPLS- An Introduction to Multiprotocol Label Switching* (Nortel Networks, 2001) se basa en la topología de la figura 9 y en la tabla LIB (Tabla 1).

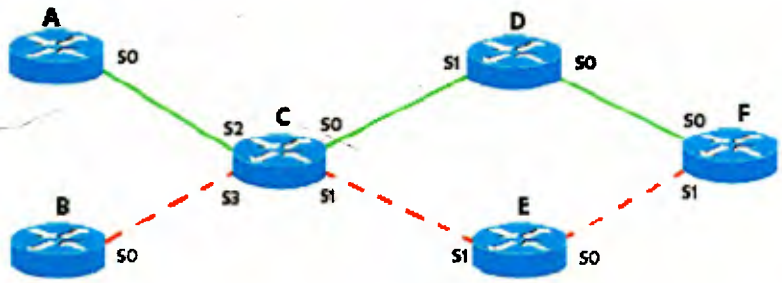


Figura 9. Ejemplo de ingeniería de tráfico MPLS

Interface IN	Label In	Destination	Exit Interface	Label Out
S2	50	F	S0	12
S3	45	F	S1	98

Tabla 1. LIB del enrutador

En la figura 9 se observa que al usar MPLS existe un control de cada paquete dentro de la red. Los paquetes destinados al enrutador F que provienen del A siguen el camino LSP representado por la línea continua, mientras que los provenientes del enrutador B serán enviados a través de la línea entre-cortada. Esto se logra al referenciar las etiquetas que entran al enrutador al LIB de manera tal que se obtenga el valor de la etiqueta de salida y de la interfaz de salida.

Los paquetes que ingresen al enrutador C por la interfaz S2 tendrán una etiqueta 50, los cuales serán referenciados a la LIB para que obtengan una información de envío. Basándose en esta LIB los paquetes que ingresaron por S2 con la etiqueta 50 serán intercambiados por una etiqueta 12 y serán enviados por la interfaz S0.

La fortaleza de controlar los patrones de tráfico de esta forma se vuelve aparente al compararlos con los IGP´s y EGP´s que envían sus paquetes basándose en decisiones de capa 3 y generalmente lo hacen sólo por aquellas rutas con la mejor métrica acumulada.

II.4.2 Señalización y enrutamiento

La arquitectura de MPLS no especifica el protocolo que debe utilizarse para la distribución de etiquetas entre distintos LSRs. La selección del protocolo que se implemente dependerá de los requerimientos específicos de la red.

De acuerdo al artículo *An introduction to Multiprotocol Label Switching* (Nortel Networks, 2001) LDP fue diseñado para tal fin, pero no contempló cubrir las necesidades en cuanto a QoS. De aquí surgen dos opciones: utilizar un protocolo de reservación de recursos y extenderlo para cubrir la distribución de etiquetas, o escoger un protocolo de distribución de etiquetas y utilizarlo para la reservación de recursos.

LDP (Label Distribution Protocol) consiste en un conjunto de procedimientos y mensajes con los que un LSR puede establecer LSPs a través de la red, con información sobre enrutamiento de las capas de red y capa de enlace. Sin embargo, establecer los LSPs no garantiza que se cumplan los requerimientos sobre QoS e ingeniería de tráfico, por lo que se desarrolla el protocolo CR-LDP (Constraint-based Routing over Label Distribution Protocol) buscando cubrir estas necesidades.

A su vez, existe el protocolo RSVP-TE (Resource Reservation Protocol-Traffic Engineering), basado en RSVP, el cual ofrece los mismos beneficios que CR-LDP pero con características que le permiten una mejor administración de la ingeniería de tráfico.

A continuación se expondrán las especificaciones; según el autor Rick Gallaher (2003), sobre cada uno de estos dos protocolos, en cuanto a señalización y aplicación de políticas de control de tráfico y control de carga en MPLS,

RSVP-TE

RSVP se define como un protocolo de control de red que permite a las aplicaciones conectadas obtener cualidades especiales de servicio para manejar el flujo de datos, reservando recursos como el ancho de banda. No es un protocolo de enrutamiento, pero trabaja en conjunto con ellos para el cálculo de listas de acceso dinámico en enrutadores.

El protocolo RSVP fue desarrollado por la IETF en 1997, principalmente para lograr cumplir los objetivos de CoS, aplicando teorías de señalización similares a las utilizadas por las conexiones telefónicas pero adaptadas a la transmisión de datos.

Fue diseñado para solicitar el ancho de banda requerido y las condiciones de tráfico en un enlace definido. Si se daban estas condiciones, el enlace sería establecido. En la primera versión del protocolo, existían tres tipos de enlaces denominados: Carga garantizada, Carga controlada y Carga mejor esfuerzo. Los recursos eran reservados mediante un proceso predefinido antes del establecimiento de la conexión.

Básicamente, para el establecimiento de un enlace entre dos puntos, una estación cliente solicita una ruta específica, con ciertas condiciones de tráfico y parámetros dados, incluidos en el mensaje de solicitud de conexión llamado *PATH*. En el momento en que la estación servidor recibe este mensaje, se responde al cliente y se reserva ese ancho de banda en la red con un mensaje *RESV*. Luego de recibir la confirmación del lado del cliente, se inicia la transmisión de datos a través de la ruta definida de punto a punto.

Este proceso de señalización se conoce como *soft state*, en el cual se elimina la conexión si no se refresca la información cada cierto tiempo ya establecido. Por lo tanto, el proceso de solicitud de conexión también se da mientras se transmiten datos.

Uno de los principales problemas de RSVP representa su escalabilidad, ya que mientras más enlaces son establecidos, se enviará una mayor cantidad de solicitudes de conexión, sobrecargando el tráfico de la red con estos mensajes.

RSVP-TE es el protocolo utilizado para el control e ingeniería de tráfico en MPLS, basado en RSVP, pero agregando algunas modificaciones:

- Se mantiene en estado *soft state* solicitando la retransmisión de mensajes para mantener el LSP establecido.
- Provee distribución de etiquetas por demanda de tráfico (*downstream-on-demand).*
- Reserva recursos en la red para LSP explícitos.
- Utiliza un procedimiento llamado *make-before-break* (crear antes de romper) para el re-enrutamiento de túneles LSP ya establecidos en caso de fallas en el enlace.
- Cuenta con otras características como Label-Request, Label, Record-Route (opcional) y Explicit-Route (opcional).

CR-LDP

A diferencia del LDP, este agrega campos al formato existente, llamados *peak, committed* y *excess-data rates*, similares a los utilizados en las redes ATM.

El procedimiento para el establecimiento de la conexión solo incluye dos pasos y es mucho más simple que para RSVP-TE, dado que es un protocolo tipo *hard*

state. Esto significa que una vez establecida la conexión no se romperá el enlace hasta que sea solicitada la desconexión.

La mayor ventaja de un protocolo *hard state* es su escalabilidad, ya que no se requiere del constante envió de mensajes de solicitud de conexión ocupando parte del tráfico en la red.

Algunas de las principales capacidades de CR-LDP son:

- Establece rutas de conexión permanentes al ser un protocolo de tipo *hard state*.
- Tanto la conexión como la desconexión de la ruta se realizan de forma explícita.
- Provee un mecanismo que permite reconocer todos los LSRs vecinos conectados directamente a través de mensajes multicast UDP.
- Es un protocolo desarrollado sobre uno ya existente, LDP, y permite la transmisión sobre TCP, mientras que RSVP-TE es un protocolo independiente.

II.5 Redes VPN

Una ventaja importante de MPLS es que permite proveer redes Privadas Virtuales o VPN´s (del inglés Virtual Private Networks) con altos grados de privacidad, seguridad y ancho de banda. Para entender mejor esto en el documento una *Red privada virtual: Una descripción general* (Microsoft, 1998) se describen los principales fundamentos sobre las redes VPN los cuales se explican a continuación.

Una VPN es aquella que conecta los componentes de una red sobre otra red. Las VPNs logran esto al permitir al usuario hacer un túnel a través de Internet u otra

red pública de tal forma que permita a los participantes del túnel disfrutar de la misma seguridad y funciones que antes sólo estaban disponibles en las redes privadas.

Al utilizar VPNs, los usuarios que trabajan en el hogar o en el camino pueden conectarse en una forma segura a un servidor corporativo remoto utilizando la infraestructura de enrutamiento que proporciona una red pública como Internet. Desde la perspectiva del usuario, la VPN es una conexión de punto a punto entre la computadora del usuario y un servidor corporativo. La naturaleza de la red intermedia es irrelevante para el usuario, debido a que aparece como si los datos se estuvieran enviando sobre un enlace privado dedicado.

La tecnología de VPNs también permite que una compañía se conecte a las sucursales o a otras compañías (Extranets) sobre una red pública (como Internet), manteniendo al mismo tiempo comunicaciones seguras. La conexión de la VPN a través de Internet opera de manera lógica como un enlace de Red de área amplia entre los sitios. En ambos casos, una conexión segura a través de la red aparece ante el usuario como una comunicación de red privada, a pesar del hecho de que esta comunicación sucede sobre una red pública, de ahí el nombre Red Privada Virtual.

En este trabajo de grado se utilizaron tres tipos de VPN´s.

- Pseudowires
- Servicios de red privada local o VPLS (del inglés virtual Private LAN service)
- IP VPN´s

Dichos tipos de VPN serán explicados en puntos posteriores.

II.5.1 Pseudowires y Service Interworking

Los Pesudowires, se definen en el artículo de *Riverstone Networks MPLS/VPLS Evolution: A Riverstone Perspective* (2006) como configuraciones de conexiones punto a punto entre pares de enrutadores de borde de proveedores o PE (del inglés provider edge routers). Cuya principal función es proveer capacidades adicionales de separación de tráfico entre clientes, lo cual permite multiplexar el tráfico de diferentes clientes dentro de un túnel de transporte.

Esta posibilidad de multiplexar permite emular diferentes servicios como ATM, Frame Relay, Ethernet y TDM sobre un túnel MPLS el cuál se configura bien sea con los protocolos de control RSVP-TE o LDP.

Para emular los servicios ATM, Frame Relay, Ethernet y TDM cada uno de ellos debe ser encapsulado bajo un formato común de MPLS. Al encapsular servicios bajo un formato común de MPLS, los pseudowires permiten a los portadores converger sus servicios hacia una red MPLS. El concepto general de Pseudowires se muestra en la figura 10.

Figura 10. Concepto general de Pseudowire

Para que la emulación de estos servicios no se limite a servicios iguales en ambos extremos es necesario la existencia de la interoperabilidad de servicio o Service Interworking lo cual según el artículo *Gigabit Ethernet and ATM Interworking* (Spirent, 2001), permite que dispositivos y sistemas con protocolos y velocidades diferentes puedan operar. Para que exista una buena interoperabilidad se deben cubrir 3 objetivos principales:

- El primero es lograr cambiar la información de un tipo de tecnología a otro sin que hayan pérdidas de encabezados de paquetes y sin alterar la integridad de la información.

- El segundo es lograr una alta eficiencia la cual viene representada por una alta tasa de transmisión de paquetes con un bajo retardo

- El tercero es garantizarle el servicio al cliente sobre todo en aquellas tecnologías que no soportan calidad de servicio, como es Ethernet.

II.5.2 Servicios de red privada local o VPLS

La encapsulación de Ethernet con pseudowires es la base principal de las VPLS (del inglés Virtual Private LAN Services). El modelo de referencia básico para VPLS es el que se muestra en la figura 11.

Figura 11. Modelo de Referencia básico de VPLS

Los clientes están conectados a través de la red de un proveedor de servicios. Se puede entender que esta red funciona como un conmutador capa 2 capaz de aprender y envejecer. Los clientes se conectan a la red del proveedor de servicios a través de un PE. Todos los PE´s en la red están conectados bajo una topología de túneles completamente interconectada (full-mesh) donde cada túnel transporta múltiples pseudowires; uno por cada servicio ofrecido entre PE. Dependiendo de la

ubicación y en la cantidad de clientes, el número de configuraciones de pseudowires para el servicio de un cliente puede variar entre 1 (cliente con solo 2 locaciones) hasta una topología de interconexión total (cliente con locaciones conectadas a cada PE).

Cada PE en la red es capaz de configurar túneles para cada PE y de señalizar pseudowires que atraviesan esos túneles. Como la red principal ofrece un servicio al usuario que se entiende como capa 2, cada PE es capaz de aprender todas las direcciones MAC conectadas así como de asociar las direcciones remotas aprendidas a través de un pseudowire. Todos los paquetes desconocidos unicast, multicast y broadcast son inundados hacia todos los PE participantes.

Este modelo de red asume que todos los PE´s dentro de un servicio están conectados bajo una topología de pseudowires completamente interconectada. Por lo tanto, para asegurar que la topología es libre de lazos se requiere un concepto similar al de horizonte dividido en el cual ningún PE enviará paquetes que recibe de cualquier PE a otro PE.

II.5.3 IP VPN´s

Según el TMOS User Manual (2006) de Tellabs una IP VPN es un servicio que enruta tráfico de áreas geográficas de clientes separados por una nube MPLS de un proveedor de servicios. En este modelo BGP distribuye la información de enrutamiento hacia afuera de la nube MPLS, mientras que MPLS enruta tráfico entre los bordes de la nube MPLS y el núcleo de la nube MPLS.

En la figura 12, se muestran 3 áreas geográficas de un mismo cliente separadas por una red MPLS

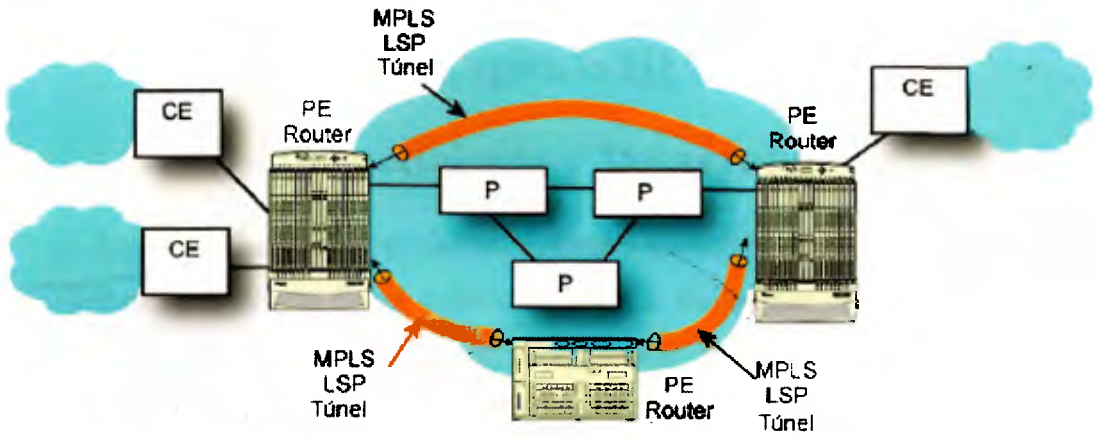


Figura 12. Servicio IP VPN

Los extremos del cliente o CE (del inglés Customer Edge) pueden utilizar rutas estáticas o un IGP para intercambiar información de enrutamiento y poder enviar tráfico hacia los extremos del proveedor de servicios o PE (del inglés provider edge). Los PE intercambian información de enrutamiento de VPN con otros PE utilizando IBGP, los proveedores o P están localizado en el núcleo de la red MPLS del proveedor de servicios. Los enrutadores PE manejan la información de enrutamiento de las VPN en la forma de una tabla de envío de rutas VPN´s y deciden cual túnel LSP tomar para un destino determinado, de esta forma se alivian las tareas del CE. Debido a esto muchas veces la nube MPLS; cuando se configura IP-VPN´s, es vista como un enrutador.

Capítulo III

Metodología y Desarrollo

Los objetivos del presente Trabajo Especial de Grado comprenden principalmente el diseño de un modelo de red y la realización de diferentes tipos de pruebas a este modelo. Por el tipo de investigación a realizar, y para lograr definir cada una de las pruebas de manera eficiente, se estableció una metodología con las siguientes fases:

1. Investigación Preliminar
2. Ingeniería de Detalles
3. Desarrollo de pruebas

Se inició el desarrollo del Proyecto con una etapa de investigación que permitió diseñar de manera concreta las pruebas a realizar, seguida de la Ingeniería de Detalle, en la cual se definieron todos los puntos necesarios para concluir con la ejecución de las pruebas. A continuación se detallan cada de una de estas tres fases.

III.1 Investigación Preliminar

Con el fin de alcanzar un diseño de pruebas ajustado a los objetivos que se desean lograr, se establecieron dos pasos dentro de la etapa de investigación:

- *Investigación Documental.* Comprende la recopilación y asimilación de teorías y conceptos referidos al modelo de red, como estándares, tecnologías y protocolos a utilizar, así como los servicios que la red puede ofrecer. También incluye información técnica con respecto a los equipos bajo prueba, obtenida a partir de los manuales del fabricante.
- *Investigación de Contexto.* Consiste en la recolección de información relacionada con la instalación del modelo de red, así como la delimitación del diseño bajo ciertos parámetros y lineamientos establecidos entre EPROTEL,

C.A. y CANTV a través de un "*Protocolo de Pruebas*". Este documento detalla las configuraciones necesarias que se deben realizar a los equipos paso a paso, topologías de red, entre otros. En esta etapa de la investigación también se recogió información sobre la instalación física de los equipos que posteriormente es reflejada en la Ingeniería de Detalles.

III.2 Ingeniería de Detalles

Una vez se obtuvo información sobre los equipos a utilizar en el modelo de red y sobre la configuración que se debía realizar en los nodos, se elaboró una Ingeniería de Detalle (Apéndice A) con el fin de reducir el tiempo empleado en el proceso de instalación de la maqueta y optimizar el desarrollo de las pruebas.

Este documento contiene a nivel general tres secciones:

- *Descripción de equipos.* En esta sección se describen las unidades de la serie Tellabs 8800 que se emplean en el proyecto, incluyendo tarjetas y módulos. Se presentan características físicas como dimensiones, peso, alimentación, así como funcionalidades de cada una.
- *Instalación.* Contiene todas las especificaciones necesarias para llevar a cabo la instalación de la maqueta en la sede de CANTV. Estas incluyen características mecánicas, de alimentación y aterramiento, como longitudes y tipo de cableado, consumo de energía, conectores, etc. Además presenta planos del rack y fotografías del lugar que indican los recorridos de cableado.
- *Configuración.* Dado que la configuración de ambos nodos se efectúa vía línea de comando (CLI), se detallan en esta sección, para cada prueba, los puertos utilizados en las conexiones y otros parámetros obtenidos a partir del *Protocolo de Pruebas*.

III.3 Desarrollo de Pruebas

Esta fase especifica los objetivos perseguidos en cada prueba, una descripción de la misma que incluye la topología de red con todos los elementos y conexiones a utilizar, resultados esperados y las herramientas utilizadas para su desarrollo.

III.3.1 Herramientas de prueba

Se describen a continuación los equipos, herramientas y comandos principales utilizados para realizar las mediciones y pruebas sobre el modelo de red.

- *FrameScope Pro Agilent.* Este instrumento permite realizar análisis y mediciones de rendimiento en los equipos activos dentro de una red Ethernet. Puede trabajar con conexiones desde 1 Mbps hasta 1 Gbps a través de fibra óptica o cable UTP para transmisiones no mayores a 100 Mbps. Puede ser utilizado como generador de tráfico o para realizar pruebas de rendimiento como el RFC 2544, el cual será explicado con detalle posteriormente.
- *Computadores.* Son utilizados dos computadores para las pruebas que involucren redes Ethernet y no requieran de configuración de interfaces VLAN. Con ellos es posible generar tráfico con las capacidades de conexión de red del sistema operativo Windows.
- *Ping.* Este comando es utilizado para probar conectividad a nivel de capa 3, indicando la dirección IP que se desea alcanzar. Puede ejecutarse desde los FrameScope, los computadores o los mismos equipos 8800. También existe el ping extendido, que envía paquetes de forma continua hasta que sea detenido por el usuario.
- *OAM-ping Ethernet* (Operation and Maintenance ping). Es una herramienta que proveen los equipos 8800 para comprobar conectividad a nivel de capa 2 y que permite detectar fallas en los enlaces. Puede ser utilizada entre interfaces que formen parte de un VPLS, indicando la dirección MAC del puerto que se desea alcanzar.

- *OAM-ping ATM.* Permite detectar fallas presentes en enlaces virtuales y canales virtuales en circuitos ATM. Este comando es generado desde los equipos 8800 indicando la interfaz ATM del nodo local por la que se enviará este ping, y el numero de VPI/VCI (Recomendación ITU-T I.610)
- *Traceroute.* Es similar al ping, pero este indica todos los saltos o enrutadores que debió atravesar para llegar a la dirección IP señalada, sugiriendo posibles fallas en la ruta en caso de que existiesen.
- *Rolling-Counters.* Este comando permite en los equipos 8800 verificar estadísticas de transmisión con respecto a una interfaz, un LSP o un circuito. Puede mostrar contadores de paquetes recibidos, enviados, o descartados y en ciertos casos especificar la razón por la cual se generó un error y no se procesó el paquete. Estos valores pueden tomarse en un intervalo de tiempo dado o mostrarse en tiempo real.

III.3.2 Configuración Inicial de Equipos

Previo a cualquier configuración de servicios que se realice en los equipos, se deben cubrir todos los pasos descritos en el documento *Acceptance Test Manual* (2006) proporcionado por el fabricante Tellabs, con el fin de verificar el estado de todos los componentes de hardware y que la última versión del sistema operativo haya sido instalada. Esta prueba se efectúa para descartar posibles fallas en alguno de los componentes y en caso de que existiese alguna, esta pueda ser notificada al fabricante con suficiente antelación a la instalación del modelo de red para tomar la acción que sea necesaria.

También se modificaron otros parámetros como cuentas de usuarios y contraseñas, lo cual es obligatorio para acceder al equipo, configuración de hora y fecha, nombre del nodo y parámetros de la interfaz de gestión.

Las pruebas de configuración inicial fueron realizadas con un computador conectado directamente al equipo a través del puerto serial. Sin embargo, para el resto

de las pruebas, el acceso al equipo se realizó a través de la interfaz de gestión, como se muestra en la figura 13. Las direcciones IP de gestión fueron asignadas por CANTV, para hacer posible el acceso remoto.

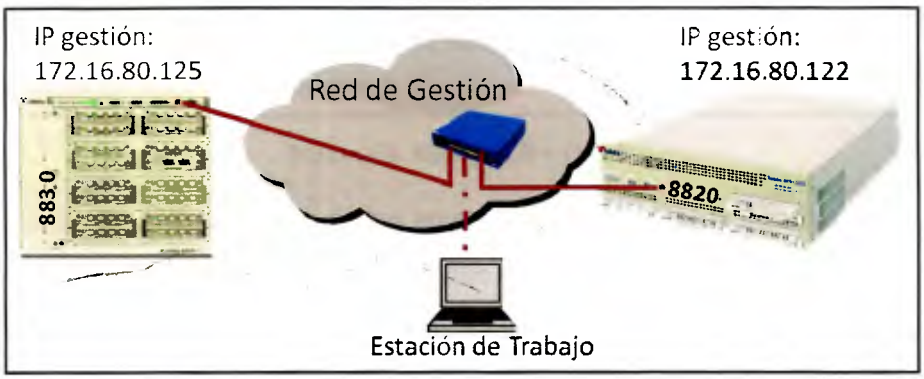


Figura 13. Red de gestión del modelo de red

III.3.3 Configuraciones Básicas de la red MPLS

Una vez verificado el estado de los equipos, se realizaron las primeras configuraciones de red de forma global, y luego de manera específica en cada puerto e interfaz a utilizar de cada nodo, que luego permitieron levantar los servicios que ofrece el sistema.

MPLS, OSPF e Ingeniería de Tráfico

En la figura 14 se muestra la topología de la red IP/MPLS configurada, la cual cuenta con dos equipos TELLABS MSR 8800 conectados entre sí a través de un enlace GigaEthernet. Antes de levantar los protocolos de enrutamiento, se establecieron las direcciones de loop-back en cada nodo, que a su vez fueron utilizadas como identificadoras del enrutador para OSPF (*router_id)* y MPLS (*lsr_id*).

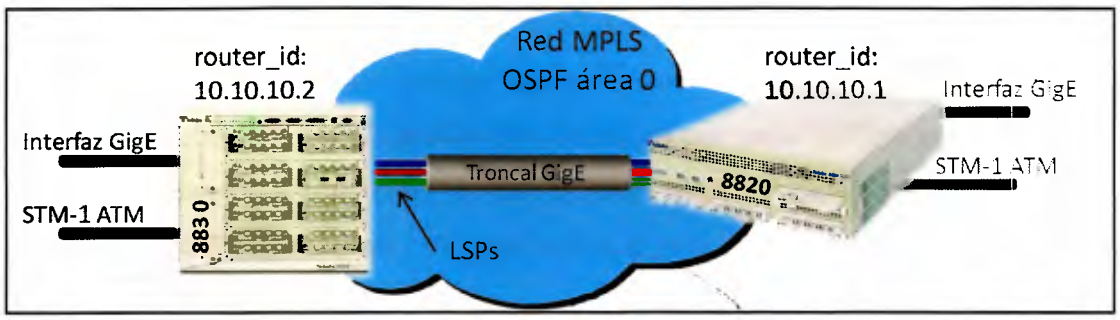


Figura 24. Red MPLS y OSPF

Como se muestra en la figura anterior, el protocolo de enrutamiento interno utilizado es OSPF, y trabaja en la troncal que comunica a los dos equipos, que en este caso es el enlace GigaEthernet. Ambas interfaces del enlace pertenecen al área 0 de OSPF.

El protocolo MPLS trabaja con OSPF como base para soportar la ingeniería de tráfico. MPLS debe ser habilitado de forma global en cada nodo, y luego en cada una de las interfaces que lo requieran, al igual que RSVP-TE. Una vez activos, las propiedades de ingeniería de tráfico indicarán el ancho de banda disponible en el enlace, que para este momento será de 1 Gbps, menos el ancho de banda utilizado para el control de la red.

Se debe verificar que el protocolo OSPF ha sido levantado, y que la tabla de enrutamiento OSPF indica la interfaz por la cual llegar al otro nodo. A través del comando *ping* se puede comprobar el alcance hacia la dirección loop-back del nodo vecino.

E-LSP y L-LSPs

Aunque MPLS se encuentre activo, para lograr la transmisión de tráfico utilizando este protocolo se deben establecer los LSP que se deseen utilizar. Es importante recordar que un LSP es unidireccional, por lo que debe configurarse uno desde cada nodo si se quiere que la transmisión sea bidireccional.

Todos los LSP creados son de tipo "dinámico", lo que les permite tomar, de acuerdo a la ingeniería de tráfico, cualquier ruta hacia el nodo destino con el suficiente ancho de banda. También son definidos por cada LSP, el ancho de banda asegurado (*committed data rate*), el cual es reservado en el enlace troncal, y el ancho de banda máximo (*peak date rate*) que indica la tasa de transmisión máxima que se puede alcanzar en el LSP.

En total se crearon cinco LSPs. El primero del tipo E-LSP por lo que será capaz de soportar las cuatro clases de tráfico que manejan los enrutadores 8800, mientras los otros cuatros serán L-LSP, uno para cada clase de tráfico.

En la siguiente tabla se muestran las propiedades de cada uno.

LSP	Elsp	Llsp0	Llsp1	Llsp2	Llsp3
Commited data rate (Mbps)	500	0	100	100	100
Peak data rate (Mbps)	600	100	100	100	100
Clase de servicio	*todas*	UBR	VBRrt	VBRnrt	CBR

Tabla 2. Propiedades de LSP configurados

Una vez levantados los LSP, se debe comprobar el estado activo de cada uno, y que los anchos de banda reservados por cada uno sean deducidos del ancho de banda total del enlace GigaEthernet en las tablas de Ingeniería de tráfico.

III.3.4 Servicios Capa 2

Este conjunto de pruebas tuvo como objetivo demostrar el funcionamiento de los equipos bajo servicios capa 2, como la configuración de un VPLS y Pseudowires entre servicios iguales.

VPLS

Para la configuración de este servicio se dispuso de la topología mostrada en la figura 15. A cada extremo de la red MPLS se conectaron dos dominios

pertenecientes a una LAN, con un número de etiqueta VLAN igual al configurado en la interfaz del nodo. Estas VLAN deben pertenecer a un mismo VPLS, aunque es posible configurar varios VPLS en un mismo equipo.

Para este tipo de servicio es fundamental que el MTU correspondiente al VPLS sea siempre menor a los MTU de las interfaces VLAN, puertos Ethernet y LSPs utilizados, ya que las tramas en este servicio no son fragmentadas, por lo que las tramas con MTU mayores a los configurados se descartarán. Además, si los MTU no coinciden entre las interfaces pertenecientes a un mismo VPLS, el servicio no se levantará.

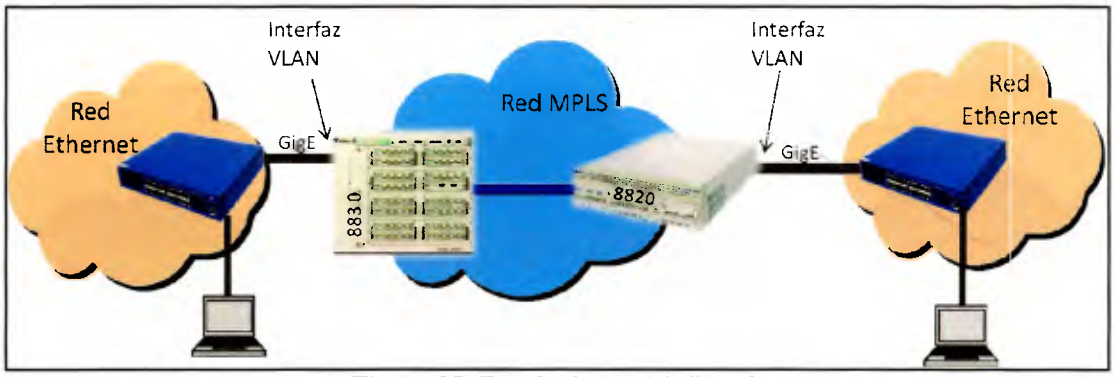


Figura 35. Topología servicio VPLS

Ambas redes Ethernet mostradas en la figura anterior, fueron simuladas utilizando los FrameScope, capaces de generar tráfico IP con etiquetas VLAN, conectados a través de enlaces GigaEthernet. La clase de servicio asignada para este circuito fue UBR y se utilizó el LSP "Elsp" establecido previamente.

Una vez en funcionamiento todos los elementos de la red, y levantado el servicio, los equipos 8800 poseen la capacidad de construir una tabla con las direcciones MAC de los equipos pertenecientes a una misma VPLS, y las interfaces locales por las cuales se pueden alcanzar.

Generando tramas desde uno de los FrameScopes, es posible verificar el flujo de tráfico en los LSPs y en las interfaces VLAN a través de la herramienta *rolling-counters* en tiempo real.

Pseudowire Ethernet.

La creación de este circuito tuvo como objetivo comprobar la capacidad de los equipos de ofrecer conectividad a dos puntos remotos del sistema, del tipo Ethernet, a través de la red MPLS.

Como se muestra en la figura 16, se dispuso de dos interfaces Ethernet a cada extremo de la red MPLS, conectadas a través de un Pseudowire configurado en ambos nodos. Estas interfaces podían ser del tipo FastEthernet o GigaEthernet. Para efectos de las estaciones en las redes externas, esta conexión debía ser transparente, como si se tratara de un puente. También se estableció una tasa de transmisión máxima en los puertos de 5 Mbps, y con clase servicio UBR.

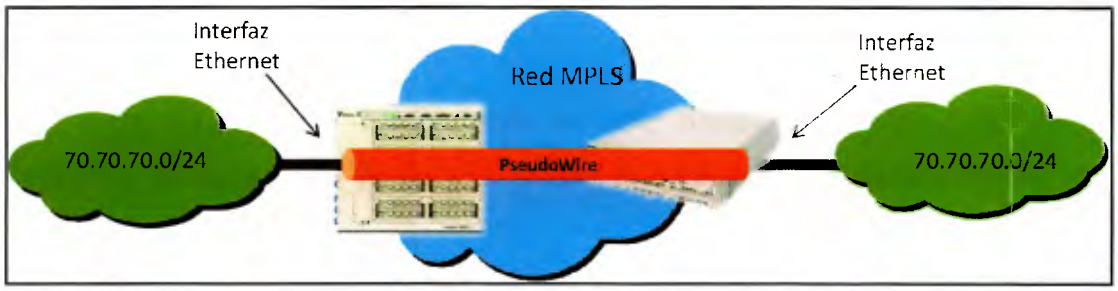


Figura 46. Pseudowire Ethernet

Una vez levantado el circuito, se debe comprobar la conectividad a través de la herramienta *ping* entre las estaciones pertenecientes a los dos extremos de la red. Además, con el comando *traceroute*, se debe verificar que la ruta para llegar desde un extremo a otro de la red no contiene saltos. El flujo de tráfico no debe superar los 5 Mbps.

La simulación de la red Ethernet pudo realizarse utilizando dos computadores configurados con direcciones IP pertenecientes a una misma LAN, o con los FrameScope. En el caso de interfaces GigaEthernet se utilizaron únicamente los FrameScope ya que poseen este tipo de puertos y manejan esa velocidad.

Pseudowire VLAN.

Para levantar este circuito, se utilizó la misma topología de la prueba anterior (Figura 16), con la diferencia de que las interfaces se configuraron del tipo VLAN, modo acceso. Para comprobar el flujo de tráfico entre los extremos del Pseudowire se utilizaron los FrameScope, al igual que en la prueba anterior.

El tipo de servicio configurado fue UBR, con una tasa de transferencia máxima de 5 Mbps. Por medio de la funcionalidad como generadores de tráfico de los FrameScope, se debe comprobar que este no supera los 5 Mbps. Además, se puede verificar el flujo de tráfico con la herramienta *Rolling-counters* tanto en las interfaces VLAN, como en el LSP en uso.

Pseudowire ATM.

Por medio de la configuración de este circuito, se buscó demostrar la capacidad de los equipos de manejar tráfico proveniente de conmutadores ATM a través de la red MPLS.

Con este fin, se creó un Pseudowire del tipo ATM entre dos puertos de los nodos 8800, como se muestra en la figura 17. Dado que se definió del tipo "dinámico", el circuito seleccionó un LSP de acuerdo a la clase de servicio definido, que en este caso fue CBR, únicamente indicando la dirección del nodo destino. Se establecieron los valores de VPI/VCI los cuales deben ser iguales en ambos lados del circuito y el PCR (*Peak Cell Rate*) y SCR (*Sustained Committed Rate*) que representan las tasas de transmisión máxima y transmisión promedio de las celdas ATM sobre el circuito. Además se fijó el MTU en 1500 bytes.

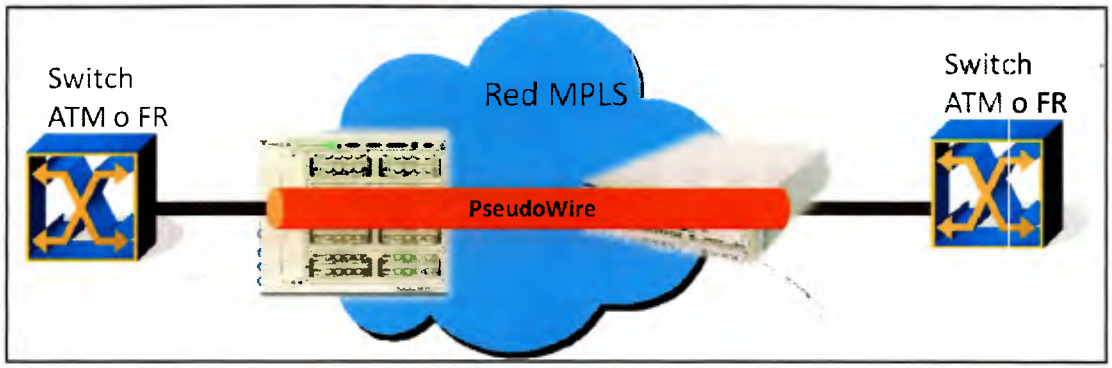


Figura 57. Pseudowire ATM o Frame Relay

Previo a la configuración del Pseudowire, se levantaron dos puertos OC-3c en ambos nodos, como extremos del circuito, configurados para trabajar con un canal STM-1 con tipo de encapsulación ATM. Así mismo se crearon las subinterfaces de tipo ATM en cada puerto.

Para simular los conmutadores ATM, y que fuese posible levantar el circuito, se conectaron estos dos puertos a otros del mismo tipo, en el mismo equipo y configurados con los mismos parámetros.

Pseudowire Frame Relay.

Para la creación de este circuito, se utilizó la misma topología que en el Pseudowire ATM, mostrada en la figura 17. En este caso, los puertos utilizados se definieron para trabajar con encapsulación Frame Relay.

También fue creado de tipo "dinámico", pero con clase de servicio UBR. Se fijó el valor de DLCI igual en ambos lados del circuito y el CIR (*Committed Information Rate*), el cual indica el máximo ancho de banda a utilizar sobre el Pseudowire.

La simulación de los conmutadores Frame Relay en este circuito se llevó a cabo de forma similar que en el Pseudowire ATM, conectando ambos extremos de la red a dos puertos pertenecientes al mismo equipo con los mismos parámetros de configuración, para lograr levantar el circuito.

III.3.5 Servicios Capa 3

A través de la configuración de una IP VPN (RFC 2547bis), se busca verificar el funcionamiento de servicios Capa 3 a través de la red MPLS. Para esto, se configuró la topología mostrada en la siguiente figura.

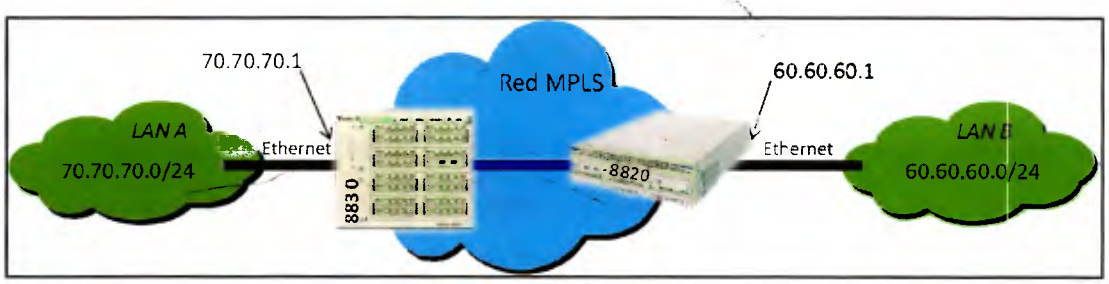


Figura 68. Red IP VPN

Para lograr levantar la VPN, fue necesario configurar el protocolo BGP de forma global en los nodos de la red MPLS y configurar un número de AS y un identificador de enrutador en cada uno de los equipos. Cada interfaz perteneciente a la VPN se define como un puerto iBGP. Esto se efectúa para lograr que los equipos distribuyan las rutas de las redes conectadas a ellos, y pertenecientes a una misma VPN, segregando las rutas que no pertenezcan a la VPN.

A cada extremo de la red MPLS se conectaron dos redes LAN, las cuales pertenecen a una misma VPN configurada en cada uno de los equipos 8800. Desde el punto de vista de las redes LAN, estas aparentan estar conectadas a un mismo enrutador, por lo que la ruta entre la LAN A y LAN B de la figura 18 es de un solo salto, aunque dentro de la red MPLS se atraviese varios enrutadores.

Al igual que las pruebas realizadas de Pseudowire Ethernet, las redes externas fueron simuladas a través del FrameScope, o un computador. En este caso, por tratarse de Capa 3, la dirección IP del equipo conectado al nodo 8800, debe pertenecer a la misma red que la dirección configurada en la interfaz del nodo.

Se debe comprobar conectividad entre dos o más estaciones de distintas LAN a través de un *ping* y comprobar la ruta mediante el comando *traceroute*. También es

posible comprobar el flujo de tráfico entre ambas redes LAN conectando un computador a cada una e intercambiando información de manera constante entre ambas estaciones, verificando el estado de los *rolling-counters* en tiempo real. A través de la herramienta de redes del Administrador de tareas de Windows se puede obtener el porcentaje del ancho de banda en uso.

III.3.6 Interoperabilidad de Servicios

Una de las capacidades de los equipos 8800 es establecer servicios de interoperabilidad (*Interworking*) de capa 2 a través de Pseudowires, sin importar el medio de acceso utilizado. Se probó la configuración de este tipo de servicio a través de diferentes Pseudowire, expuestos a continuación:

ATM / Ethernet Interworking.

En la realización de esta prueba se utilizó como base la topología mostrada en la figura 19, la cual consiste en un extremo de la red del tipo ATM y el otro extremo del tipo Ethernet.

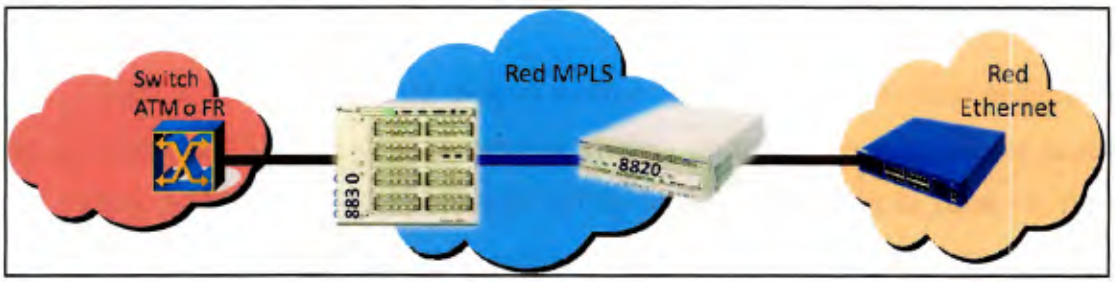


Figura 79. ATM / Ethernet Interworking propuesta

Sin embargo, para lograr la simulación del equipo ATM y lograr establecer un flujo de tráfico en el enlace, se conectó la interfaz ATM a otra del mismo tipo, en el mismo equipo, y con los mismos parámetros. A su vez, se configuraron dos redes Ethernet en el nodo 8820, quedando finalmente la red mostrada en la siguiente figura.

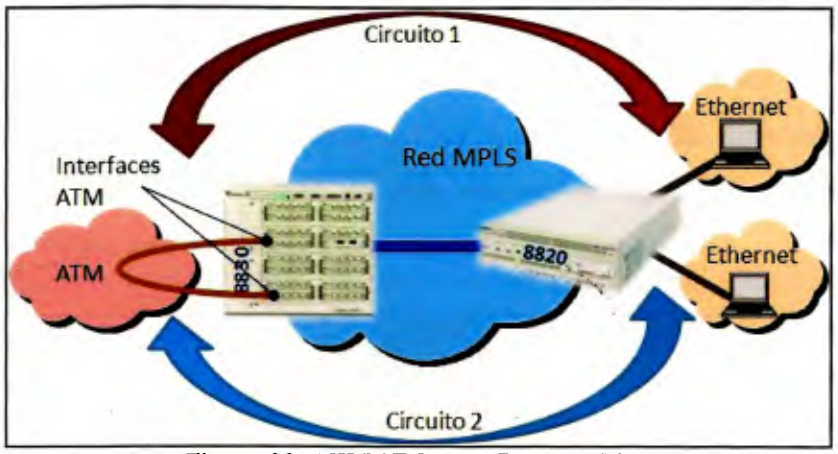


Figura 20. ATM / Ethernet Interworking

Por lo tanto, se configuraron dos circuitos remotos de interoperabilidad ATM / Ethernet, lo cual permitió generar tráfico entre las dos redes Ethernet en ambas direcciones, comprobando que este fluyera a través del enlace entre las interfaces ATM.

Al igual que para el Pseudowire ATM, se configuraron los valores VPI/VCI y MTU. Ambos circuitos fueron especificados del tipo "dinámico" y para manejar tráfico CBR en ambas direcciones, con una tasa de transmisión máxima de 1 Mbps y posteriormente incrementada a 5 Mbps.

Con la herramienta OAM-ping es posible verificar el correcto funcionamiento de la conexión ATM. Se debe comprobar el flujo de tráfico entre nodos de la red Ethernet y ATM a través del comando *rolling-counters*. También se debe verificar que el levantamiento de este circuito redujo el ancho de banda disponible en el E-LSP configurado entre ambos equipos de la red MPLS. El tráfico generado entre ambas estaciones de las redes Ethernet no debe superar la tasa de transmisión máxima establecida.

FR / Ethernet Interworking.

A diferencia de la prueba anterior, en esta se estableció un circuito local en cada nodo del tipo FR / Ethernet, resultando la topología de red mostrada en la figura

21. Se utilizaron igualmente dos puertos OC-3c configurados con tipo de encapsulación Frame Relay, ubicados en la misma tarjeta física que los puertos ATM. Las redes Ethernet en los extremos de los circuitos fueron simuladas con un computador en cada una. Además, en cada circuito se especificó el mismo valor DLCI, y para tráfico con clase de servicio UBR.

Figura 21. Red Ethernet / Frame Relay

Una vez levantados los circuitos, se debe comprobar la conectividad entre las dos estaciones en las redes Ethernet mediante un ping, y el flujo de tráfico a través de la herramienta de conexión de redes de Windows. También es posible verificar el estado de la transmisión a través del comando *rolling-counters* en los 8800.

Cabe destacar que el enlace GigaEthernet y los LSP configurados no formaron parte de esta prueba por tratarse de dos circuitos locales.

III.3.7 Calidad de Servicio (QoS)

En esta sección las pruebas realizadas utilizaron elementos de la red previamente configurados en secciones anteriores, modificando sólo algunos parámetros para comprobar la capacidad de los equipos de brindar soporte de Calidad de Servicio.

Inicialmente se crearon grupos de QoS los cuales se configuraron con los parámetros por defecto y con listas de acceso a través de las direcciones MAC que permitieran el acceso a cualquier usuario. Luego se aplicaron estos grupos a las

interfaces VLAN pertenecientes al VPLS de la sección III.3.4. Se debe comprobar que las interfaces pasan a formar parte de estos grupos de QoS.

Posteriormente se configuraron estas mismas interfaces para clasificar el tráfico como CBR, y los parámetros del LSP por el cual atraviesa el servicio VPLS para permitir el flujo de esta clase de tráfico. Se debe comprobar que por el LSP sólo viaja el tráfico CBR, y que si se modifica el LSP para no soportar CBR, no debe existir transferencia de datos.

III.3.8 Confiabilidad y Rendimiento

A partir de los servicios anteriormente configurados, se ejecutaron pruebas de confiabilidad en el enlace troncal y reenrutamiento de LSPs, redundancia en las tarjetas de conmutación y control (SCC) y finalmente pruebas de rendimiento en cuanto a tasas de transmisión.

Se instaló un enlace físico de respaldo a la troncal GigaEthernet ya existente y se configuró el sistema de protección dentro de uno de los LSP. A medida que se generaba tráfico a través de uno de los circuitos que utilizaban este LSP, se desconectó físicamente la fibra óptica de uno de los dos nodos. Por medio de un *ping* extendido se debe comprobar que el LSP toma la ruta de respaldo y el tráfico sigue fluyendo.

En cuanto a las pruebas de redundancia de Hardware, se retiró físicamente la tarjeta SCC que se encontraba en estado activo. La SCC en estado de espera debe automáticamente tomar control del equipo sin incidir en el tráfico.

Así mismo, se realizaron pruebas que permitiesen determinar el rendimiento de la red. Una de estas es el *Throughput Test* descrita en el RFC 2544, cuyo objetivo es determinar la máxima tasa de transferencia en bits por segundo, tramas por segundo o porcentajes para diferentes tamaños de trama entre dos puntos de la red, y sin pérdida de paquetes.

Esta prueba fue realizada entre dos extremos de la red VPLS mostrada en la figura 15 de la sección III.3.4 utilizando para ello los FrameScope como dispositivos de prueba. La prueba se realizó configurando estos dispositivos de dos formas diferentes:

- Como redes VLAN, con etiquetas VLAN con valor 100 y prioridad 0, conectados a puertos VLAN en cada nodo.
- Sin etiquetas VLAN, conectados directamente a interfaces GigaEthernet de cada 8800.

En un principió la prueba se ejecutó para una tasa de transmisión máxima de 1Gbps con tamaños de trama de 64, 128, 256, 512, 1024, 1280 y 1518 bytes para interfaces tipo Ethernet y 68, 132, 260, 516, 1028 y 1522 para interfaces tipo VLAN debido al tamaño de la etiqueta VLAN de 4 bytes. En los casos en que la red no soportase esa tasa de transmisión, se disminuía ese valor hasta obtener un resultado sin pérdidas de paquete. La tabla 3, tomada del artículo *RFC 2544 Testing of Ethernet Services in Telecom Networks* (BURGESS, 2004), muestra los valores máximos que se deben alcanzar en la práctica para cada tamaño de trama, para enlaces de 1 Gbps.

Tamaño de Trama (bytes)	Tasa Trasferencia (Mbps)	Cabecera e IGP (Mbps)	Tramas / segundo
64	761,90	238,10	1.488.095
128	864,86	135,14	844.594
256	927,54	72,46	452.898
512	962,40	37,59	234.962
1024	980,84	19,16	119.731
1280	984,61	15,38	96.153
1518	986,99	13,00	81.274
1522 (VLAN)	987,02	12,97	81.063

Tabla 3. Valores máximos de Transferencia GigaEthernet

La siguiente figura (Figura 22) muestra la topología utilizada para el desarrollo de la prueba.

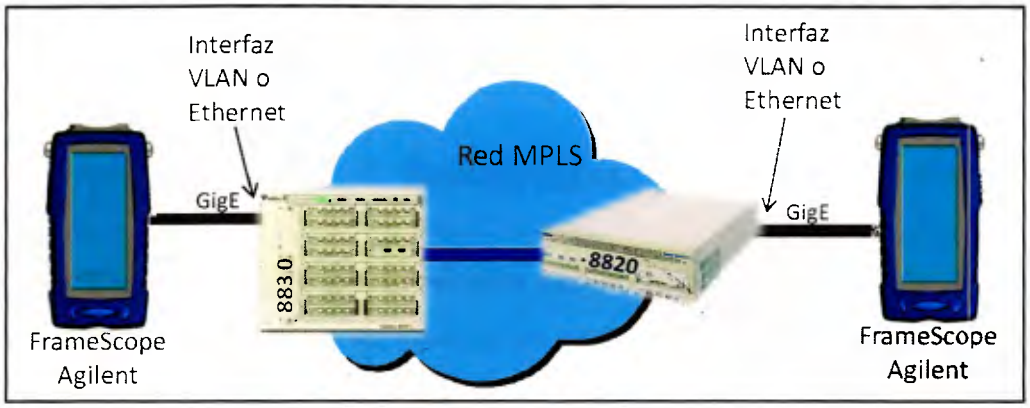


Figura 22. Topología prueba Throughput

Capítulo IV

Resultados

Todas las configuraciones realizadas para la ejecución de las pruebas descritas en el capítulo anterior fueron llevadas a cabo mediante CLI, el cual es un método de interacción con el sistema operativo a través de una serie de comandos que brindan acceso al control del equipo, de manera local o remota.

El control del equipo puede ser clasificado en varios modos, los cuales otorgan distintos niveles de privilegios a cada usuario. Por lo general, los sistemas operativos de este tipo de equipos poseen un modo operacional, el cual permite únicamente visualizar la configuración actual del terminal y un modo privilegiado desde donde se puede manipular la configuración global del equipo, así como acceder a un modo de configuración más específico como interfaces, protocolos, servicios, etc.

Por lo tanto, la configuración de protocolos y servicios se realizó a través del modo privilegiado, mientras que la verificación de estas configuraciones y generación de estadísticas y reportes, se dio a través del modo operacional, con el comando ***show***. Este comando, junto con otros parámetros, muestra información específica sobre interfaces, circuitos existentes, protocolos activos, tablas de enrutamiento creadas, etc., que permiten verificar el estado de operación del equipo.

Los puntos descritos a continuación, muestran los resultados obtenidos para cada una de las pruebas reseñadas en el capítulo anterior, utilizando principalmente el comando *show*.

IV.1 Configuración Inicial de Equipos

Al realizar las pruebas de configuración inicial lo primero que se observó fue como se cargaron exitosamente los parámetros iniciales del sistema, así como se obtuvo acceso a la interfaz de línea de comando o CLI (del inglés Command Line Interface). Esto se observa en la figura 23 mostrada a continuación

```
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
*                                                                           *
*        Welcome to Tellabs Multi-service OS Command Line Interface         *
*                                                                           *
*                              Tellabs, Inc.                                *
*                            Santa Clara, CA 95050                          *
*                              www.tellabs.com                              *
*                                                                           *
*     North America: 1 (800) 443 5555   International: (630) 512 7040       *
*                                                                           *
*          Copyright(c) 2006 Tellabs.      All rights reserved.             *
*                                                                           *
* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *


Login:
```

Figura 23. Pantalla inicial de bienvenida Tellabs 8800

Desde esta posición de pantalla se logró cambiar sin ningún inconveniente las contraseñas y nombres de usuario preestablecidas por el sistema; verificándose que este pasó era obligatorio.

El siguiente resultado obtenido tiene que ver con la versión del software instalado en los nodos, donde a través del comando *show version* se observó que la versión instalada para el 8820 era la 4.0.0.0.102375 y para el 8830 la 5.2.0.1.147932 y no la última versión como era de esperarse para ambos equipos. Para solucionar esto fue necesario descargar a los nodos la versión de software requerida, lo cual se logró exitosamente a través del protocolo de transferencia de archivos o FTP (del inglés File Transfer Protocol). Para el caso del 8830 fue necesario instalar el software en todas las ULC y SCC. Finalmente se comprobó que el software se había actualizado correctamente en todas las tarjetas del equipo utilizando el comando *show node extensive* como se muestra a continuación.

- En el 8820

```
8820# show node extensive

Crd Op Image1          Sts    Image2          Sts   Select Image    Fail Reason
--- -- ------          ---    ------          ---   ------------    -----------
L1  up 4.0.0.0.102375  C      6.0.0.3.174332  R     6.0.0.3.174332  none
```

Figura 24. Versión de Software 8820

- En el 8830

```
8830# show node extensive

Crd Op Image1          Sts    Image2          Sts   Select Image    Fail Reason
--- -- ------          ---    ------          ---   ------------    -----------
S1* up 5.2.0.1.147932  C      6.0.0.3.174332  R     6.0.0.3.174332  none
S2  up 5.2.0.1.147932  C      6.0.0.3.174332  R     6.0.0.3.174332  none
L1  up 6.0.0.3.174332  R      5.2.0.1.147932  C     6.0.0.3.174332  none
L2  up 6.0.0.3.174332  R      5.2.0.1.147932  C     6.0.0.3.174332  none
L3  dn not available   I      not available   I     6.0.0.3.174332  none
L4  dn not available   I      not available   I     6.0.0.3.174332  none
```

Figura 25. Versiones de Software 8830

A continuación se comprobó que el hardware de los nodos estaba funcionado correctamente, para el caso del 8830 fue necesario verificar los SCC, ULC y PLM mientras que para el 8820 sólo los PLM. Esto se logró a través de los siguientes comandos de CLI:

```
8830# show equip sw-card

     Card Idx   Admin      Operational   Config Type     State
     --------   -----      -----------   -----------     -----
     1/1        enabled    up            SCC-1           active
     1/2        enabled    up            SCC-1           standby
```

Figura 26. Estado tarjetas SCC en 8830

Se comprobó que ambas SCC estaban habilitadas estando la 1/1 en estado activo y la 1/2 en estado de espera.

```
8830# show equip line-card

     Card Idx  Admin     OpSts  Config Type  Actual Type  Equip. State
     --------  -----     -----  -----------  -----------  ------------
     1/1       enabled   up     ULC-1        ULC-1        plugged
     1/2       enabled   up     ULC-1        ULC-1        plugged
     1/3       disabled  down   none         none         empty
     1/4       disabled  down   none         none         empty
```

Figura 27. Estado ULCs en 8830

Se observó que las ULC instaladas; en este caso la 1/1 y 1/2, estaban en estado habilitado.

```
8830# show equip line-module

     LineMod Idx  Admin    OpSts  Cfg Type       Act Type       Equip State
     -----------  -----    -----  --------       --------       -----------
     1/1/1        disable  down   ds3[DS3]       ds3            plugged
     1/1/2        disable  down   gige           gige           plugged
     1/1/3        disable  down   oc3c           oc3c           plugged
     1/2/1        disable  down   fast-enet      fast-enet      plugged
     1/2/2        disable  down   oc3-ds310      oc3-ds310      plugged
```

Figura 28. Estado PLMs en 8830

Tanto para el 8830 como para el 8820 los módulos instalados fueron reconocidos por el sistema, aún cuando administrativamente se encontraban deshabilitados. Los tipos de módulos mostrados en la tabla coincidieron con los módulos instalados en el panel frontal del sistema, como se esperaba.

El próximo paso en las pruebas de configuración inicial era verificar los LED´s de alarma en el panel del sistema. Aquí se observó que en ambos equipos un LED de alarma mayor se encontraba encendido; para saber a que estaba asociada dicha falla se consultó el panel del sistema de la siguiente manera:

```
8820# show event current-table

LEGEND:
   Severity:   C: Critical, M: Major, m: Minor, I: Info

          S
Seq       e Description
#         v Cat  Instance          Text/Explanation
---       - ---  --------          ----------------
5         M SHLF PWR-1/1/B         Power failure
```

Figura 29. Alarmas en 8820

A través de este comando se pudo observar que la falla mayor estaba relacionada con energía. Según el manual de instalación no se debían continuar las pruebas en caso de presentarse un evento de este tipo, pero se determinó que éste se debía a la falta de energía en el bloque B del panel de alimentación DC del equipo. Este bloque sólo representa alimentación redundante y para comprobar el correcto funcionamiento de dicho bloque de energía, se procedió a conectar el equipo sólo a través de esta entrada (desconectando el bloque A) y se activó sin presentarse ningún problema. Finalmente se volvió a energizar el equipo a través del bloque A y el bloque B no fue conectado. De esta forma se continuó con la realización de las pruebas obviando este evento.

Para el caso del 8830 además de la falla de energía explicada anteriormente se observaba otra falla, la cual estaba relacionada con la bandeja de ventiladores

```
8830# show event current-table

LEGEND:
   Severity:   C: Critical, M: Major, m: Minor, I: Info

          S
Seq       e Description
#         v Cat  Instance          Text/Explanation
---       - ---  --------          ----------------
11        M SHLF FAN-1/2/1/1       Fan failed
```

Figura 30. Alarmas en 8830

Este evento muestra una falla en la bandeja 2 de ventiladores. Para comprobar que la falla no era en la ranura del equipo 8830 sino en la bandeja de ventiladores, esta se cambio a la otra ranura del equipo y se observó cómo se asoció la falla a la

nueva ranura. A pesar de este error en la bandeja de ventiladores no se notaba ninguna falla física o mecánica. En el manual System Installation Manual. Tellabs 8830 se indica que el Tellabs 8830 puede funcionar sólo con una bandeja de ventiladores e incluso sin bandeja alguna por un lapso no mayor a 3 minutos, debido a esto se pudo proceder con las pruebas.

IV.2 Configuración Básica de la red MPLS

Como era de esperarse el protocolo interno de enrutamiento OSPF se levantó correctamente entre los dos equipos. A través de la instrucción *show protocol ospf neighbor* se observó cómo se aprendieron los vecinos OSPF pertenecientes al área 0, donde el 8830 fue escogido como enrutador designado por poseer un identificador de enrutador mayor que el del 8820. Al 8820 se le asignó la cualidad de enrutador designado de respaldo. Con este comando también se especifica la dirección IP del vecino así como la interfaz por donde se le llega. Dicho comando se muestra a continuación visto desde el Tellabs 8820

```
8820(config)# show protocol ospf neighbor

Router Id       IP Address      Interface             State Status Pri   Opts
--------------- --------------- --------------------- ----- ------ ----- ----
10.10.10.2      172.16.0.2      ge-1/1/4/2.1          Full  DR     1     0x42
```

Figura 31. Tabla de nodos vecinos OSPF

El protocolo MPLS fue habilitado globalmente así como en las interfaces pertenecientes al núcleo IP/MPLS. Esto se observa a continuación.

```
8830# show interface ge-1/1/2/1.1 extensive
Interface: ge-1/1/2/1.1 [IP - Ethernet];  IP Address: 172.16.0.2/24
Oper Status: up;  Failure Reason: none
Protocol Family: Inet  Mpls[Up]
```

Figura 32. MPLS habilitado en interfaz 8830

```
8820# show interface ge-1/1/4/2.1 extensive
Interface: ge-1/1/4/2.1 [IP - Ethernet];  IP Address: 172.16.0.1/24
Oper Status: up;  Failure Reason: nonen State: enable
Protocol Family: Inet  Mpls[Up]
```

Figura 33. MPLS habilitado en interfaz 8820

Respecto al protocolo de reservación de recursos, este se observa de forma similar a OSPF viendo los vecinos RSVP aprendidos. Observándose esto desde el 8830.

```
8830# show protocol mpls rsvp neighbor

MPLS RSVP Neighbors;
  Interface            NbrAddr          Encap Proto
  ---------            -------          -----------
  ge-1/1/2/1.1         172.16.0.1       IP
```

Figura 34. Tabla de nodos vecinos RSVP

Finalmente el ancho de banda presentado en el enlace fue de 999 Mbps tomándose 1 Mbps para control de red

```
8820# show protocol mpls traffic-eng topology ospf extensive
NodeId: 10.10.10.1      type: Router;
      Max Bw: 999000 Kbps, Max Resv Aggr Bw: 999000 Kbps
NodeId: 10.10.10.2      type: Router;
      Max Bw: 999000 Kbps, Max Resv Aggr Bw: 999000 Kbps
```

Figura 35. Ancho de banda disponible en el enlace troncal

Como se detalló en el capítulo de Metodología y Desarrollo se crearon 5 LSP´s con propiedades diferentes.

```
8830# show protocol mpls lsp
                                Ad Op                          Svc
 LSP NAME                       St St Type Mode Fec (to)       Class
 ------------------------------ -- -- ---- ---- --------------- ------
 lsp1                           en up TE   ingr 10.10.10.1     ELSP
 llsp0                          en up TE   ingr 10.10.10.1     UBR+
 llsp1                          en up TE   ingr 10.10.10.1     VBRrt
 llsp2                          en up TE   ingr 10.10.10.1     VBRnrt
 llsp3                          en up TE   ingr 10.10.10.1     CBR
```

Figura 36. LSPs configurados

Con el comando *show protocol mpls lsp extensive* se pudo comprobar que los valores Commited Data Rate y Peak Data Rate concuerdan con los expresados en la tabla 2 para cada LSP.

IV.3 Servicios Capa 2

VPLS

Para que este servicio funcione correctamente fue necesario cumplir con las reglas de MTU que se exigen y que fueron explicadas en el capítulo de Metodología y Desarrollo. Para corroborar que los valores de MTU fueron asignados a las interfaces puertos y LSP´s; y aceptados por el sistema se ejecutaron diversos comandos show, de los cuales fueron extraídos los valores MTU que se registraron en la tabla 4.

	MTU	
	8820	***8830***
Interfaz VLAN	*2008*	*2008*
Puerto Ge VLAN	*2008*	*2008*
Interfaz del Núcleo	*2050*	*2050*
Puerto Ge del Núcleo	*2100*	*2100*
LSP	*2008*	*2008*
MTU de VPLS	*2004*	*2004*

Tabla 4. Valores MTU configurados para VPLS

A través de esta tabla se puede observar como el MTU de la VPLS coincide en ambos equipos, así como es menor al de las interfaces VLAN, puertos Ethernet y LSP´s.

Para comprobar que la VPLS se había levantado se tomó como apoyo el siguiente comando

```
8830(config)# show bridging-instance name bi1 brief

Bridging                        Ad Op            Interface   Circuit
Instance Name                   St St VcId       Cfg   Up    Cfg   Up
------------------------------- -- -- ---------- ----- ----- ----- -----
bi1                             en up 100        2     0     1     0
```

Figura 37. Estado VPLS en 8830

Para comprobar que la VPLS estaba funcionando correctamente fue necesario verificar que los equipos pertenecientes a este servicio habían aprendido las direcciones MAC de todos los equipos pertenecientes a la VPLS. Esta verificación se realizó con el comando *show bridging instance name bi1 learnt-mac-table*, el cual se muestra a continuación.

```
8830(config)# show bridging-instance name bi1 learnt-mac-table
Last clear time on bridging instance learnt-mac-table: not available
[ Legend:
    Type: D: Dynamic; S: Static
]
                                                                  Time to
 ULC    Mac address        Interface/Circuit                Type  Age(sec)
 ----   -----------------  -------------------------------  ----  --------
 1/1    00:30:D3:0B:6B:03  ge-1/1/2/2.1                     D     275
 1/1    00:30:D3:0B:8B:30  ckt1                             D     275
```

Figura 38. Tabla de direcciones MAC aprendidas por 8830

En este show se observa como desde el 8830 se aprendió la dirección MAC del equipo Framescope directamente conectado a través de la interfaz ge-1/1/2/2.1 así como la dirección del Framescope conectado a través del servicio VPLS identificado como ckt1.

Con la herramienta ping se verificó que había conectividad entre los dos Framescopes conectados a través de la VPLS y con traceroute se comprobó que los Framescopes están sólo a un salto de separación, lo cual comprueba que los equipos Tellabs 8820 y 8830; como era de esperarse, son invisibles para los usuarios finales al utilizar este tipo de servicio.

Pseudowire Ethernet

Para verificar que el Pesudowire Ethernet se había creado correctamente, así como habilitado administrativamente se acudió al comando *show ckt* donde se confirmó esto. A continuación se muestra el comando desde el 8820

```
8820(config)# show ckt

Circuit Name                    Type  Ad Op out-vclabel*/vcid
------------                    ----  -- -- -----------------
PSWE                            eth   en up 200
```

Figura 39. Estado VPLS en 8830

Para confirmar que el equipo había aceptado la clase de servicio como UBR y la tasa máxima de transmisión en 5Mbps, se realizó el siguiente show.

```
8830# show ckt name PSWE extensive

flow(1->2) CFG: UBR; Max Rate: 5000; Min Rate: 0; MBS: 0
           ACT: UBR; Max Rate: 5000; Min Rate: 0; MBS: 0
flow(2->1) CFG: UBR; Max Rate: 5000; Min Rate: 0; MBS: 0
           ACT: UBR; Max Rate: 5000; Min Rate: 0; MBS: 0
```

Figura 40. Parámetros de servicio en Pseudowire Ethernet

Para que este servicio pueda funcionar las interfaces de acceso al proveedor de servicio (en este caso el núcleo Tellabs 8820-8830) deben estar configuradas como Ethernet. A través de *show interface* se pudo observar la interfaz configurada como Ethernet; denominada *enet* según Tellabs, además de estar habilitada administrativa y operacionalmente.

```
8820(config)# show interface

                                Service/          BR-Inst Name/   Ad Op Failure
Interface            Type       IPAddr/Mask       RT-Inst Name    St St Reason
-------------------- ------- ------------------ --------------- -- -- --------
fe-1/1/3/1           enet       Layer 2           -               en up none
```

Figura 41. Interfaz Ethernet

Al configurar el servicio de Pseudowire se notó que este servicio solo puede ser habilitado entre dos clientes lo cual puede ser visto como un puente, a diferencia de la VPLS donde varios clientes pueden pertenecer al mismo servicio simulando un conmutador.

Al igual que en el servicio VPLS se comprobó conectividad con la herramienta ping, así como la transparencia de la red MPLS al utilizar traceroute.

Pseudowire VLAN

Al igual que en Pseudowire Ethernet se observó que el servicio había sido creado y que se encontraba habilitado a través de *show ckt*

```
8830(config)# show ckt

Circuit Name                    Type  Ad Op out-vclabel*/vcid
------------                    ----  -- -- ----------------
PSWE-VLAN                       vlan  en up 210
```

Figura 42. Estado Pseudowire VLAN

A diferencia de Pseudowire Ethernet, acá las interfaces de acceso al proveedor de servicios debían ser del tipo vlan, esto se observa a continuación

```
8820(config)# show interface

                                Service/            BR-Inst Name/    Ad Op Failure
Interface              Type     IPAddr/Mask         RT-Inst Name     St St Reason
-------------------- -------- ------------------- --------------- -- -- --------
fe-1/1/3/2             vlan     Layer 2             -                en up none
```

Figura 43. Estado VPLS en 8830

En este tipo de servicio se volvieron a usar las herramientas de ping y traceroute con la misma finalidad que en puntos anteriores.

Pseudowire ATM

Primero se verificó la configuración de los puertos del tipo ATM, mostrados en el siguiente comando, así como el tipo de interfaz capa 2, también del tipo ATM.

```
8830(config)# show interface

                                Service/            BR-Inst Name/    Ad Op Failure
Interface              Type     IPAddr/Mask         RT-Inst Name     St St Reason
-------------------- -------- ------------------- --------------- -- -- --------
so-1/1/3/2:1           atm      Layer 2             -                -  up none
```

Figura 44. Interfaz ATM en 8830

Una vez el circuito se encontró en estado activo, fue posible verificar los parámetros establecidos, que se observan dentro de la configuración del circuito:

```
8820(config)# show ckt name maal5 extensive

circuit: maal5; type: atm
 admin: enable; oper: up; failure reason: none
 side1: port; in status: up; out status: up
  int: so-1/1/1/2:1; type: atm vc-aal5; mtu: 1500; vpi: 157; vci: 157
 side2: lsp; in status: up; out status: up
  dynamic out-lsp: llsp2 (Learnt);
  dest: 10.10.10.2; preference: all
 flow(1->2) CFG: CBR-p; PCR: 4; SCR: 0; MBS: 0; CDVT: 0
 flow(2->1) CFG: CBR-p; PCR: 4; SCR: 0; MBS: 0; CDVT: 0
```

Figura 45. Estado Pseudowire ATM

Pseudowire Frame Relay

Al igual que para el circuito anterior, se verificó el tipo de encapsulación del canal perteneciente al puerto el cual debía ser Frame Relay, y el tipo de interfaz asignada a ese puerto. Además, se verificaron los parámetros del circuito, comprobando que fueron los configurados y el estado activo del Pseudowire.

IV.4 Servicios Capa 3

Para verificar que la IP-VPN estaba activa administrativa y operacionalmente se recurrió al siguiente comando

```
8820(config)# show routing-instance

 Number of routing instances: 1;  Enabled: 1;  Up: 1

 Routing          Adm Op  Route                  Num Of      Max Num Of
 Instance Name    St  St  Distinguisher          Routes      Routes
 --------------- --- --- --------------------- ---------- ----------
 vpn2             en  up  65000:1                0                -
```

Figura 46. Estado IP VPN en 8820

Para este tipo de servicios las interfaces deben estar configuradas para soportar IP, esto el fabricante Tellabs lo llama en su software ipEnet. En el siguiente show se observa como las interfaces a utilizar cumplen con este requerimiento.

```
8820(config)# show interface

                                Service/           BR-Inst Name/   Ad Op Failure
Interface              Type     IPAddr/Mask        RT-Inst Name    St St Reason
------------------- ------- ------------------ --------------- -- -- --------
fe-1/1/3/3.1           ipEnet   60.60.60.1/24      vpn2            en up none
```

Figura 47. Interfaz Ethernet para IP VPN en 8820

Luego de conectar dos ordenadores a los puertos de acceso de la nube MPLS se comprobó conectividad con ping así como se utilizó traceroute para certificar que las dos redes están separadas por un solo salto. De esta forma se pudo observar como el servicio IP-VPN simula un enrutador al darle conectividad a dos redes diferentes. Para este caso solo se comunicaron dos redes LAN pero este valor puede ser mayor.

IV.5 Interoperabilidad de Servicios

ATM/ Ethernet Interworking

Al igual que en el resto de las pruebas lo primero que se comprobó fue que las interfaces que iban a estar relacionadas con estas pruebas estuvieran habilitadas y configuradas de la forma esperada. Para el caso del 8830 era necesario que las interfaces de acceso estuvieran configuradas como ATM, como se mostró en la figura 44.

En el 8820 las interfaces de acceso debían ser del tipo Ethernet y asociadas a puertos FastEthernet para permitir la conexión de ordenadores, de forma similar a la figura 41.

A continuación se comprobó como los dos circuitos necesarios para desarrollar este esquema de red fueron creados y habilitados satisfactoriamente. En el siguiente show se observan los circuitos de interoperabilidad denominados *intw1* e *intw2* habilitados administrativa y operativamente

```
8830# show ckt

Circuit Name                    Type  Ad Op out-vclabel*/vcid
------------                    ----  -- -- -----------------
intw1                           eiwf  en up 2500
intw2                           eiwf  en up 2600
```

Figura 48. Circuitos de Interoperabilidad ATM / Ethernet

Debido a la naturaleza de la prueba era muy importante el uso de los rolling-counters para certificar que el tráfico en verdad estaba viajando por donde se esperaba y no simplemente estaba conmutando entre puertos del 8820. Con esta herramienta se verificó el paso de tráfico tanto en las interfaces Ethernet, como en el LSP en uso y en el circuito, observando el número de bytes totales que fluyeron, la tasa de transmisión promedio y el tamaño de paquete promedio.

Como prueba extra se procedió a retirar el cable que unía los dos puertos ATM del 8830 mientras se generaba tráfico. Al realizar esto se cayó la conexión

como era de esperarse. Esto ratifica que el tráfico está viajando a través del modelo de red propuesto para esta prueba y no de otra forma.

Para certificar que se estaba cumpliendo la tasa de transmisión máxima, se procedió a generar tráfico de video entre los ordenadores y, a través de la herramienta de redes del Administrador de Tareas de Windows, se observó en gráficas y porcentaje de utilización que se respetaban los valores máximos de 1Mbps inicialmente y de 5Mbps posteriormente.

Frame Relay/ Ethernet Interworking

A través del comando de la interfaz de línea *show interface* se puede observar como las interfaces que van a conformar el núcleo entre los dos enrutadores Multi-servicio son del tipo Frame Relay; expresado como fr en el CLI de Tellabs, así como están listas para entrar en funcionamiento.

```
8830# show interface

                                Service/          BR-Inst Name/   Ad Op Failure
Interface            Type       IPAddr/Mask       RT-Inst Name    St St Reason
-------------------- ------- ----------------- --------------- -- -- --------
so-1/1/3/2:1         fr         Layer 2           -               -  up none
```

Figura 49. Interfaz Frame Relay en 8830

A continuación se muestra desde el 8820 como el circuito de interoperabilidad Ethernet-Frame Relay está configurado de la manera apropiada. En el 8830 ocurre lo mismo.

```
8820(config)# show ckt

Circuit Name                    Type  Ad Op out-vclabel*/vcid
------------                    ----  -- -- -----------------
pw-fr                           fr    en up 400
```

Figura 50. Estado Pseudowire Frame Relay

Para certificar que en verdad existía comunicación entre los dos ordenadores a través del enlace Frame Relay se utilizó la herramienta ping la cual tuvo un porcentaje de éxito del 100%.

IV.6 Confiabilidad y Rendimiento

Para comprobar que el enlace de respaldo de la troncal MPLS operaba correctamente se procedió a realizar un ping extendido y simultáneamente se desconectó el enlace principal, aquí se observó que el ping seguía siendo exitoso debido a que el LSP había conmutado hacia la ruta de protección.

Dentro de las pruebas de redundancia de Hardware era necesario verificar para el caso del 8830 la de las SCC. Para certificar esto se observó a través del comando *show equip sw-card* que la SCC 1/1 se encontraba activa mientras la 1/2 se encontraba en estado de espera.

```
8830# show equip sw-card

     Card Idx   Admin      Operational   Config Type     State
     --------   -----      -----------   -----------     -----
     1/1        enabled    up            SCC-1           active
     1/2        enabled    up            SCC-1           standby
```

Figura 51. Estado SCC en 8830

Posterior a esto se retiro la SCC 1/1 y se observó como el equipó siguió funcionando. A través del mismo comando ejecutado en el paso anterior se observó como el control del equipo cambio hacia la SCC 1/2 y como la SCC 1/1 dejó de estar presente.

```
8830# show equip sw-card

     Card Idx   Admin      Operational   Config Type     State
     --------   -----      -----------   -----------     -----
     1/1        enabled    down          SCC-1           empty
     1/2        enabled    up            SCC-1           active
```

Figura 52. Estado SCC removida en 8830

En las tablas presentadas a continuación se muestran los resultados para las pruebas de rendimiento al utilizar independientemente cada uno de los FrameScopes como maestro. Igualmente se exponen los valores máximos de tasa de transferencia.

- Para Interfaces VLAN

FrameScope Maestro conectado al:	**Tamaño de Trama**	**Tasa de Transferencia**		
		Tramas por segundo	Mbps	Máximo (Mbps)
8820 (8830 como esclavo)	**68**	1143033	621.8	-
	132	722573	763.0	-
	260	416244	865.8	-
	516	225236	929.8	-
	1028	117474	966.1	-
	1284	94876	974.6	-
	1522	80444	979.5	987.02
8830 (8820 como esclavo)	**68**	1142066	621.2	-
	132	722105	762.5	-
	260	416574	866.5	-
	516	225273	929.9	-
	1028	117526	966.3	-
	1284	94583	971.5	-
	1522	80416	979.1	987.02

Tabla 5. Tasas de transferencia para VLAN

- Para interfaces Ethernet

FrameScope Maestro conectado al:	**Tamaño de Trama**	**Tasa de Transferencia**		
		Tramas por segundo	Mbps	Máxima (Mbps)
8820 (8830 como esclavo)	64	1186024	607.2	761.90
	128	739604	757.4	864.86
	256	421732	863.7	927.54
	512	227022	929.8	962.40
	1024	117952	966.3	980.84
	1280	76923	787.7	984.61
	1518	80180	973.7	986.99
8830 (8820 como esclavo)	64	1186198	607.3	761.90
	128	739604	757.4	864.86
	256	421732	863.7	927.54
	512	226933	929.5	962.40
	1024	118012	966.8	980.84
	1280	76923	787.7	984.61
	1518	80579	978.8	986.99

Tabla 6. Tasas de transferencia para Ethernet

Los resultados presentados en esta tabla no son óptimos debido a que a diferentes tamaños de tramas se presentaron errores al realizar la prueba de Throughput a la tasa de transferencia esperada de 1Gbps. Esto obligó a bajar la tasa de transmisión hasta que no se presentaron errores.

Capítulo V

Conclusiones y Recomendaciones

V.1 Conclusiones

El desarrollo de este Trabajo Especial de Grado brinda todas las herramientas necesarias para presentarle al cliente CANTV todas las características, funcionalidades y ventajas que brindan la serie de enrutadores multi-servicios pertenecientes a la serie 8800 del fabricante Tellabs.

Estos equipos buscan crear una red paquetizada basada en IP/MPLS la cual tiene como virtudes la ingeniería de tráfico de MPLS y la capacidad de ofrecer calidad de servicio. A través de la ingeniería de tráfico de MPLS se permite un mejor manejo del ancho de banda de la red; optimizando el desempeño de la misma, a su vez con la utilización de calidad de servicio se puede diferenciar el tráfico y garantizar un desempeño por cada tipo de tráfico.

Los Tellabs 8800 representan para CANTV una ventaja importante al ofrecer un conjunto de capacidades pertenecientes a la capa 2 y 3 del modelo OSI. Una de estas capacidades es la interoperabilidad de servicios con la cual estos nodos otorgan virtudes operativas importantes a CANTV al poder integrar y migrar diferentes servicios sobre una plataforma común de transporte

Dado que la red de acceso y el transporte son fundamentales para los operadores como CANTV, en este estudio y evaluación técnica se entiende que nodos del tipo multiformato permiten la convergencia de servicios y tecnologías, facilitando el mejor uso de las tecnologías existentes, y la migración a bajo costo de usuarios de servicios, Wifi, Ethernet, IP banda ancha, Frame Relay, ATM, entre otros.

Haciendo transporte eficiente de tráfico en MPLS con QoS y nodos multiservicio, CANTV podría dar más aplicaciones a los usuarios finales y

administrar sus costos sin tener que crecer en plataformas de transporte descartadas por el mercado y fabricantes de tecnología.

V.2 Recomendaciones

En procesos de homologación se recomienda que el conjunto de pruebas a desarrollar esté basado en el seguimiento de un protocolo de pruebas. Dado que todos los clientes no tienen requerimientos iguales ni las mismas redes de servicios de telecomunicaciones, los protocolos de pruebas deben ser realizados en base a sus necesidades, para que al momento de realizar la homologación se evalúen las funcionalidades que en verdad sean de interés. De esta forma se recomienda que estos protocolos sean realizados en conjunto entre el cliente y el proveedor de los equipos Tellabs. Asimismo se debe instruir al cliente sobre los resultados que se esperan para cada una de las pruebas.

A través de proyectos de este tipo se pueden poner en práctica conocimientos teóricos de redes de datos, comparando en laboratorios sus ventajas y debilidades. A pesar de las virtudes de estos proyectos los equipos utilizados suelen ser muy costosos y por lo tanto inaccesibles para las universidades, lo mismo ocurre con los laboratorios de prueba. En base a esto se recomienda a los estudiantes de los últimos años de carreras referentes a tecnologías de información, a vincularse con organizaciones que les permitan vivir experiencias de esta naturaleza.

La incorporación de los enrutadores Multi-Servicio de Tellabs en CANTV se traduciría en la integración y modernización de su red de servicios de telecomunicaciones, así como en la posibilidad de ofrecer una mayor cantidad de servicios a los usuarios finales.

Lista de Acrónimos

ABR	Area Border Router
ATM	Asynchronous Transfer Mode
BDR	Backup Designated Router
BGP	Border Gateway Protocol
CANTV	Compañía Anónima Nacional de Teléfonos de Venezuela
CBR	Constant Bit Rate
CDR	Committed Data Rate
CE	Customer Edge
CLI	Command Line Interface
CoS	Class of Service
CR-LDP	Constrained Based Routing over Label Data Protocol
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DCE	Data Circuit-Terminating Equipment
DLCI	Data Link Connection Identifier
DR	Designated Router
DTE	Data Terminal Equipment
EBGP	External Border Gateway Protocol
EGP	Exterior Gateway Protocol
FEC	Forward Equivalence Class
FTP	File Transfer Protocol
IBGP	Internal Border Gateway Protocol
IETF	Internet Engineering Task Force
IGP	Internal Gateway Protocol
IP	Internet Protocol
IPX	Internetwork Packet Exchange
LAN	Local Area Network
LDP	Label Distribution Protocol
LED	Light Emitting Diode
LER	Label Edge Router
LIB	Label Information Base
LSA	Link State Advertisement
MAC	Media Access Control
MPLS	Multi Protocol Label Switching
MTU	Maximum Transfer Unit
NGN	New Generation Network
NNI	Network Node Interface
OAM-Ping	Operation and Maintenance Ping
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PE	Provider Edge

PLM	Physical Line Module
PSN	Packet Switched Network
PVC	Permanent Virtual Connection
QoS	Quality of Service
RFC	Request for Comment
RIP	Routing Information Protocol
RSVP-TE	Resource Reservation Protocol Traffic Engineering
SDH	Synchronous Digital Hierarchy
SCC	Switch and Control Card
STM-1	Synchronous Transport Module
SPF	Shortest Path First
SVC	Switched Virtual Connection
TEG	Trabajo Especial de Grado`
TCP	Transmission Control Protocol
UBR	Unspecified Bit Rate
ULC	Universal Line Card
UNI	User Network Interface
VBR	Virtual Bit Rate
VCI	Virtual Channel Interface
VLAN	Virtual Local Area Network
VPI	Virtual Path Identifier
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
WAN	Wide Area Network

Bibliografía

Alles, A. (1995). *ATM Internetworking*. Cisco Systems

AT&T. (1998). *Frame Relay Service in Today's Enterprise Network Environment.* USA: The Applied Technologies Group, Inc.

Burgess, N. (2004). *RFC 2544 Testing of Ethernet Services in Telecom Networks.* Agilent Technologies.

Cisco Systems, Inc. (9 de Abril de 2007). *CCNA 2: Principios básicos de routers y enrutamiento. USA.*

Cisco Systems, Inc. (1999). *Internetworking Technology Overview.* USA.

Cisco Systems, Inc. (2000). *Catalyst LAN Switchin.* USA.

Gallaher, R. (2003). *Rick Gallagher's MPLS Training Guide: Building Multi-Protocol Label Switching Networks.* Syngress Publishing.

Held, G. (2003). *Ethernet Networks.* USA: Wiley.

IXIA. (2004). *Open Shortest Path First (OSPF) Conformance and Performance Testing.*

Juniper Networks. (2006). *Configuring Juniper Networks Routers. Student Guide Volume 1.*

Kershaw. (2001). *What is Atm?*. Nextep Broadband.

Mendillo, V. (2005). *Redes ATM.*

Microsoft. (1998). *Red privada virtual: Una descripción general.* Microsoft Corporation.

Nortel Networks. (2001). *MPLS- An Introduction to Multiprotocol Label Switching.*

Rahul Sawant, A., & Qaddour, J. (2003). *MPLS Diffserv: A combined approach.*

Riverstone Networks. (2006). *MPLS/VPLS Evolution: A Riverstone Perspective.*

Spirent. (2001). *Gigabit Ethernet and ATM.*

Spurgeon, C. (2000). *Ethernet: The Definitive Guide.* USA: O'Reilly & Associates, Inc.

Tellabs, inc. (2006). *TMOS QoS Application Manual.*

Tellabs, Inc. (2006). *TMOS User Manual.*

Vázquez, E., (2004). Álvarez-Campana, M. & García, A. *Network Convergence over MPLS.* Madrid: Universidad Tecnológica de Madrid.

Vidaurrázaga, I. (2004). *Voz sobre IP, la convergencia de redes y servicios.* Autelsi, 27-28.

Xiao, X., Hannan, A., & Bailey, B. (2000). *Traffic Engineering with MPLS in the Internet.* IEEE Network March/April , 28-33.

Apéndice A

Ingeniería de Detalles

Índice

1. Descripción General 3
2. Listado y descripción de equipos. 4
   2.1. Tellabs 8820 MSR 5
   2.2. Tellabs 8830 MSR 7
3. Descripción de la instalación física 15
   3.1. Cálculo del consumo de energía 15
   3.2. Características mecánicas 15
   3.3. Alimentación y cableado 16
4. Pruebas de configuración inicial 17
5. Pruebas de funcionalidad 19
   5.1. Configuraciones básicas MPLS 19
   Configuración de OSPF 19
   Configuración de MPLS 20
   5.2. Servicios Capa 2 21
   VPLS 21
   Circuitos Martini entre puertos capa 2 22
   VLAN sobre circuitos Martini 22
   Frame Relay DLCI sobre circuitos Martini 23
   ATM VPI/VCI sobre circuitos Martini 23
   5.3. Servicios Capa 3 24
   5.4 Service Interworking 25
   ATM / Ethernet Interworking 25
   FR / Ethernet Interworking 25
6. Pruebas de Calidad de Servicio, QoS 26
7. Memoria Fotográfica y Planos 27

2. Listado y descripción de equipos.

A continuación se presenta una lista de los equipos a ser instalados y posteriormente una descripción detallada de cada uno.

Qty	Descripción del componente	Código
1	**Tellabs 8820 Multi-service Router Chasis - DC**	**81.8820-DC**
1	2port OC-3/STM-1 Multi-Service PLM - (to DS0/E1) SMF IR	81.8800-PLM003E-20
1	4port OC-3c/STM-1 Multi-Service PLM - SMF IR	81.8800-PLM003C-20
1	4port Gigabit Ethernet PLM - 1000BaseSX (Includes 4 LC/SFP optics)	81.8800-PLMGE-10
1	24 Port Fast Ethernet 10/100Base-TX PLM	82.8800-PLMFE-10
1	**Tellabs 8830 Multi-service Router Chasis - DC**	**81.8830-DC**
2	Tellabs 8830 Switch and Control Card	81.8830-SCC-A
2	Tellabs 8830 2M Universal Line Card	81.8830-ULC-1
1	4port OC-3c/STM-1 Multi-Service PLM - SMF IR	81.8800-PLM003C-20
2	6 Port Clear Channel DS3/E3 IP/FR PLM	81.8800-PLMT3E3-10
1	4port Gigabit Ethernet PLM - 1000BaseSX (Includes 4 LC/SFP optics)	81.8800-PLMGE-10
1	24 Port Fast Ethernet 10/100Base-TX PLM	82.8800-PLMFE-10

Tabla 1. Listado de equipos para la instalación.

Serie Tellabs 8800 Multi-Service Routers (MSR)

La serie Tellabs 8800 es una familia de enrutadores multi-servicio, con tecnología de próxima generación, desarrollados para trabajar con un alto desempeño cubriendo los requerimientos a nivel de proveedores de servicios (*carrier-class services).* Estos equipos brindan soporte a conexiones entre cualquier red y/o servicio de capa 2 de manera confiable y concurrente.

Los 8800 representan un camino para la migración hacia la convergencia de redes IP a través de las capacidades de Ingeniería de Tráfico del protocolo MPLS, valiéndose de características de las redes orientadas a la conexión como la Calidad de Servicio y seguridad, manteniendo las propiedades de escalabilidad y flexibilidad de las redes IP.

El sistema operativo utilizado por estos equipos es el TMOS (Tellabs Multi-service Operating System), el cual provee protocolos estándares de conexión y control para todos los enrutadores de la serie 8800.

Comercialmente, estos equipos se encuentran en tres modelos: Tellabs 8830, 8840 y 8860. Para efectos de este trabajo, se utilizará el equipo 8830 y un modelo de prueba no comercial, el Tellabs 8820. A continuación, se exponen las principales características de cada equipo, así como las especificaciones de cada tarjeta que se empleará.

2.1. *Tellabs 8820 MSR*

El equipo 8820, como parte de la serie de productos Tellabs 8800, cumple con todas las capacidades multi-protocolo y multi-servicio basados en redes IP al igual que los otros modelos, pero con un diseño mucho más compacto y eficiente en cuanto al ahorro de energía. Este enrutador es sólo un modelo de prueba, a diferencia de los otros MSR.

El MSR 8820 consiste en un chasis de cuatro ranuras para la conexión de distintos PLMs (Physical Line Modules) que provee conexiones con velocidades de 12.5 Gbps, full-duplex, con alto desempeño en enrutamiento. La figura 1 muestra el diseño externo de este equipo. A continuación se detallarán las distintas características de esta unidad tomando como referencia el manual *System Installation Manual for Tellabs 8820 MSR* (TELLABS, 2005) y el texto *Tellabs 8820 MSR Product Guide* (TELLABS, 2003), los cuales pueden ser consultados para información específica sobre el producto.

Figura 1. Tellabs 8820

En la figura 2 se detalla la vista frontal del equipo, en donde se señalan los 4 módulos PLM instalados, el panel del sistema y el conector para descargas electrostáticas (ESD Jack). En la tabla 2 se describen las especificaciones físicas de este equipo.

Descripción	Detalle
Alto	13.34 cms
Ancho	43.5 cms
Largo	63.5 cms
Peso del chasis	12.25 Kg

Tabla 2. Especificaciones físicas. Tellabs 8820.

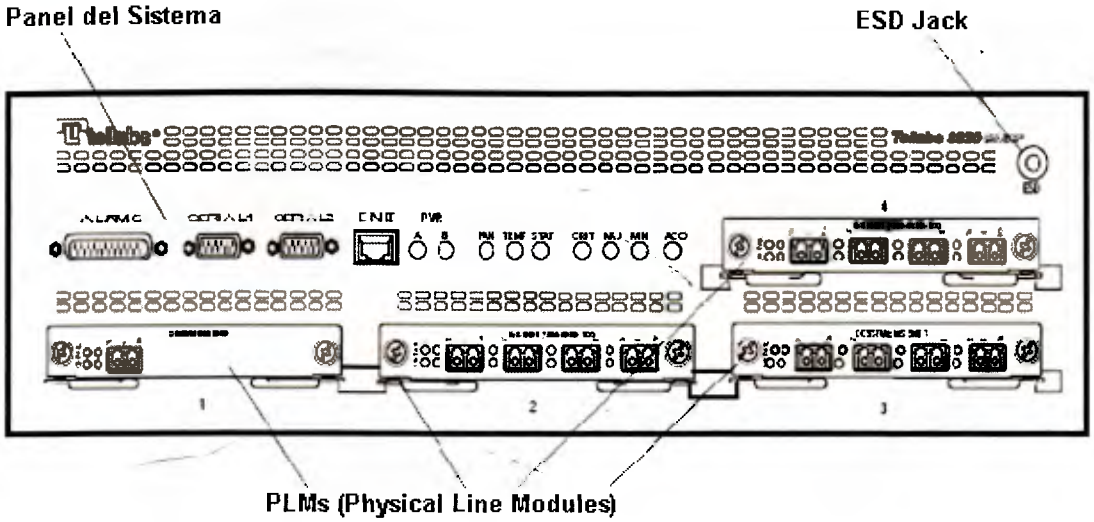


Figura 2. Vista Frontal del Tellabs 8820.

El panel del sistema provee acceso a los puertos del equipo y a los indicadores de estado y alarmas. A través de este panel se accede a la configuración del equipo y su sistema operativo mediante la línea interfaz de comandos (CLI). En la figura 3 se detallan los diferentes componentes del panel del sistema, descritos a continuación.

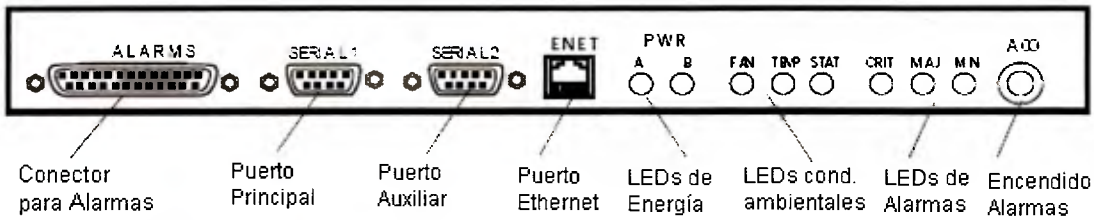


Figura 3. Panel del Sistema del Tellabs 8820.

- Conector para alarmas: terminal de salida DB-25 hembra, para soporte de 3 alarmas visuales y 3 audibles.
- Puertos Seriales (principal y auxiliar): terminal DB-9 macho con soporte RS-232. Aunque el puerto 1 (principal) es el recomendado para las conexiones locales con la consola, en ambos se puede acceder al sistema, ejecutar diagnósticos y correr rutinas para solucionar problemas.
- Puerto Ethernet: Conector 10/100 Base-T Ethernet RJ-45. Provee acceso al sistema de gestión de red al cual esté conectado el equipo.
- LEDs de energía: indican el módulo de energía por el cual se está alimentando el equipo.
- LEDs de condiciones ambientales: indican que el estado de energía del sistema, ventiladores, temperatura del equipo y estado de operación son los correctos.
- LEDs de alarma: indican si se detecta un problema en el sistema según grados de severidad: crítica, mayor y menor.
- Encendido Alarmas: este botón permite silenciar o activar las alarmas audibles y los LEDs.

Existen dos modelos de equipos en cuanto a la alimentación de energía: AC y DC. Para esta instalación se cuenta con el modelo DC. En la figura 4 se presenta el panel de conexión de energía de este modelo.

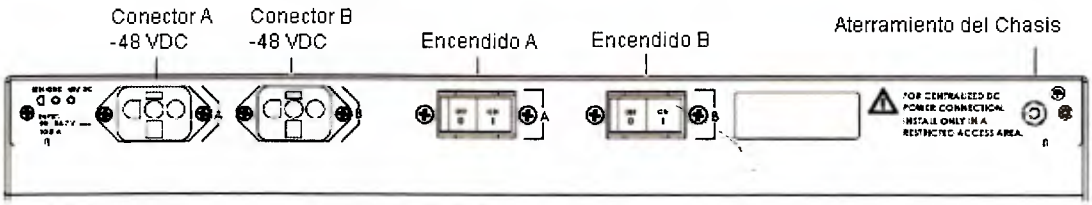


Figura 4. Panel de conexión Tellabs 8820.

Este panel cuenta con dos conectores para alimentación, módulos A y B, con sus interruptores correspondientes y un conector para el aterramiento del chasis. El equipo 8820 solo requiere un modulo de alimentación conectado para operar, que cumpla con los requerimientos mínimos presentado en la tabla 3. Si ambos módulos son conectados, el equipo se ajusta para proveer alimentación redundante 1:1, pero ambos deben cumplir con los requerimientos mínimos de energía.

Descripción	Mínimo	Máximo
Voltaje	-40 VDC	-56.7 VDC
Corriente	--	7,5 Amps (a 40 v)
Máximo Potencia	300 W	300 W
Fusibles	12 Amps.	15 Amps.

Tabla 3. Requisitos de alimentación DC del Tellabs 8820.

2.2. Tellabs 8830 MSR

El MSR 8830 (figura 5) es uno de los modelos comerciales de la serie Tellabs 8800, de alto desempeño, diseñado para colocarse en las instalaciones de los proveedores de servicios en los nodos terminales de las redes IP/MPLS. Aunque sus funciones son las mismas que el MSR 8820, ofrece mayor capacidad de tráfico.

Figura 5 Tellabs 8830.

Las especificaciones, fotografías y tablas acerca de este modelo, descritas a continuación, son tomadas del manual *System Installation Manual for Tellabs 8830 MSR* (TELLABS, 2006) y el texto *Tellabs 8830 MSR Data Sheet* (TELLABS, 2005), los cuales pueden ser consultados para información más específica sobre el producto.

En la siguiente tabla se describen las dimensiones físicas y peso de este equipo.

Descripción	Detalle
Alto	35.6 cms
Ancho	44.4 cms
Largo	59.7 cms
Peso del chasis (con tarjetas)	72 Kg

Tabla 4. Especificaciones físicas. Tellabs 8830.

En la figura 6 se detalla la vista frontal del equipo y cada uno de sus componentes. Un máximo de 16 módulos PLM pueden ser instalados en esta unidad, a través del panel frontal. En la figura mostrada aparecen las 16 ranuras con PLMs ya instalados.

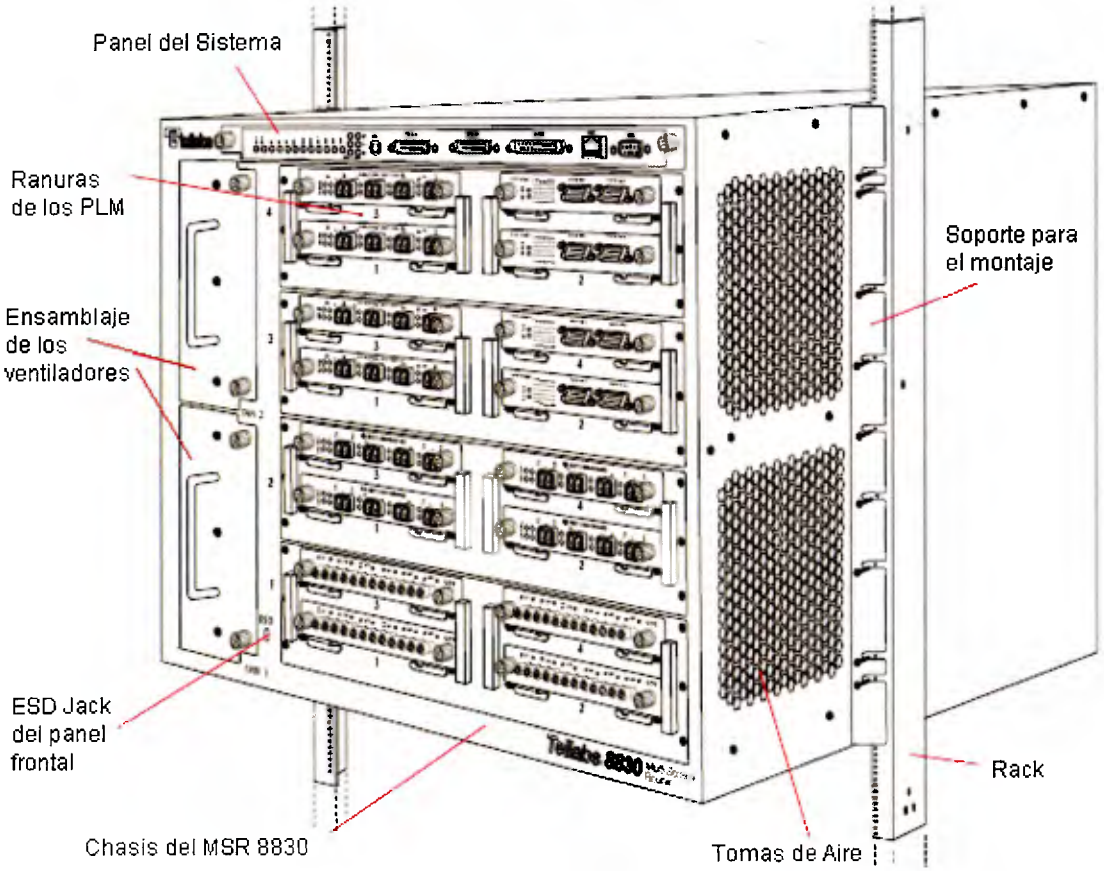


Figura 6. Vista Frontal del Tellabs 8830.

También se aprecia el panel del sistema, detallado en la figura 7, con funcionalidades similares a las descritas anteriormente para el modelo MSR 8820. Sin embargo, este panel presenta LEDs adicionales, que indican el estado de funcionamiento de las tarjetas SCC (Switch and Control Card) y ULC (Universal Line Card). Este panel sólo presenta un conector serial DB-9 conocido como puerto auxiliar, ya que cada tarjeta SCC contiene un puerto serial principal.

Para realizar tareas de gestión de la red IP, configuraciones iniciales o de diagnóstico u otras actividades, siempre debe utilizarse el puerto serial principal de una de las tarjetas SCC activas en el equipo, a través de la Interfaz de comando de línea (CLI) del sistema operativo TMOS.

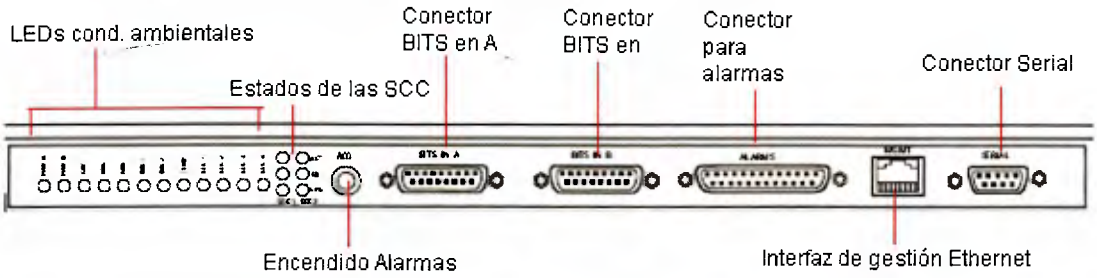


Figura 7. Panel del Sistema del Tellabs 8830.

De las ranuras que se presentan en la parte posterior del equipo (figura 8), cuatro están reservadas para las tarjetas ULC con la característica *hot-swappable,* la cual permite remover o insertar las tarjetas con el equipo en plena operación, sin necesidad de apagar toda la unidad. Las otras dos ranuras restantes son para la instalación de las tarjetas SCC. En caso de ausencia de alguna de las tarjetas, estos espacios deben cubrirse con unos paneles especiales.

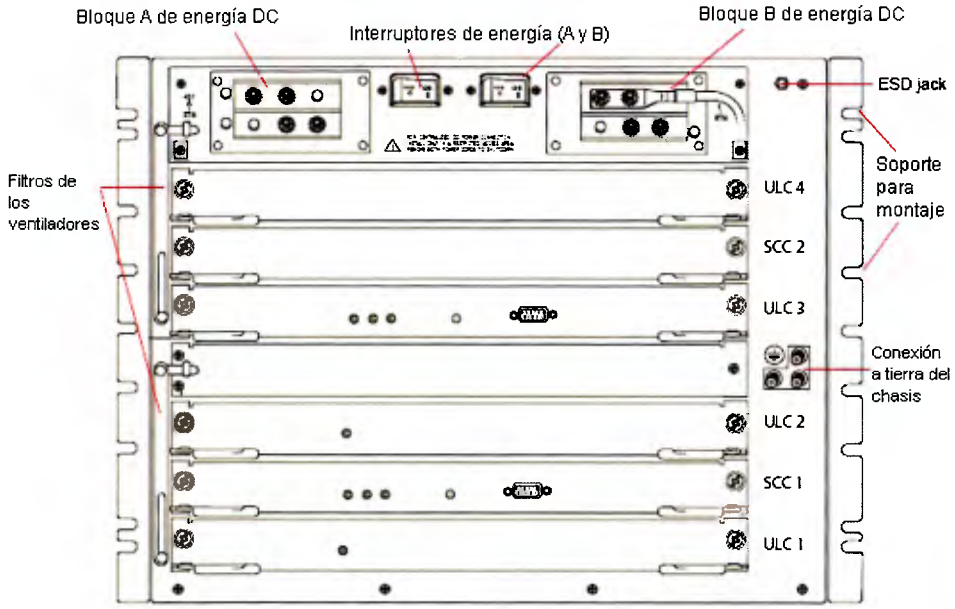


Figura 8. Vista posterior del Tellabs 8820.

Para realizar la configuración inicial del MSR 8830, es necesaria la instalación de al menos una tarjeta SCC, una tarjeta ULC y un módulo PLM, como se describe en la sección 2 del texto *Acceptance Test Manual for Tellabs 8800 series MSR* (TELLABS, 2006).

La versión DC del MSR 8830 cuenta también con dos bloques terminales de poder que deben ser alimentados según los requerimientos especificados en la tabla 5.

Descripción	Mínimo		Nominal	Máximo
Voltaje	-40 VDC	-42 VDC	-48 VDC	-56.7 VDC
Corriente	32.5 A	30.95 A	27.08 A	22.93 A
Máximo Poder	1300 W	1300 W	1300 W	1300 W
Fusible (sugerido)	50 A	50 A	50 A	40 A
Breaker (sugerido)	50 A	40 A	40 A	30 A

Tabla 5. Requisitos de alimentación DC del Tellabs 8830.

Cada uno de estos bloques (figura 8) tiene la capacidad de proveer de energía a todas las tarjetas instaladas, al panel de sistema y al chasis incluyendo ventiladores, LEDs, etc., y es controlado por el interruptor dedicado a ese bloque. El bloque B provee redundancia 1:1 en caso de que el bloque A presente alguna falla o ausencia de corriente. El equipo es capaz de transformar la carga de entrada y producir los voltajes de operación requeridos por cada tarjeta instalada.

Switch and Control Card, SCC

Las tarjetas SCC (figura 9) representan el recurso central para la conmutación de datos, control y funciones de gestión de red del equipo MSR. El panel frontal de la tarjeta cuenta con tres LEDs para representar el estado de funcionamiento, así como un puerto serial DB-9 utilizado para la conexión con la consola (CLI).

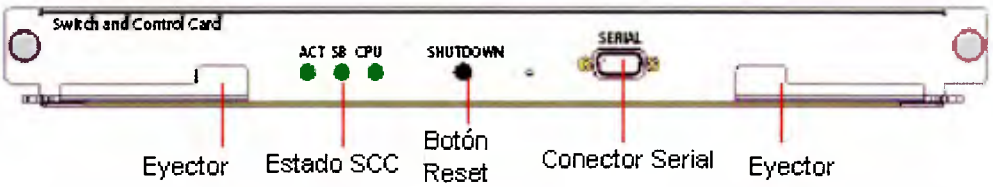


Figura 9. Switch and Control Card.

El chasis del modelo 8830 tiene soporte para la instalación de hasta dos tarjetas SCC, ubicadas entre las ranuras de las tarjetas ULC, diseñadas para proveer redundancia 1:1 automáticamente, incluyendo el intercambio de datos cuando ambas están activas.

Sus principales características técnicas son:

- Procesador PowerPC MPC755 RISC de 400 MHz con cache L2 de 1 MB.
- Memoria PC100 SDRAM de 1 GB.
- Memoria Flash Boot ROM de 4 M.
- Disco duro de 20 GB con 256 MB Flash.

Universal Line Card, ULC

Cada ULC (figura 10) se conecta de manera directa hasta con cuatro PLMs, instalados desde el panel frontal del módulo 8830. El diseño de estos MSR elimina la dependencia entre tarjetas SCCs y ULCs, permitiendo ser removidas del sistema en pleno funcionamiento, mientras existan otras tarjetas que provean redundancia. El modelo 8830 soporta hasta 4 tarjetas ULC.

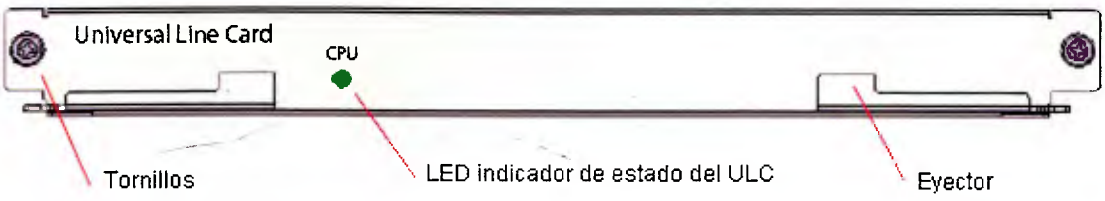


Figura 10. Universal Line Card (ULC).

El procesador que contiene esta tarjeta actúa como procesador de gestión y enrutamiento para el módulo MSR, de forma local.

Algunas de las especificaciones técnicas de estas unidades son:

- Procesador IBM 750FX MPC755 RISC de 400 MHz con cache de 1 MB.
- Memoria PC100 SDRAM de 1 GB.
- Memoria Flash Boot ROM de 4 MB
- Memoria Flash de 256 MB.
- Búsqueda: 50 millones búquedas/segundo.
- Redireccionamiento: 25 millones paquetes/segundo.

Physical Line Modules, PLM

Los PLM son unidades físicas que proveen interfaces ópticas y eléctricas entre los routers y la red. Estas tarjetas son conectadas a los MSR a través de las ULC, mencionadas anteriormente.

A continuación se describen las especificaciones de los PLM que serán utilizados en este trabajo, mencionados en la tabla 1, tomando como referencia el manual *PLM Reference Manual for Tellabs 8800 series MSR* (TELLABS, 2007), el cual puede ser consultado para mayores detalles sobre cada uno.

- *OC-3/STM-1 de 2 puertos*

Este PLM presenta dos puertos independientes SONET/SDH STS-3/STM-1 que trabajan a 155,52 Mbps sobre fibras ópticas monomodo y multimodo para aplicaciones en distancias cortas (2 Km) e intermedias (15 Km). Puede ser instalado en cualquier equipo de la serie Tellabs 8800. En la siguiente figura se aprecia la cara frontal del PLM.

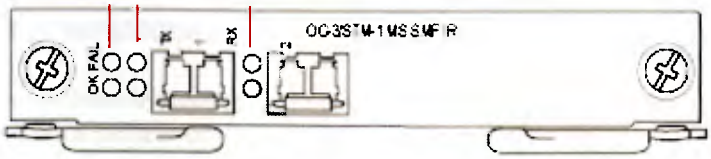


Figura 11. PLM OC-3/STM-1 de 2 puertos.

OC-3/STM-1 brinda soporte a los siguientes protocolos de capa 2:

- Point-to-Point Protocol PPP
- PPP de múltiples niveles
- HDLC (High Level Data Link Control)
- Frame Relay
- Ethernet sobre SONET con 6 canales por cada PLM.

La siguiente tabla especifica las características técnicas del modelo a utilizar.

Código	Descripción	Tipo Aplicación	Tipo de Cable	Potencia promedio Emitida (dBm)	Saturación Sensibilidad (dBm)	Longitud de Onda (nm)	Dist. (Km)
81.8800-PLM003E-20	OC-3/STM-1 de 2 puertos MS PLM SMF IR	IR	Monomodo (LC)	-15 a -8	-8 a -31	1310	15

Tabla 6. Especificaciones Técnicas OC-3/STM-1

- *OC-3c/STM-1 de 4 puertos*

Provee 4 puertos independientes SONET/SDH STS-3/STM-1 que trabajan a una velocidad de 155,52 Mbps sobre fibras monomodo utilizando un conector *LC duplex*. Este PLM se encuentra disponible en versiones para distancias cortas (2 Km), intermedias (15 Km) y largas (40 Km), y brinda soporte a los protocolos PPP, Frame Relay y ATM.

La figura 12 muestra el PLM OC-3c/STM-1 de 4 puertos y la tabla 7 las características técnicas.

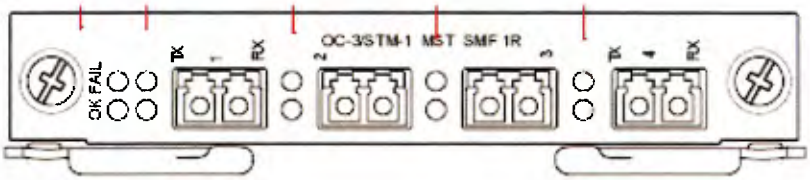


Figura 12. PLM OC-3c/STM-1 de 4 puertos.

Código	Descripción	Tipo Aplicación	Tipo de Cable	Potencia promedio Emitida (dBm)	Saturación Sensibilidad (dBm)	Longitud de Onda (nm)	Dist. (Km)
81.8800-PLM003C-20	OC-3c / STM-1c MS SMF IR	IR	Monomodo (LC)	-15 a -8	-8 a -28	1310	15

Tabla 7. Especificaciones Técnicas OC-3c/STM-1

- *Gigabit Ethernet 1000BaseSX de 4 puertos*

Cuenta con 4 puertos independientes 1000 Base-SX (500mts) para Ethernet Gigabit a través de fibra óptica utilizando conectores MR-RJ o LC. Puede ser utilizado en cualquier modelo de la serie Tellabs 8800. Este modelo se observa en la figura 13.

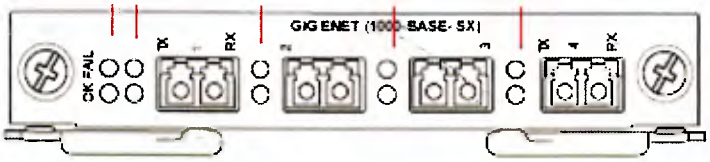


Figura 13. Gigabit Ethernet 1000BaseSx de 4 puertos.

En la siguiente tabla se detallan las especificaciones del modelo de PLM disponible para el proyecto.

Código	Descripción	Tipo Aplicación	Tipo de Cable	Potencia promedio Emitida (dBm)	Saturación Sensibilidad (dBm)	Longitud de Onda (nm)	Dist. (Km)
81.8800-PLMGE-10	Óptico, 4 puertos, GigE 1000 BASE-SX, MMF	1000BASE-SX	Multimodo (LC)	-9.5 a -4	-0 a -17	850	550m

Tabla 8. Especificaciones Técnicas Gigabit Ethernet 1000BaseSX.

- *Fast Ethernet 10/100Base-TX de 24 puertos*

Este PLM, mostrado en la figura 14, provee conexiones con cables de par cruzado compatibles con los estándares Ethernet, con conectividad 10/100Base-TX. El módulo consiste en dos conectores Mini-RJ-21 para 12 puertos cada uno compatibles con los cables del estándar Ethernet. Además, permite remover y reemplazar las conexiones durante su funcionamiento sin afectar otras actividades (*hot swap*). La tabla 9 presenta sus especificaciones.

Figura 14. PLM Fast Ethernet 10/100Base-TX de 24 puertos.

Código	Descripción	Conector	Distancia (mts)
82.8800-PLMFE-10	24-Port Fast Ethernet 10/100Base-TX Mejorado	2 x Mini RJ-21	100

Tabla 9. Especificaciones Técnicas Fast Ethernet 10/100Base TX.

- *DS3/E3 IP/FR de 6 puertos*

Este PLM provee seis puertos T3 o E3 por medio de seis pares de conectores *bayonet* (mini-SMB) como se muestra en la figura 3.15. Algunas de sus características son:

- Selección T3 o E3 por cada puerto.
- Puertos en modo *frame* o *unframed.*
- Selección por puerto independiente de ATM, FR, PPP, HDLC o EoS.
- Indicadores de error por puerto.
- Pueden ser removidas y reemplazadas en sin cortar la alimentación (*hot swap capability).*

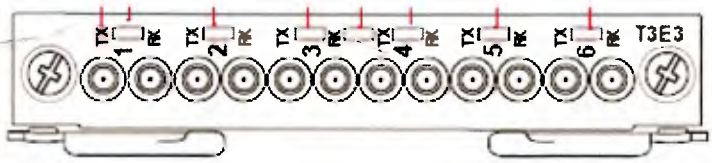


Figura 15. PLM DS3/E3 IP/FR de 6 puertos.

Puede ser instalado en cualquiera de las ranuras dispuestas para PLM de los equipos de la serie 8800.

3. Descripción de la instalación física

3.1. *Cálculo del consumo de energía*

Qty	Descripción del componente	Código	Consumo de energía x unidad (Watts)	Consumo de energía total (Watts)
1	**Tellabs 8820 Multi-service Router Chasis - DC**	**81.8820-DC**	**300**	**300**
1	2port OC-3/STM-1 Multi-Service PLM - (to DS0/E1) SMF IR	81.8800-PLM003E-20	16,5	16,5
1	4port OC-3c/STM-1 Multi-Service PLM - SMF IR	81.8800-PLM003C-20	16,5	13,5
1	4port Gigabit Ethernet PLM - 1000BaseSX (Includes 4 LC/SFP optics)	81.8800-PLMGE-10	13	13
1	24 Port Fast Ethernet 10/100Base-TX PLM	82.8800-PLMFE-10	16,5	16,5
1	**Tellabs 8830 Multi-service Router Chasis - DC**	**81.8830-DC**	**415**	**415**
2	Tellabs 8830 Switch and Control Card	81.8830-SCC-A	165	330
2	Tellabs 8830 2M Universal Line Card	81.8830-ULC-1	90	180
1	4port OC-3c/STM-1 Multi-Service PLM - SMF IR	81.8800-PLM003C-20	13,5	13,5
2	6 Port Clear Channel DS3/E3 IP/FR PLM	81.8800-PLMT3E3-10	16,5	33
1	4port Gigabit Ethernet PLM - 1000BaseSX (Includes 4 LC/SFP optics)	81.8800-PLMGE-10	13	13
1	24 Port Fast Ethernet 10/100Base-TX PLM	82.8800-PLMFE-10	16,5	16,5
	Todos los equipos utilizan -48v DC	**TOTAL**		**1360 W.**

Tabla 10. Consumo de energía.

3.2. *Características mecánicas*

Tellabs 8820

Características	Descripción
Dimensiones del Equipo (cm)	13,3 x 44,1 x 63,5 (alto, ancho, profundo)
Peso del Chasis (Kg)	12,25
Ubicación del equipo	Ver Plano de Elevación de Rack
Adecuación de la Sala Requerida	Sí
Tipo de Anclaje	Tornillo de rosca continua

Tabla 11. Características mecánicas 8820.

Tellabs 8830

Características	Descripción
Dimensiones del Equipo (cm)	35,6 x 44,4 x 59,7 (alto, ancho, profundo)
Peso del chasis con tarjetas (Kg)	72
Ubicación del equipo	Ver Plano de Elevación de Rack
Adecuación de la Sala Requerida	Sí
Tipo de Anclaje	Tornillo de rosca continua

Tabla 12. Características mecánicas 8830.

3.3. Alimentación y cableado

Tellabs 8820

Características	Mínimo	Máximo
Voltaje	-40 VDC	-56.7 VDC
Corriente	--	7,5 Amps (a 40 v)
Consumo de energía (Max.)	300 W	300 W
Fusibles	12 Amps.	15 Amps.
Alimentación Redundante	1:1	
Disponibilidad de Energía DC	Si. –48 VDC, rectificadores	
Disponibilidad de Energía AC	Si. 110 VAC tomas de pared	
Disponibilidad de Panel de Breakers	Sí	
Longitud de cable de Energía Breakers-Equipo	3 mts	
Tipo de cable de Energía	AWG #10	
Longitud de cable de Energía Breakers-Rectificador	10 mts	
Tipo de cable de Energía	AWG #8	

Tabla 13. Características mecánicas 8820.

Tellabs 8830

Características	Mínimo		Nominal	Máximo
Voltaje	-40 VDC	-42 VDC	-48 VDC	-56.7 VDC
Corriente	32.5 A	30.95 A	27.08 A	22.93 A
Consumo de energía (Max.)	1300 W	1300 W	1300 W	1300 W
Fusible (sugerido)	50 A	50 A	50 A	40 A
Breaker (sugerido)	50 A	40 A	40 A	30 A
Alimentación Redundante	1:1			
Disponibilidad de Energía DC	Si. –48 VDC, rectificadores			
Disponibilidad de Energía AC	Si. 110 VAC tomas de pared			
Disponibilidad de Panel de Breakers	Sí			
Longitud de cable de Energía Breakers-Equipo	3 mts			
Tipo de cable de Energía	AWG #8			
Longitud de cable de Energía Breakers-Rectificador	10 mts			
Tipo de cable de Energía	AWG #8			

Tabla 14. Características mecánicas 8830.

4. Pruebas de configuración inicial

Antes de comenzar a trabajar con los equipos, Tellabs en el *Acceptance Test Manual* (2006) de la serie de Multi Service Routers 8800 recomienda realizar una serie de procedimientos de verificación y aceptación los cuales se resumirán a continuación.

Antes de realizar estas pruebas se deben realizar dos pasos importantes:

- Verificar que el hardware del Tellabs 8830 MSR u 8820 MSR está instalado correctamente, y,
- Verificar que una versión actualizada del sistema operativo de Tellabs está instalada.

La verificación del Hardware del equipo se realizará utilizando como base la tabla 15:

Tarea de Instalación	Completada	Tarea de Instalación	Completada
Chasis montado correctamente en el rack	____	PLM´s conectados y cableados correctamente	____
Chasis Aterrado	____	Chasis conectado a alarmas externas	____
Chasis conectado correctamente a UPS	____	Computadora de administración conectada correctamente	____
SCC´s conectados correctamente al chasis	____	Configuración correcta de IP, máscara y gateway por defecto	____
ULC´s conectados correctamente al chasis	____	Poder aplicado correctamente	____
PLM´s conectados correctamente al chasis	____	Boot inicial correcto	____
Los ventiladores funcionan correctamente	____	LED´s encendidos en verde	____
Chasis conectado correctamente a la sincronización T1/E1	____	LED´s de estado de las tarjetas en verde	____

Tabla 15. Verificación del Hardware

A diferencia del 8830, el 8820 por ser un modelo de prueba sólo soporta la agregación de PLM´s; por lo tanto los valores de la tabla que tengan relación con los ULC y SCC sólo deberán ser tomados en cuenta cuando se trabaje con el equipo de Tellabs 8830 MSR.

Es importante saber que el 8830 MSR soporta hasta 4 ULC y 2 SCC instalados horizontalmente, así como 2 PLM´s sobredimensionados que ocupan el mismo espacio que 4 PLM´s regulares. Estos PLM´s sobredimensionados no serán utilizados en el desarrollo de este proyecto.

Para poder trabajar estos equipos necesitan como mínimo:

- Una Fuente AC o DC
- Un sistema operativo de Tellabs
- Por lo menos un SCC (Sólo para el 8830 MSR)
- Por lo menos un ULC (Sólo para el 8830 MSR)
- Por lo menos un PLM

Una vez realizada la verificación de Hardware y del sistema operativo el manual de TELLABS propone un conjunto de procesos de verificación y aceptación mostrados en la tabla 16:

Procesos	Pasos
Verificación	- Verificar la instalación física - Verificar la configuración del software
Configuración	- Configurar las contraseñas
Confirmación de estados	- Verificar el status de los SCC - Verificar el status de los ULC - Verificar el status de los PLM
Pruebas a las tarjetas	- Probar los SCC - Probar los ULC - Probar los PLM
Pruebas a los puertos	- Probar los puertos ópticos - Probar los puertos Fast Ethernet - Probar los puertos DS3
Sincronización	- Establecer los parámetros de sincronización

Tabla 16. Procesos de verificación y aceptación

Al igual que en la tabla anterior los pasos que involucren ULC´s y SCC´s sólo deberán ser tomados en cuenta para el Tellabs 8830 MSR.

Para realizar estas pruebas es necesario estar conectado como administrador al equipo Tellabs 8800 y a través de la interfaz de línea de comando, utilizando el software *Hyperterminal*, acceder al sistema. Conectándose a través del puerto serial (COM1) del PC y el puerto serial MAIN del equipo, se deben configurar los siguientes parámetros en *Hyperterminal*:

- Baud Rate: 9600
- Data: 8 bit
- Parity: None
- Stop: 1 bit
- Flow control: None

5. Pruebas de funcionalidad

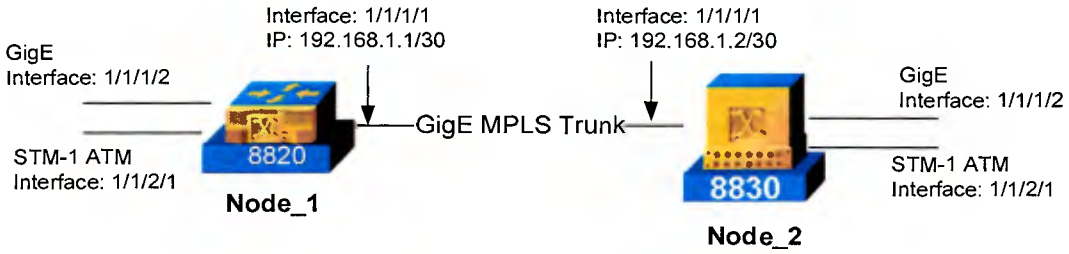
5.1. *Configuraciones básicas MPLS*

El propósito de esta prueba es llevar a cabo la configuración básica de los equipos Tellabs 8820 y 8830 necesaria para configurar una red IP/MPLS. Con esta prueba, CANTV puede verificar el proceso de configuración de los elementos de la red, así como las diferentes opciones disponibles para configurar las interfaces para mostrar las características Cualquier-Puerto Cualquier-Servicio. Estos servicios pueden ser ajustados dinámicamente de acuerdo a las necesidades del mercado.

La realización de estas pruebas será dividida en tres etapas:

- Configuración OSPF
- Configuración del protocolo MPLS
- Configuraciones E-LSP y L-LSP

Se configurará la topología de red mostrada en la figura 16:



Node 1 Configuration:
- Loopback: 10.10.10.1/32
- Mngmt: 192.168.2.1/24

Node 2 Configuration:
- Loopback: 10.10.10.2/32
- Mngmt: 192.168.2.2/24

Figura 16. Topología MPLS.

Las pruebas descritas a continuación se encuentran detalladas en el manual *TMOS User Manual for Tellabs 8800 Series MSR* (76.8800525/4).

Configuración de OSPF

El objetivo de esta prueba es configurar y verificar el funcionamiento de los protocolos OSPF, RSVP-TE y OSPF-TE. Se debe asegurar que las direcciones IP y las direcciones de loopback de las troncales formen parte del proceso OSPF.

OSPF por lo general requiere coordinación con varios enrutadores internos. Si únicamente se configura OSPF básico, se utilizan los parámetros por defecto, sin autentificación e interfaces asignadas a las áreas.

Procedimiento:

Paso 1: Habilitar OSPF Globalmente: entrar al modo de configuración de OSPF, habilitar administrativamente el protocolo OSPF.
Paso 2: Habilitar OSPF en la interfaz a conectar. Asignar la interfaz al área OSPF.
Paso 3: Hacer que la dirección de loopback sea igual a la del identificador del enrutador.
Paso 4: Mostrar y verificar la configuración de OSPF.

Configuración de MPLS

Se debe habilitar MPLS en cada enrutador de manera global y habilitar MPLS-TE para el área 0 de OSPF. Configurar la apropiada interfaz de troncal para MPLS y habilitar RSVP-TE.

Procedimiento:

Paso 1: Habilitar MPLS Globalmente.
Paso 2: Habilitar MPLS y su protocolo de distribución en las interfaces del backbone.

Resultados esperados:

- Verificar que las rutas IGP son distribuidas en la instancia de enrutamiento global.
- Hacer *ping* a las direcciones de loopback de los enrutadores para comprobar el funcionamiento de la red.
- Verificar que los *vecinos OSPF* se encuentran activos, así como IGP.
- Utilizar el comando "show protocol mpls traffic-eng topology ospf extensive" para visualizar la topología de red y anchos de banda disponible.

Configuración E-LSP y L-LSP

Procedimiento:

Paso 1: Configurar un E-LSP con un *committed date rate* de 400 Mbps y *peak data rate* de 990 Mbps.
Paso 2: Configurar 4 L-LSP, uno para cada clase de servicio.

Resultados esperados:

- Verificar que el ancho de banda tomado por el E-LSP ha sido deducido del ancho de banda de la interfaz GigaEthernet.
- Verificar que los 4 L-LSP están activos y en correcto funcionamiento.
- Verificar que el ancho de banda tomado por cada L-LSP para cada clase de servicio ha sido deducido del total del enlace troncal.

5.2. Servicios Capa 2

El propósito de las siguientes pruebas es demostrar el funcionamiento de servicios capa 2 en los equipos *Tellabs 8800* y verificar su correcta operación a través de cinco etapas:

- VPLS
- Circuitos Martini entre puertos capa 2
- VLAN sobre circuitos Martini
- Frame Relay DLCI sobre circuitos Martini
- ATM VPI/VCI sobre circuitos Martini

VPLS

Para la configuración de redes MPLS para el transporte de tráfico LAN a través de instancias de VPLS debe tomarse en cuenta los siguientes aspectos:

- Configurar las mismas instancias de puenteo (*bridging instances)* a través de todos los enrutadores PE (*Provider Edge)*.
- Configurar las interfaces de puenteo entre el enrutador PE y el dispositivo CE (*Customer Edge)* y asociarlas a la instancia de puenteo correcta. De esta forma se identifica que interfaces transportarán tráfico VPLS sobre interfaces PE-to-CE y pseudowires PE-to-PE.
- Configurar circuitos entre PEs asociados a la instancia de puenteo.
- VPLS sobre MPLS requieren que el enrutador PE aprenda las direcciones MAC. La tabla de direcciones MAC almacenadas debe ser verificada.
- Se debe garantizar que cada instancia VPLS esté libre de *loops* dentro de la red MPLS.

Procedimiento:

Paso 1: Configuración de las instancias VPLS en cada nodo 8800.
- Asignación de nombre a cada instancia.
- Habilitación de la instancia.
- Configurar los PE (Provider Edge) que pertenecen a la misma instancia VPLS.

Paso 2: Configuración de las interfaces que van a formar parte de la VPLS. Por ejemplo, la interfaz GigE conectada al equipo Alcatel 7450 o al Tellabs 8600.

Paso 3: Creación de los circuitos que conectan los nodos 8800.

Paso 4: Crear los Pseudowires en los equipos Alcatel 7450 o Tellabs 8600 que conecten los enrutadores CPE a la VPLS.

Resultados esperados:

- ❑ Verificar la configuración del VPLS.
- ❑ Verificar que el circuito VPLS está activo y en funcionamiento.
- ❑ Verificar que es posible hacer *ping* entre los enrutadores CPE.
- ❑ Verificar que las direcciones MAC son intercambiadas entre enrutadores CPE.

- Verificar que es posible el envío de tráfico entre enrutadores CPE.
- Verificar las estadísticas en los *Tellabs 8800* a través del comando "show protocol mpls lsp name POTS stats".

Circuitos Martini entre puertos capa 2

Configurar un circuito Martini entre dos puertos Fast Ethernet de los nodos 1 y 2 con los siguientes parámetros:

Nombre del circuito: **PSWE**
Tipo: **Ethernet**
Side ID 1: **fe-1/1/1/1**
Side ID 2: **Dynamic LSP**, Destino: **192.168.120.253**, Nombre del LSP: **DATA_DSL**
VCID = **123**
Clase del servicio: **UBR** Tasa máxima de datos = **5,000**

Procedimiento:

Paso 1: Configuración de Pseudowires en las interfaces de los puntos finales en ambos nodos.
Paso 2: Creación de los circuitos Pseudowires entre ambos nodos.

Resultados esperados:

- Verificar que los puertos Ehternet basados en circuitos Martini pueden crearse.
- Verificar que a diferentes puertos se le pueden asignar diferentes clases de servicios.
- Verificar que se pueden asignar circuitos estáticamente a rutas LSP.
- Verificar que cada circuito consume ancho de banda disponible del E-LSP.
- Verificar que el tráfico puede ser enviado entre los dos puertos Fast Ethernet a una tasa máxima de 5 Mbps.

VLAN sobre circuitos Martini

Configurar circuitos Martini entre dos puertos Fast Ethernet (VLAN) entre nodos 1 y 2 con los siguientes parámetros:

Nombre del circuito: **PSWE-VLAN**
Tipo de circuito: **Ethernet**
Side ID 1: **fe-1/1/1/2.1**
VLAN-ID: **123**
Side ID 2: **Dynamic LSP**, Destino: **192.168.120.253**, Nombre del LSP: **DATA_DSL**
VCID = **1234**
Clase de Servicio: **CBR-ssx** Tasa máxima de datos = **5,000**

Nota: La única diferencia entre esta, y la prueba anterior, es que el Pseudowire será creado basado en la VLAN configurada sobre la interfaz Fast Ethernet.

Procedimiento:

Paso 1: Configuración de Pseudowires en las interfaces de los puntos finales en ambos nodos.
Paso 2: Creación de los circuitos Pseudowires entre ambos nodos.

Resultados esperados:

- Verificar que la VLAN Ethernet basada en circuitos Martini pueda ser creada.
- Verificar que diferentes VLAN pueden ser asignadas a diferentes clases de servicio.
- Verificar que el circuito puede ser asignado de manera dinámica a la ruta LSP.
- Verificar que cada circuito consume ancho de banda disponible del LSP seleccionado.
- Verificar el envío de tráfico entre las dos VLANs a un máximo de 5 Mbps.

Frame Relay DLCI sobre circuitos Martini

Configurar un circuito Martini entre dos puertos DS3 (FR DLCI) en los nodos 1 y 2 con los siguientes parámetros:

Nombre del circuito: **PSWE-FR**
Tipo de circuito: **FrameRelay**
Side ID 1: **ds3**
VLAN-ID: **123**
Side ID 2: **Dynamic LSP**, Destino: **192.168.120.253**, Nombre del LSP: **DATA_DSL**
VCID = **1234**
Clase de Servicio: **CBR-ssx** Tasa máxima de datos = **5,000**

Resultados esperados:

- Verificar que Frame Relay DLCI basada en circuitos Martini pueda ser creada.
- Verificar que el circuito puede ser asignado de manera dinámica a la ruta LSP.
- Verificar que cada circuito consume ancho de banda disponible del LSP seleccionado.
- Verificar el envío de tráfico entre las dos interfaces Frame Relay a un máximo de 5 Mbps.

ATM VPI/VCI sobre circuitos Martini

Configurar un circuito Martini entre dos puertos OC-3c (ATM) en los nodos 1 y 2 con los siguientes parámetros:

Nombre del circuito: **PSWE-ATM**
Tipo de circuito: **ATM**
Side ID 1: **ATM**
VLAN-ID: **123/123**
Side ID 2: **Dynamic LSP**, Destino: **192.168.120.253**, Nombre del LSP: **DATA_DSL**
VCID = **1234**
Clase de Servicio: **CBR-ssx** Tasa máxima de datos = **5,000**

Resultados esperados:

- Verificar que ATM VCI/VPI basada en circuitos Martini pueda ser creada.
- Verificar que el circuito puede ser asignado de manera dinámica a la ruta LSP.
- Verificar que cada circuito consume ancho de banda disponible del LSP seleccionado.
- Verificar el envío de tráfico entre los dos conmutadores ATM a un máximo de 5 Mbps.

5.3. Servicios Capa 3

El propósito de esta prueba es demostrar cómo se crean los servicios capa 3 en los Tellabs 8800 y verificar su correcto funcionamiento.

Procedimiento:

Paso 1: Configuración del protocolo de enrutamiento. Para este caso se utilizará el protocolo de enrutamiento BGP. Como identificador del enrutador se utilizará la dirección de *loopback* y se utilizara 6500 como número de sistema autónomo.

Paso 2: Configuración de la instancia de enrutamiento IP-VPN llamada vpn2 para uno de los nodos, en este caso para el 8830:
- Asignar un nombre a la instancia VPN.
- Habilitar la instancia.
- Configurar el diferenciador de rutas 6500:1. Este comando se utiliza para diferencia las direcciones entre VPN´s.
- Configurar la ruta importación / exportación 100:200.

Paso 3: Configurar la instancia de enrutamiento BGP para cada nodo. Esto se logra distribuyendo la información desde el 8830.

Paso 4: Configurar dos interfaces Fast Ethernet en el nodo 1 y 2 para que sean parte de la VPN, utilizando las siguientes direcciones:
- 60.60.60.1/24 (Para el primer puerto)
- 70.70.70.1/24 (Para el primer puerto)

Paso 5: Definir los pares internos BGP (iBGP).

Resultados esperados:

- Verificar la configuración iBGP.
- Verificar que iBGP está habilitado y funcionando.

- Verificar que la VPN se ha creado.
- Verificar las tablas de enrutamiento.
- Verificar que se puede enviar tráfico a través de 2 enrutadores CPE conectados a los equipos Tellabs 8800.

5.4 Service Interworking

El propósito de las siguientes pruebas es demostrar la interoperabilidad a nivel de capa 2 implementada en los equipos Tellabs 8800 y verificar su correcto funcionamiento.

Cuando diferentes nubes de servicios como ATM, Frame Relay o Ethernet están separadas geográficamente, la interoperabilidad entre estos servicios se puede proveer a través de una nube multi-servicio. Esto se puede hacer sin la necesidad de extender el núcleo de una nube hasta el acceso de otra. A continuación se describen los tres tipos de servicios Interworking que serán configurados.

ATM / Ethernet Interworking

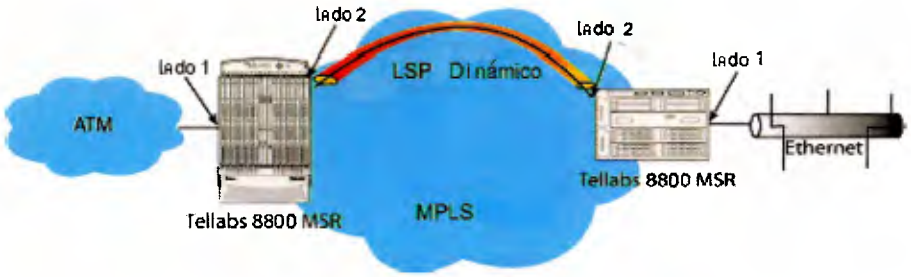


Figura 17. ATM/Ethernet Interworking.

Procedimiento:

Paso 1: Configuración del equipo que conecta directamente la nube ATM:
- Configurar el lado 1.
- Configurar el lado 2 como un LSP dinámico.

Paso 2: Configuración del equipo que conecta directamente a Ethernet:
- Configurar el lado 1.
- Configurar el lado 2 como un LSP dinámico.

Resultados esperados :

- Verificar que la interoperabilidad de circuitos Martíni ATM-Ethernet puede ser creada.
- Verificar que cada circuito consume ancho de banda del TE disponible en el E-LSP.
- Verificar que el tráfico puede ser enviado entre los 2 nodos CPE.

FR / Ethernet Interworking

Procedimiento:

Paso 1: Configuración del lado 1 del circuito indicando la interfaz Ethernet
Paso 2: Configuración del lado 2 del circuito especificado el valor de DLCI y la interfaz FR.

Resultados esperados:

- Verificar que la interoperabilidad de circuitos Martíni Frame Relay-Ethernet puede ser creada
- Verificar que cada circuito consume ancho de banda del TE disponible en el E-LSP
- Verificar que el tráfico puede ser enviado entre los 2 nodos CPE

6. Pruebas de Calidad de Servicio, QoS

Procedimiento:

Paso 1: Configurar la plantilla de parámetros de tráfico
Paso 2: Levantar la lista de acceso basada en direcciones MAC.
Paso 3: Crear el grupo de Calidad de Servicio.
Paso 4: Configurar la lista de control acceso y asociarla al VPLS previamente configurado.
Paso 5: Asignar el grupo de Calidad de Servicio y la lista de control de acceso a la Interfaz.
Paso 6:

Resultados esperados:

- Verificar que la configuración de QoS puede ser creada.
- Verificar que puede fluir tráfico entre ambos puntos de la red.
- Verificar la clase de tráfico que atraviesa el LSP y coincide con la configurada.

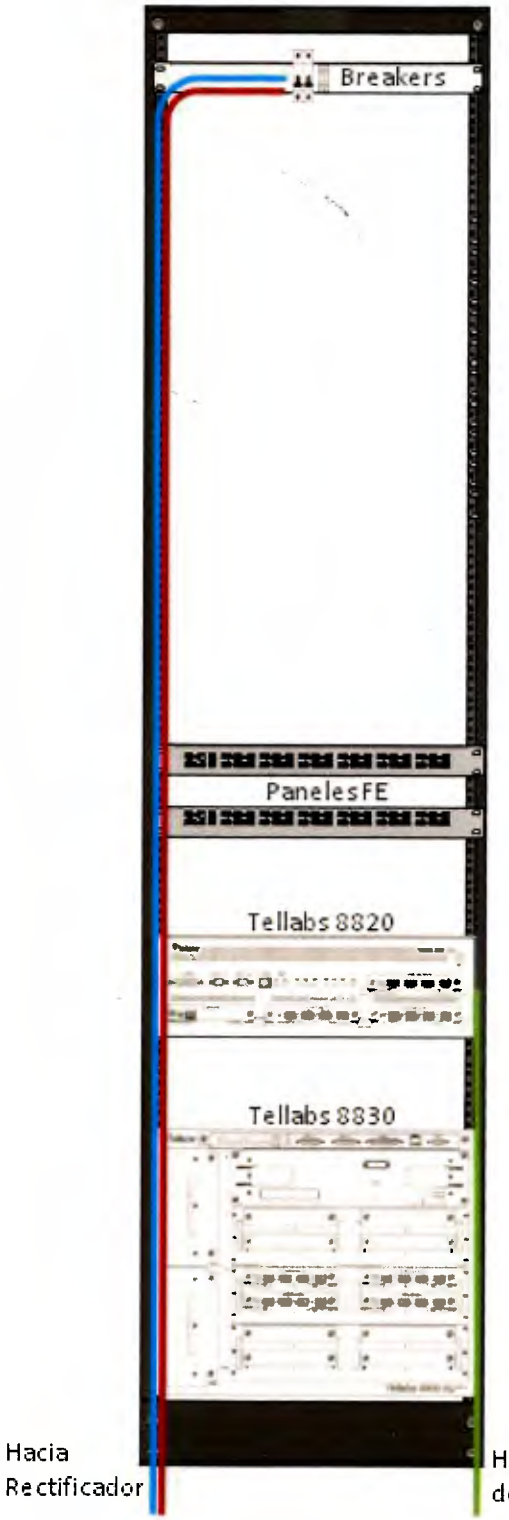
7. Memoria Fotográfica y Planos

7.1. Ubicación Rack

7.2. Bus de Tierra

7.3. Panel de Breakers DC

7.4. Escalerillas acceso inferior rack

7.5. Escalerillas hacia sala contigua

Plano Elevación Rack