ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO EN INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES

ANÁLISIS DE INTEROPERABILIDAD DE LOS ESQUEMAS DE PROTECCIONES ENTRE EQUIPOS MULTIPLEXORES SDH DE CELEC EP - TRANSELECTRIC

AUTOR: SANTIAGO ALEXIS MORALES VALENCIA

SANGOLQUÍ – ECUADOR

ENERO DE 2013

ESCUELA POLITÉCNICA DEL EJÉRCITO

INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

SANTIAGO ALEXIS MORALES VALENCIA

DECLARO QUE:

El proyecto de grado denominado “ANÁLISIS DE INTEROPERABILIDAD DE LOS ESQUEMAS DE PROTECCIONES ENTRE EQUIPOS MULTIPLEXORES SDH DE CELEC EP - TRANSELECTRIC”, ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan al pie, de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, Enero de 2013

_____

Santiago Alexis Morales Valencia

ESCUELA POLITÉCNICA DEL EJÉRCITO

INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES

CERTIFICACIÓN

ING. DARWIN AGUILAR
ING. JORGE ÁLVAREZ

C E R T I F I C A N

Que el trabajo titulado "ANÁLISIS DE INTEROPERABILIDAD DE LOS ESQUEMAS DE PROTECCIONES ENTRE EQUIPOS MULTIPLEXORES SDH DE CELEC EP - TRANSELECTRIC", realizado por Santiago Alexis Morales Valencia , ha sido guiado y revisado periódicamente y cumple normas estatutarias establecidas por la ESPE, en el Reglamento de Estudiantes de la Escuela Politécnica del Ejército.

El mencionado trabajo consta de un documento empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (PDF). Autorizan a Santiago Alexis Morales Valencia que lo entregue al Ingeniero Darío Duque, en su calidad de Director de la Carrera.

Sangolquí, Enero de 2013

_____	_____
Ing. Darwin Aguilar	Ing. Jorge Álvarez
Director	**Codirector**

AGRADECIMIENTO

A la Escuela Politécnica del Ejército, que me acogió durante un largo periodo de mi vida para formar mi carácter, mi capacidad de razonamiento y en conclusión por enseñarme a ser libre mediante el conocimiento.

Al Ing. Darwin Aguilar, Director de tesis de grado, por guiarme en cada uno de los pasos que debía tomar para el desarrollo de este proyecto con paciencia y objetividad.

Al Ing. Jorge Álvarez, Codirector, por su apoyo constante para la ejecución de este proyecto, por su comprensión, interés e incentivo para la finalización de esta meta.

A mi madre, por ser la gran amiga que me ayudó en cada lapso de mi vida mediante su amor incondicional, ejemplo y guía pese a las adversidades. Por ser mi más grande ejemplo a seguir y siempre darme ese ánimo que me lleva a continuar mirando hacia adelante.

A mi padre, por darme el empuje espiritual desde el cielo; porque sé que donde quiera que él esté, siempre estará a mi lado guiándome, cuidándome y encaminándome sin que yo lo viese.

A mi hermana querida, por recibir su apoyo incondicional cuando más lo necesité, por estar siempre a mi lado en muchos momentos por difíciles que estos fueran, por ser conjuntamente con mi madre las dos mujeres más importantes en mi vida.

A mi familia materna, porque en su seno he encontrado permanente comprensión, cariño y apoyo incondicional.

A todo el personal de la Gerencia de Telecomunicaciones de CELEC EP – TRANSELECTRIC, puesto que depositaron su entera confianza en mí y abrieron sus puertas brindándome todo lo necesario para poder culminar mi proyecto de grado.

A mis tutores, Ing. Paulina Criollo e Ing. Alejandro Castillo, quienes a más de ser mí guía en el desarrollo del proyecto de tesis son amigos a quienes admiro y aprecio mucho. Ellos fueron un pilar muy importante para llevar a cabo este propósito.

DEDICATORIA

A mi madre...

Ya que este logro y primer paso en mi vida profesional se da gracias a su esfuerzo, trabajo y dedicación por cultivar una enseñanza de valores humanos y espirituales sin importar las adversidades de la vida; porque de su sacrificio diario obtuve todo para poder educarme; extiendo mi compromiso de continuar entregándole satisfacciones sin importar lo duro que esto signifique para alcanzarlas, ya que ella es y seguirá siendo un ejemplo a seguir tanto como madre, mujer, amiga y profesional.

A mi hermana…

Puesto que ha sido mi compañera de juegos y travesuras yendo desde la infancia hasta hoy convertirse en mi gran amiga y consejera. Gracias a ti he visto un impulso extra para seguir adelante sabiendo que los dos siempre seremos triunfadores como lo quiere nuestra madre y como lo hubiese querido nuestro padre.

A Fabricio Vizuete…

Dios tenía planes diferentes para ti amigo, tuviste que partir para dejarme de enseñanza muchas cosas buenas. Gracias por compartir algunos años del colegio y universidad; lo prometí cuando partiste hacia el cielo y lo cumplí. Gracias amigo Panda. Fuiste y seguirás siendo uno de mis mejores amigos.

Con amor y cariño, Santiago Alexis Morales Valencia.

PRÓLOGO

CELEC EP - TRANSELECTRIC como empresa de transporte de servicios de telecomunicaciones brinda a sus clientes alta calidad y disponibilidad en su red de fibra óptica, manteniendo un excelente nivel tecnológico para el control y gestión de los servicios.

Debido a la alta demanda de servicios de voz, datos e internet se está fomentando la creación de redes de transporte de gran capacidad; la pérdida de un enlace de este tipo podría dejar fuera de funcionamiento una cantidad considerable de servicios. Para evitar interrupciones, las redes de hoy se deben diseñar para ser auto recuperables y tolerantes a fallos.

El estándar SDH se ha aceptado extensamente en la industria de las telecomunicaciones a través del mundo. Una de las razones principales del éxito de este estándar es la funcionalidad de supervivencia de la red.

Las actuales redes de telecomunicaciones se caracterizan por un constante incremento del número, complejidad y heterogeneidad de los recursos que los componen; que dificultan enormemente gestionar el rendimiento, encontrar y solucionar problemas, y planificar el crecimiento futuro de la red.

Por ello, la interoperabilidad entre sistemas de gestión de los diferentes fabricantes y sus esquemas de protección son de suma importancia para la administración general de la red de transporte SDH.

ÍNDICE DE CONTENIDO

CAPÍTULO I

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

CAPÍTULO V

CAPÍTULO VI

CAPÍTULO I

INTRODUCCIÓN

GENERALIDADES DEL PROYECTO

CELEC EP - TRANSELECTRIC al ser una empresa líder en el campo de telecomunicaciones en el país, posee la red de fibra óptica más grande de Ecuador, con conexiones a Perú y Colombia gracias a Transnexa, filial de ISA (Internexa S.A).

Estas condiciones hacen que tanto empresas grandes, medianas y pequeñas deseen contratar servicios con CELEC EP - TRANSELECTRIC, por lo tanto es deber de la empresa mantener una alta disponibilidad en su red de fibra óptica con el uso de protecciones y sistemas anillados. Es por esto la necesidad de probar la interoperabilidad en la red de transporte SDH de las diversas protecciones que hoy existe con respecto a las marcas de equipos que se posee el área de Telecomunicaciones de CELEC EP - TRANSELECTRIC. La finalidad del proyecto es probar los múltiples tipos de protecciones para la red de transporte SDH en el tendido de fibra óptica que se posee en todo el país, tanto en topologías en anillo como en topologías lineales, con las marcas de multiplexores SDH SIEMENS y HUAWEI.

Puesto que la red de fibra óptica que posee CELEC EP - TRANSELECTRIC es muy amplia y que todos sus clientes son importantes, no se puede generar indisponibilidad en los servicios para efectuar las pruebas. Las mismas se realizarán en tramos aislados tanto en topologías en anillo como en topologías lineales, con el fin de no afectar ningún servicio.

En lo que respecta a equipos multiplexores, las marcas a utilizar serán SIEMENS y HUAWEI tanto en topologías lineales como en anillo. Se utilizarán equipos SMA 16 en versiones 4.2 y 4.3, hiT7070 Single Core (SC) y Doble Core (DC) y OSN 3500 y OSN 7500 respectivamente para realizar pruebas en tramos donde se analizará el tráfico entrante y saliente, además del grado de importancia de los clientes para determinar con exactitud los nodos con los cuales se harán las pruebas de interoperabilidad con las dos marcas de multiplexores y los diferentes tipos de protecciones para redes de transporte SDH.

El objetivo del proyecto es analizar la interoperabilidad de estos equipos multiplexores probando por lo menos un tipo de protección en línea y un tipo de protección en anillo para la red de transporte SDH de CELEC EP - TRANSELECTRIC.

PRINCIPIOS BÁSICOS DE LA TECNOLOGÍA DE TRANSPORTE SDH

Las redes troncales en el Área de Telecomunicaciones transportan tráfico de diferentes fuentes mediante la compartición de sistemas de transmisión y conmutación entre distintos usuarios. La capacidad de los enlaces entre centrales de conmutación varía, desde las tasas mínimas, correspondientes a centrales locales, periferia de la red troncal, etc.; hasta las tasas más altas, requeridas, por ejemplo, por los enlaces entre grandes centrales de conmutación.

Actualmente estamos viviendo una gran explosión en la demanda de servicios sofisticados de Telecomunicaciones, servicios tales como video conferencias, acceso a bases de datos remotas y transferencia de archivos multimedia, por lo que se requiere de una red que tenga la habilidad de ser lo suficientemente flexible para tener virtualmente un ancho de banda ilimitado. Por lo tanto surge la necesidad de definir un estándar internacional de comunicaciones que permita manejar y supervisar con facilidad esta capacidad de transporte, este estándar se denomina SDH (Síncronos Digital Hierarchy, Jerarquía Digital Sincrónica).

SDH permite una revolución en los servicios de Telecomunicación que significa grandes cambios para usuarios finales, operadoras y fabricantes de equipos de telecomunicaciones. Para comenzar el análisis de la tecnología SDH es preciso mencionar las barreras y aspectos generales de su antecesor PDH (Plesiochronous Digital Hierarchy, Jerarquía Digital Plesiócrona).

PDH surgió como respuesta a la necesidad de transmisión de voz POST (Plain Old Telephone Service, Servicio Telefónico Tradicional), el cual no fue diseñado para tener una entrega eficiente de datos, ni conexiones que requieran el manejo de un gran ancho de banda. Los equipos PDH coparon el mercado de la transmisión hasta principios de los años 90, estando actualmente en pleno declive frente a SDH, salvo en sistemas de radio. La velocidad de transmisión mínima utilizada en Europa es 2,048 Mbps (El) y en Estados Unidos, Canadá y Japón es 1,544 Mbps (TI).

Una señal de voz con calidad telefónica es limitada en la banda de 0,3 a 3,4 kHz (su ancho de banda es 3,1 kHz), se toma una frecuencia máxima nominal de 4 kHz para muestrear a una frecuencia de 8 kHz (es decir una muestra cada 125 µs) y se suele utilizar una representación con 8 bits por muestra (256 niveles de cuantificación), para luego ser transmitida a una tasa binaria de 64 kbps. En el sistema norteamericano se multiplexan 24 canales de 64 kbps para formar el T1 y en el europeo son multiplexados 32 (30+2) canales para integrar el El, de los cuales 2 canales son para señalización y sincronización.

El sistema PDH europeo es el más utilizado en Latinoamérica y especialmente en nuestro país, los canales a multiplexar se unen formando tramas de nivel superior a capacidades estandarizadas de 2 Mbps, 8 Mbps, 34 Mbps, 140 Mbps y 565 Mbps, el método de multiplexación a partir de la segunda jerarquía se realiza bit a bit, que es una de las barreras de PDH, para poder manejar altas tasas de transmisión que en la actualidad se hace necesario para el uso de sofisticadas aplicaciones demandadas por los usuarios.

Otra limitación que se puede identificar es la falta de sincronismo entre los equipos, PDH es *plesiócrona* (casi sincrónica), significa que no todas las señales

multiplexadas proceden de equipos que transmiten a la misma velocidad de transmisión, para poder igualar las velocidades de las fuentes se añade o se retira bits al multiplexar o demultiplexar en cada uno de los niveles de la jerarquía, a estos bits se denomina bits de justificación. Esta falta de sincronización obliga a implantar complicadas y caras técnicas de relleno.

Además, los estándares de la jerarquía PDH solo se encuentran en algunas regiones como: Europa: ETSI *(European Telecommunications Standards Institute,* Instituto Europeo de Normas de Telecomunicaciones), Norte América: ANSI *(American National Standards Institute,* Instituto Nacional Estadounidense de Estándares) y Japón: JSA *(Japanese Standards Association,* Asociación de Estándares Japoneses), este hecho causa dificultades para la administración de la red, la interconexión entre redes y la forma de estructurar las redes.

Por ejemplo, en PDH de Europa las capacidades superiores a los 140 Mbps, manejan códigos de línea propietarios; es decir, no han sido estandarizados. Todas las limitaciones antes mencionadas de la jerarquía PDH son hoy en día solucionadas por la jerarquía SDH.

En los primeros años de la telefonía analógica se utilizaba multiplexación por división en frecuencia o FDM *(Frecuency Division Multiplexing)* para transportar un determinado número de canales telefónicos sobre un único cable coaxial. La idea de todo esto era modular cada canal telefónico en una frecuencia portadora distinta para desplazar las señales a rangos de frecuencia distintos. Los sistemas de transporte analógicos han sido ahora abandonados y reemplazados por sistemas de transporte digitales, donde la señal telefónica es digitalizada, es decir, es convertida en una ristra de bits para su transmisión por la línea. Para ello la señal telefónica analógica es muestreada a una frecuencia de 3,1 kHz, cuantificada y codificada y después transmitida a una tasa binaria de 64 kbps. Mediante la modulación de impulsos codificados o PCM *(Pulse Code Modulation),* que apareció en la primera década de los 60. PCM permite la utilización múltiple de una única línea por medio de la multiplexación por división en el tiempo o TDM *(Time Division Multiplexing),* consistente en segregar muestras de cada señal en

ranuras temporales que el receptor puede seleccionar mediante un reloj correctamente sincronizado con el transmisor.

El primer estándar de transmisión digital fue PDH, pero sus limitaciones resultaron en el desarrollo de SONET y SDH. Las dos tecnologías se basan en multiplexores digitales que, mediante técnicas de multiplexación por división en el tiempo o TDM permiten combinar varias señales digitales (denominadas señales de jerarquía inferior o señales tributarias) en una señal digital de velocidad superior. La última tecnología de transmisión en aparecer, ha sido DWDM *(Dense Wavelength Division Multiplexing)*, caracterizada por su alta capacidad de transmisión, su transparencia sobre los datos de jerarquías inferiores, y por una transmisión totalmente óptica.

1.1.1 Concepto de SDH

Todas las carencias presentadas por PDH propiciaron la definición entre 1988 y 1992 de un nuevo estándar mundial para la transmisión digital denominada SDH *(Syncronous Digital Hierarchy)* o JDS *(Jerarquía Digital Síncrona)* en Europa, y SONET *(Syncronous Optical NETwork)* en Norte América. Mientras SONET es un estándar concebido por Bellcore y definido por el ANSI[1] para ser utilizado en Norte América, SDH es un estándar definido por el sector de estandarización de telecomunicaciones de la unión internacional de telecomunicaciones ó ITU-T[2] para su uso en todo el mundo y compatible en parte con SONET. Aunque SONET y SDH fueron concebidos originalmente para la transmisión por fibra óptica, existen sistemas radio a tasas compatibles con SONET y SDH.

El principal objetivo en la definición de SDH era la adopción de una verdadera norma mundial que posibilitara una compatibilidad máxima entre diferentes suministradores y operadoras. Este estándar especifica velocidades de transmisión, formato de las señales (tramas de 125 µs), estructura de

[1] Instituto Nacional Americano de Estándares.
[2] (International Telecommunication Union-Standarization): Sector de Normalización de la Unión Internacional de Telecomunicaciones.

multiplexación, codificación de línea, parámetros ópticos, etc.; así como normas de funcionamiento de los equipos y de gestión de red. Por otro lado, SDH aportará a la red con una mayor flexibilidad, un mejor aprovechamiento del ancho de banda potencial de la fibra óptica, y más capacidad de monitorización de la calidad y gestión centralizada.

El estándar SDH define interfaces de tráfico que son independientes de los distintos equipos, denominadas módulos de transporte síncrono o STM-n *(Syncronous Transport Module).* El nombre que reciben estas interfaces en SONET son los de señal de transporte síncrono o STS *(Syncronous Transport Signal)* en la interfaz cobre y contenedor óptico u OC *(Optical Carrier)* en la interfaz óptica. En SDH se parte de una señal de 155 Mbps denominada módulo de transporte síncrono de primer nivel o STM-1, definida tanto para interfaz óptica como de cobre.

En SONET, sin embargo, se parte de una señal de 51,84 Mbps denominada señal de transporte síncrono de primer nivel ó STS-1 en la interfaz cobre, o bien contenedor óptico de primer nivel ó OC-1 en la interfaz óptica.

Los restantes STM-n, definidos exclusivamente para la interfaz óptica, se obtienen mediante el entrelazado de bytes de varias señales STM-1. En la actualidad se encuentran normalizados los valores de: STM-4 (622 Mbps), STM-16 (2,5 Gbps). STM-64 (10 Gbps) y STM-256 (40 Gbps); que, como vemos, son múltiplos enteros de 155 Mbps en una secuencia de n x 4. Seleccionando las opciones adecuadas, un subconjunto de SDH es compatible con un subconjunto de SONET; por consiguiente, es posible la interoperabilidad del tráfico entre nodos de SDH de SONET. No obstante, no es posible la interoperabilidad de alarmas y la supervisión de calidad entre ambos sistemas.

Las dos tecnologías, PDH y SDH, se basan en multiplexores digitales que, mediante técnicas de TDM, permiten combinar varias señales digitales (denominadas señales de jerarquía inferior o señales tributarias) en una señal digital de velocidad superior. En ambos sistemas, la fibra óptica se utiliza como sistema de transmisión, puesto que las funciones de amplificación,

encaminamiento, extracción e inserción de señales, etc., se realizan en el dominio eléctrico.

SDH trabaja con una estructura o trama básica denominada STM-l, que tiene una duración de 125 µs (se repite 8.000 veces por segundo), y se corresponde con una matriz de 9 filas y 270 columnas, cuyos elementos son octetos de 8 bits; por consiguiente, la trama tiene una velocidad binaria de (9 x (270 x 8)) x 8.000 = 155,520 kbps. La transmisión se realiza fila por fila, empezando por el byte en la esquina superior izquierda y terminando en el byte en la esquina inferior derecha. En la trama STM-1 se distinguen tres áreas: la tara de sección, los punteros de justificación y la carga útil. Cada byte de la carga útil se corresponde con un canal de 64 kbps, de modo que cada columna de 9 bytes se corresponde con 576 kbps. Las primeras 9 columnas contienen la tara de sección o SOH *(Section OverHead)* para soportar características del transporte tales como el alineamiento de trama, los canales de operación y mantenimiento, la monitorización de errores, etc. Se distingue entre la tara de la sección de regeneración o RSOH *(Regenerator Section OverHead)* y la tara de sección de multiplexación o MSOH *(Multiplex Section OverHead).* Las columnas siguientes pueden ser asignadas de diversas formas para transportar las señales de tasas de bit inferior, tales como los 2 Mbps; cada columna tiene su propia tara.

El estándar SDH está definido originalmente para el transporte de señales de 1,5 Mbps, 2 Mbps, 6 Mbps, 34 Mbps, 45 Mbps y 140 Mbps a una tasa de 155 Mbps, y ha sido posteriormente desarrollado para transportar otros tipos de tráfico, como por ejemplo ATM ó IP, a tasas que son múltiplos enteros de 155 Mbps. La flexibilidad en el transporte de señales digitales de todo tipo permite, de esta forma, la provisión de todo tipo de servicios sobre una única red SDH: servicio de telefonía, provisión de redes alquiladas a usuarios privados, creación de redes WAN, servicio de videoconferencia, distribución de televisión por cable, etc.

1.1.2 Formato de Tramas

El contenedor o C-n *(Container)* es la unidad básica de empaquetamiento para los canales tributarios. Se tiene un contenedor especial para cada señal tributaria de PDH (ITU-T G.703[3]): C-4 para señales de 140 Mbps, C-3 para 45 y 34 Mbps, C-2 para 6,3 Mbps, C-12 para 2 Mbps, y C-l1 para 1,5 Mbps. Estos contenedores tienen siempre un tamaño mayor que la carga a transportar. La capacidad remanente es utilizada, en parte, para la justificación; con el fin de eliminar las desviaciones temporales entre las señales PDH (siempre dentro de las tolerancias establecidas por el ITU-T). Cuando se hace la correspondencia con tributarios síncronos, se insertan bytes de relleno fijos, en vez de bytes de justificación.

Un contenedor virtual o VC-n *(Virtual Container)* es el conjunto de un contenedor y la tara de trayecto. La tara de trayecto o POH *(Path OverHead)* tiene corno misión monitorizar la calidad e indicar el tipo de contenedor; por lo tanto, el formato y tamaño del POH depende del tipo de contenedor. El VC es la entidad de carga útil que viaja sin cambios a lo largo de la red, siendo creada y desmantelada en los distintos puntos de acceso o terminación del servicio de transporte. El siguiente paso para formar la señal STM-n completa, consiste en añadir un puntero en una posición fija indicando el comienzo del VC dentro de la trama. En consecuencia, el VC puede flotar dentro del área de carga que le es destinado, debiendo como consecuencia, alinearse el puntero. La unidad formada por el puntero y el VC se denomina unidad administrativa o AU-n *(Administrative Unit),* o bien unidad tributaria o TU-n *(Tributario Unit).* Después, se realiza un simple proceso de multiplexación por entrelazado de byte de un conjunto de TUs, obteniendo una estructura denominada grupo de unidades tributarias o TUG-n *(Tributary Units Group).* Este proceso es completamente síncrono. Una o más unidades administrativas forman un grupo de unidades administrativas o AUG *(Administrative Unit Group).* Finalmente, se debe dotar a la estructura obtenida de información adicional que permita su transporte por el

[3] Estándar de la UIT-T que define las características físicas y eléctricas de la interfaz para transmitir voz o datos sobre canales digitales tales como los E1 (hasta 2048 kbit/s) ó T1 (equivalente US de 1544 kbit/s).

medio físico, es decir, del SOH. El grupo de unidades administrativas junto a la SOH forman el STM-n. En un STM-n no se utilizan todos los bytes de información de control de todos los STM-1s, sino que las funciones de algunos bytes se realizan con la información contenida en los bytes correspondientes del primer STM-1.

Las taras u OHs son bytes reservados para la información del propio sistema. Parte de ellos son asignados a los VCs y otros a los STM´s. La información contenida en las taras se utiliza básicamente para el monitoreo de la calidad, detección de errores, canales de comunicaciones, canales de datos, protección automática, etc. La tara de trayecto o POH se asigna al contenido útil al multiplexarse en el VC, permaneciendo con este VC hasta que sea demultiplexada la carga útil. De esta forma, un trayecto es el tramo de la red SDH comprendido entre dos puntos de ensamblado y desensamblado de VCs. La tara de sección o SOH forma parte de la trama STM. Puesto que una sección de multiplexación puede estar formada por varias secciones de regeneración, la SOH se divide en la tara de sección de multiplexación o MSOH y la tara de sección de regeneración o RSOH. En los regeneradores sólo se tiene acceso a la RSOH. De este modo, una sección es aquella parte de un trayecto en la que se mantiene la integridad de la señal STM-n, es decir, la multiplexación o demultiplexación se realiza sólo en los extremos. La utilización de punteros en SDH supone muchas ventajas respecto a la utilización de bits de justificación en PDH, desempeñando principalmente dos funciones. La primera misión del puntero es identificar la posición de los VC´s en la trama correspondiente, que será una AU o TU. Esto permite asignar de forma flexible y dinámica el VC con la información útil dentro de la trama AU o TU. La segunda misión del puntero es adaptar la velocidad binaria de los VC a la velocidad binaria del canal de transmisión. Es decir, mediante un mecanismo de justificación positiva, negativa o nula, permiten absorber las diferencias de frecuencia entre las diferentes señales que forman un STM-n.

Finalmente, una vez creada la trama STM-n, esta es transmitida utilizando los códigos de línea NRZ y RZ en el caso de la interfaz óptica. En el caso del STM-l e interfaz eléctrica, el código de línea utilizado es CMI. Para evitar la

transmisión de largas cadenas de 0s ó 1s que pueden dificultar la recepción de la señal, se utiliza un mezclador o *scrambler* en el momento de generar la señal óptica.

Los únicos bytes que no son mezclados son los tres primeros, siendo los dos primeros aquellos que identifican el inicio de las tramas y el tercero aquel que identifica el número de trama STM-1 dentro de una trama STM-n.

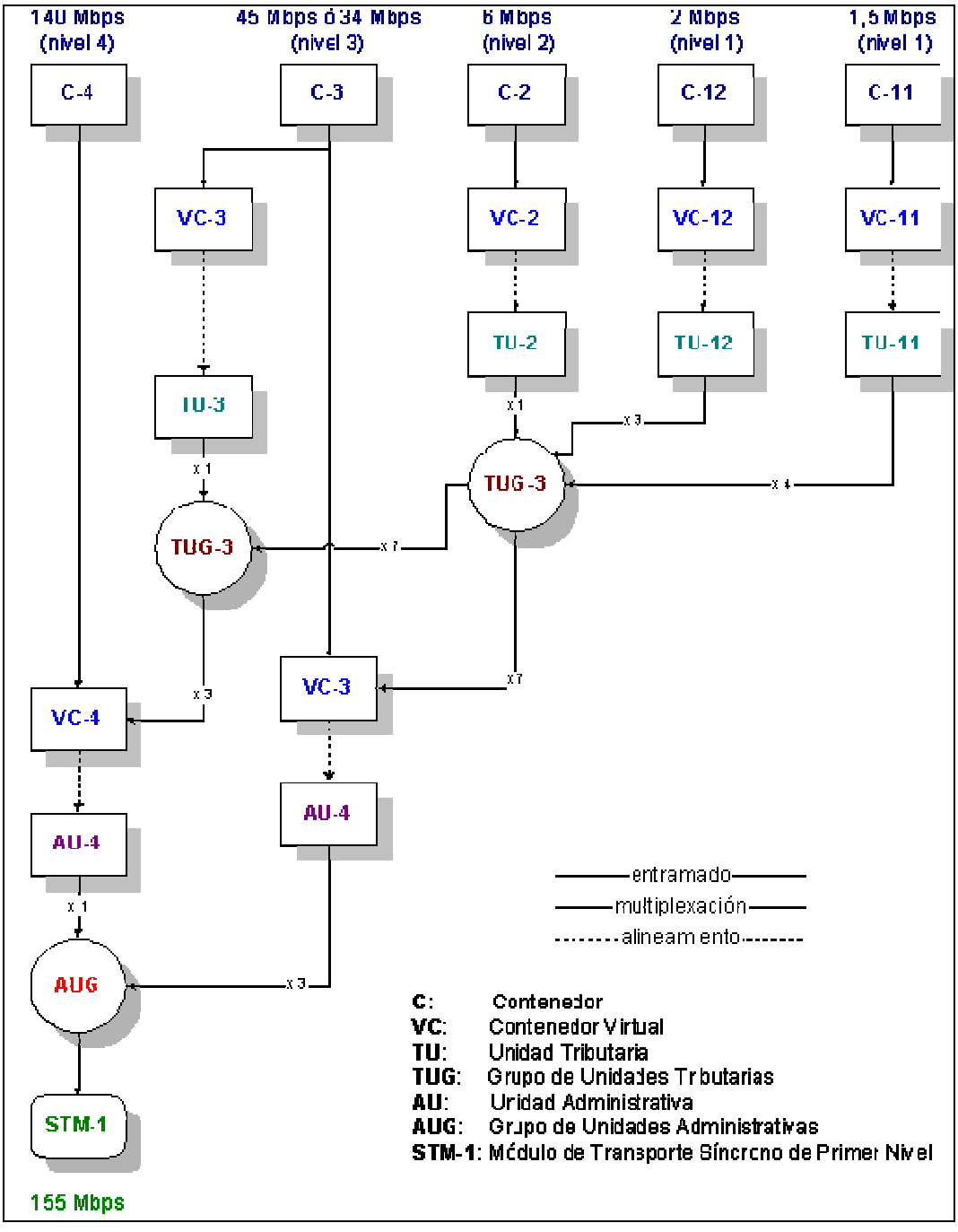

Figura 1.1 Estructura de Multiplexación de SDH.

1.1.3 Elementos de la Red

Las redes SDH actuales están construidas, básicamente, a partir de cuatro tipos distintos de equipos o elementos de red[4]: regeneradores, multiplexores terminales, multiplexores de inserción y extracción, y distribuidores multiplexores. Estos equipos pueden soportar una gran variedad de configuraciones en la red, incluso, un mismo equipo puede funcionar indistintamente en diversos modos, dependiendo de la funcionalidad requerida en el nodo donde se ubica. En la Figura 1.2 se muestra un diagrama de bloques de un elemento SDH genérico, sin considerar amplificadores o *boosters* opcionales.

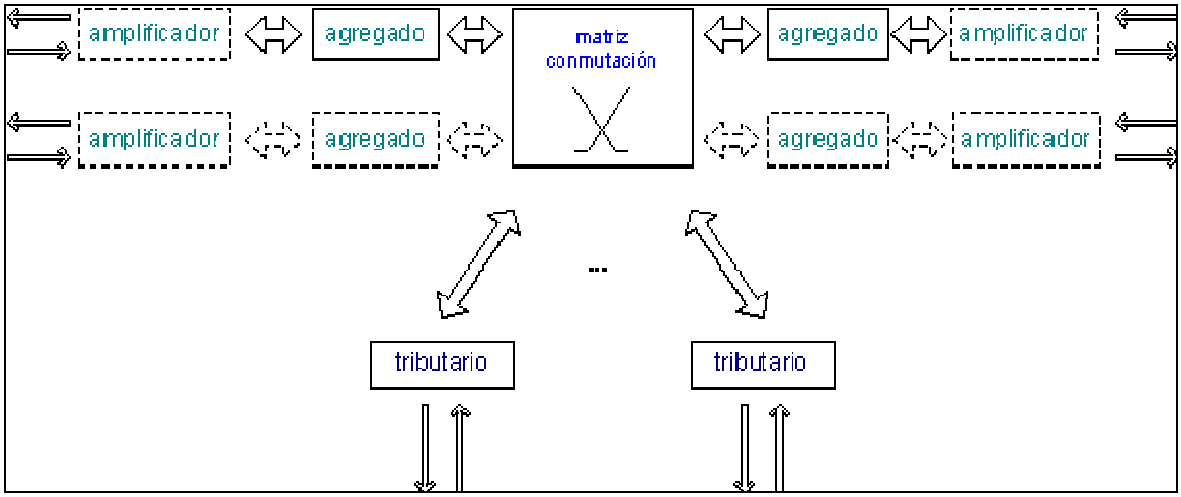

Figura 1.2 Elemento SDH genérico.

Los equipos regeneradores intermedios o IRs *(Intermediate Regenerators),* como su propio nombre indica regeneran la señal de reloj y la relación de amplitud de las señales digitales a su entrada, que han sido atenuadas y distorsionadas por la dispersión de la fibra Óptica por la que viajan. Los regeneradores obtienen la señal de reloj a partir de la ristra de bits entrante.

Los equipos multiplexores terminales o TMs *(Terminal Multiplexers)* se utilizan para multiplexar las distintas señales plesiócronas o síncronas en sus interfaces tributarias de entrada y crear la señal STM-n, que enviará por su puerto de agregado. Por ejemplo, un TM STM-4, puede tener entradas a 155 Mbps, 140

[4] ITU-T G.782

Mbps, 34 Mbps y 2 Mbps; y la interfaz de línea será a 622 Mbps. Del mismo modo, los TMs se utilizan para recibir la señal STM-n y demultiplexarla en las distintas señales plesiócronas o síncronas. Las fibras ópticas que se utilizan para la transmisión y recepción de los STM-n son distintas y, por lo tanto, el TM hace de inicio y final de las comunicaciones. En el elemento genérico de la Figura 1.2, el TM STM-4 dispondría de una única interfaz agregada óptica STM-4 (con transmisión y recepción) y, dependiendo de la configuración, de varias interfaces tributarias eléctricas (1,5 Mbps, 2 Mbps, 34 Mbps, 45 Mbps, 140 Mbps, STM-1) u ópticas (STM-1).

Los equipos multiplexores con funciones de inserción y extracción o ADMs *(Add and Drop Multiplexers),* se encargan de extraer o insertar señales tributarias plesiócronas o sícronas de cualquiera de las dos señales agregadas STM-n que recibe (una en cada sentido de transmisión), así como dejar paso a aquellas que se desee. El ADM permite, para ello, acceder a los VCs de la señal agregada, sin demultiplexar la señal completa STM-n.

Los equipos SDH ofrecen sistemas de protección hardware, como: unidades de control redundante, interfaces tributarias redundantes (o protección de circuito), matrices de conmutación redundante, etc. Los equipos distribuidores multiplexores o DXC *(Digital Cross-Connect)* permiten la interconexión sin bloqueo de señales a un nivel igual o inferior, entre cualquiera de sus puertos de entrada y de salida. Los DXCs admiten señales de acceso, tanto plesiócronas como síncronas, en diversos niveles. Los DXCs son los puntos de mayor flexibilidad en la red SDH, posibilitando que el operador realice de forma remota interconexiones semipermanentes entre diferentes canales, capacitando el encaminamiento de flujos a nivel de VC sin necesidad de multiplexaciones o demultiplexaciones intermedias. Se suele emplear la notación DXC N/M, donde el número entero N indica el nivel más alto de las señales terminadas en sus puertos y el número M indica el nivel mínimo de interconexión. Los dos tipos principales son: el DXC 4/4 y el DXC 4/1. El DXC 4/4 proporciona una interconexión totalmente transparente para el encaminamiento de canales de 140 Mbps o 155 Mbps, que pueden formar parte de conexiones a 622 Mbps o 2,5 Gbps. El DXC 4/1 en cambio, es un equipo mucho más completo que el DXC 4/4, pues

proporciona interconexión transparente hasta los 2 Mbps. En el elemento genérico de la Figura 1.2, el DXC 4/1 dispondría de varias interfaces ópticas (STM-1, STM-4 o STM-16) o eléctricas (1,5 Mbps, 2 Mbps, 34 Mbps, 45 Mbps, 140 Mbps, STM-1), generalmente hasta un máximo de 512 (la mitad para la parte Este y la otra mitad para la Oeste).

EVOLUCIÓN DE LAS REDES DE TRANSPORTE DE NUEVA GENERACIÓN

1.1.4 Prospecto de la Red de Transporte de Nueva Generación

Tradicionalmente su arquitectura y sus características particulares estaban subordinadas al tipo de información que se deseaba transportar y a las características de las redes de acceso utilizadas. Así, por ejemplo, existen redes de transporte de señal de televisión (para el servicio convencional de difusión de televisión), redes de transporte de televisión por cable, múltiples tipos de redes de transporte de datos dependientes del servicio de datos en cuestión, redes de transporte de telefonía fija y redes de transporte de comunicaciones móviles. Sin embargo, la llegada de la digitalización comenzó un proceso de convergencia en las redes de transporte para hacerlas potencialmente capaces de transportar cualquier tipo de información, independientemente de su origen. A este proceso contribuyó también el uso masivo de la fibra óptica como el medio físico de preferencia para el transporte. A lo largo de este proceso han ido apareciendo una serie de tecnologías digitales para su aplicación en el transporte: X25, Frame Relay, SDH, ATM, cada una de ellas orientada inicialmente a solventar problemas específicos en arquitecturas específicas de transporte y que han tenido diferentes períodos de éxito y decadencia.

La llegada de la conmutación de paquetes y del paradigma de Internet, con el éxito de los protocolos IP como la base del transporte masivo de datos, introdujo una nueva cuestión al plantear si las redes de transporte debían o no tener un grado significativo de inteligencia en su núcleo central o si esta inteligencia se debía encontrar en los bordes de la red de transporte. La cuestión es muy relevante pues se pretende que las nuevas redes de transporte sean lo más transparentes posibles frente al despliegue de nuevas aplicaciones de interés

para los usuarios, es decir, que sean válidas para cualquier nueva aplicación sin cambios significativos y sobre todo sin inversiones y retardos que puedan impedir cumplir las expectativas de los usuarios.

Se tiende hacia velocidades mayores, tal como en el sistema STM-64 (multiplexado por división en el tiempo, TDM de 10 Gbps), pero los costos de los elementos de ese tipo son aún muy elevados, lo que está retrasando el proceso. La alternativa es una técnica llamada DWDM (Multiplexación Densa por División de Longitud de Onda) que mejora el aprovechamiento de las fibras ópticas monomodo, utilizando varias longitudes de onda como portadoras de las señales digitales y transmitiéndolas simultáneamente por la fibra. Los sistemas actuales permiten transmitir 16 longitudes de onda, entre 1520 nm y 1580 nm, a través de una sola fibra. Se transmite un canal STM-16 por cada longitud de onda, lo que da una capacidad de unos 40 Gbit/s por fibra. Ya se ha anunciado la ampliación a 32, 64 e incluso 128 longitudes de onda. Conectada al empleo del multiplexado DWDM se observa una tendencia hacia las redes en las que todos los elementos son ópticos. Ya existen en el mercado multiplexores add/drop (inserción / extracción) ópticos y se están realizando pruebas de dispositivos ópticos de transconexión (cross-connects). En términos del modelo de capas ISO-OS, este desarrollo significa básicamente la aparición de una capa DWDN, adicional debajo de la capa SDH. Probablemente pronto veremos velocidades binarias aún más elevadas gracias a la tecnología DWDM.

1.1.5 Red de Transporte orientada a ALL IP

La red ALL IP contiene una variedad de tecnologías en distintas capas como WDM, OTN, Ethernet, MPLS e IP, etc. Los operadores pueden confundirse al elegir una solución adecuada para sus redes de transporte cuando se encuentran rodeados por distintos tipos de tecnologías de networking. Se reducirán los errores al elegir el equipo si se presta atención a los siguientes dos aspectos: Si una red de transporte presenta una gran capacidad de adaptación para las redes de servicio actuales y del futuro, o si ofrece una buena ventaja de relación precio/rendimiento.

El WDM de nueva generación basado en OTN es una tecnología clave en el curso de la evolución hacia la red portadora ALL IP. Una red OTN/WDM realiza las funcionalidades de aprovisionamiento, grooming y protección de los servicios de longitudes de onda y sub-longitudes de onda, así como el networking Meshed. Por lo tanto, podrá cumplir con los requerimientos de la red de core para un gran ancho de banda, networking flexible, alta eficacia y una significativa mejora en la confiabilidad.

En el futuro, la red OTN/WDM puede extenderse hasta la capa de acceso Metro para cubrir la demanda y con esto aumentar el acceso a ancho de banda. Como resultado, OTN/WDM construirá la tercera red de extremo a extremo desde el acceso a core, siguiendo los pasos de SDH e IP.

El equipo PTN derivado de MSTP es otro componente principal de la red de nueva generación. Soporta una evolución sin problemas hacia la red de nueva generación concentrándose alrededor de T-MPLS o PBT y brindando una red orientada hacia la conexión que soporta rendimiento de extremo a extremo de tipo SDH. La evolución de MSTP a PTN es una forma rentable para los servicios de línea privada o móvil que necesitan TDM e IP e incluso interfaces ATM durante un largo período.

En la próxima red portadora, IP/MPLS se utilizará para procesar servicios en la capa core, PTN accederá y convergerá servicios de granularidad fina. OTN/WDM sirve como una red de transporte de extremo a extremo.

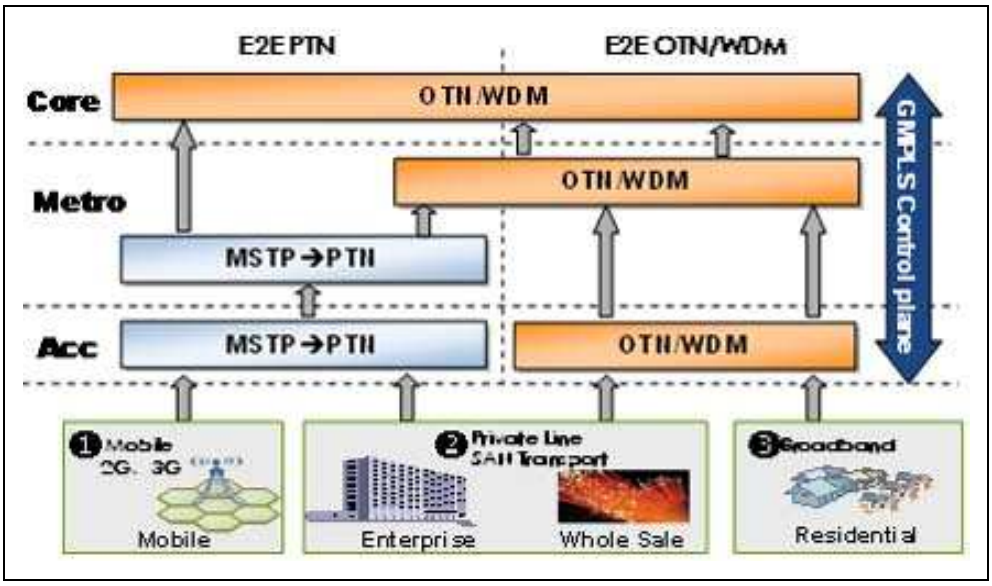

Figura 1.3 Red de Transporte orientada a ALL IP.

CAPÍTULO II

TIPOS DE PROTECCIÓN PARA RED DE TRANSPORTE SDH

Descripción de los diferentes tipos de protecciones para la red SDH

La gran capacidad de los enlaces SDH hace que un simple fallo de enlace pueda tener un impacto nocivo en los servicios proporcionados por la red si no se dispone de una protección adecuada. Una red resistente que asegure el tráfico que porta y que puede restaurarlo automáticamente ante cualquier evento de fallo es de vital importancia. Los sistemas de transmisión SDH permiten desplegar esquemas de protección estándar.

Los procedimientos de protección de red son empleados para auto-recuperarse de eventos de red del estilo de un fallo de enlace o elemento de red. Lo que efectivamente ocurre es que un elemento de red detectará un fallo o una pérdida de tráfico e iniciará acciones correctivas sin involucrar al sistema de gestión de red.

Hay mecanismos de protección definidos por los organismos de estandarización, los cuales pueden ser subdivididos en aquellos que protegen la capa de sección y en aquellos que protegen la capa de camino o subred:

La protección de la capa de sección involucra la conmutación de todo el tráfico de una sección a otra sección de fibra alternativa.

La protección de la capa de camino involucra la protección de un contenedor virtual de un extremo a otro del camino en la subred. Ante un evento de fallo, únicamente el contenedor virtual en cuestión es conmutado a un camino alternativo.

El tipo de esquema de protección empleado viene usualmente dictado por la arquitectura de red.

1.1.6 Protección Camino / Ruta VC Dedicada

Este tipo de protección implica duplicar el tráfico en forma de contenedores virtuales, los cuales son introducidos en la red y transmitiendo esta señal simultáneamente en dos direcciones a través de la red.

Un camino de protección dedicado lleva el tráfico en una dirección y el camino operativo porta la señal a través de otra ruta diferente. El elemento de red que recibe las señales compara la calidad de los dos caminos y la señal de mayor calidad es seleccionada, ésta será nombrada como la ruta activa. Ante un evento de fallo en la ruta activa el extremo receptor conmutará al otro camino, a la ruta de protección.

Esto protegerá a los mismos enlaces por sí mismos, pero también protegerá contra fallos de un nodo intermedio. Un ejemplo especial de este tipo de mecanismo es el anillo de camino de protección. Según el tráfico entra al anillo es transmitido simultáneamente en ambas direcciones en torno al anillo. La selección es realizada por el nodo de salida de la mejor de las dos conexiones.

El mecanismo puede ser aplicado a anillos y también a circuitos punto a punto a través de redes malladas o mixtas mediante muchos elementos de red y subredes intermedias.

1.1.7 Protección de Conexión de Subred (SNCP)

SNCP es similar a camino de protección, pero en el cual, el camino de protección dedicado involucra conmutación en ambos extremos del camino, mientras que la conmutación SNCP puede ser iniciada en un extremo de la ruta y llegar hasta un nodo intermedio. La red puede ser descompuesta con un número de subredes interconectadas. Con cada protección de subred se proporciona un

nivel de ruta y la conmutación automática de protección entre dos caminos es proporcionada en las fronteras de subred.

La selección de la señal de mayor calidad se realiza, no únicamente por el elemento de red en el extremo del camino, sino que también en nodos intermedios a la salida de cada subred que es atravesada por la ruta. El contenedor virtual no termina en el nodo intermedio, en cambio compara la calidad de la señal en los dos puertos entrantes y selecciona la señal de mejor calidad.

Ante un evento de dos fallos simultáneos, la conmutación de protección debe ocurrir en el nodo intermedio A para que el tráfico alcance el extremo contrario. SNCP genera una alta disponibilidad para la conexión que el camino dedicado porque SNCP permite a la red sobreponerse a dos fallos simultáneos cosa que el camino de protección no permite.

En principio, el camino de protección extremo a extremo parece tener mucho atractivo; una amplia protección en redes extremo a extremo es posible y las rutas individuales pueden ser selectivamente protegidas. Aun así, es requerido un complejo control que asegure realmente diversas rutas.

Una gran cantidad de capacidad es usada y es muy difícil de coordinar actividades de mantenimientos programados a lo largo de la red. El camino de protección llega a ser, de todos modos, cuando queda limitado al nivel de subred, es decir, SNCP. SNCP trabaja especialmente bien sobre anillos, porque se aseguran diversas rutas de fibra.

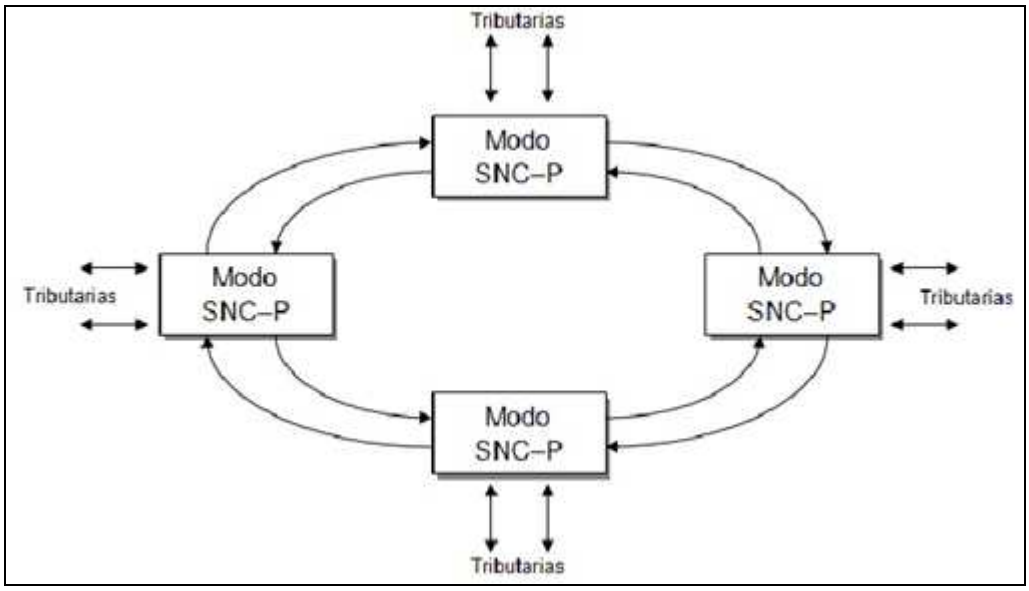

Figura 2.1 Anillo con protección SNCP.

La resistencia puede ser ofrecida a un número de capas incluyendo el camino extremo a extremo (trazado), el nivel de subred y el nivel de sección de multiplexión. Los mecanismos descritos anteriormente ofrecían protección a la ruta extremo a extremo y al nivel de subred. Esto involucra la protección de contenedores virtuales individuales a través de una ruta punto a punto. Si existe un evento de fallo, únicamente el contenedor virtual en cuestión es conmutado a una ruta alternativa, así que la protección individual para un único VC es posible. Por ejemplo, un cliente puede requerir protección para una línea alquilada, de modo que el camino de este circuito pueda ser protegido a través de toda la red sin necesidad de proteger el resto de tráfico que por ella transita.

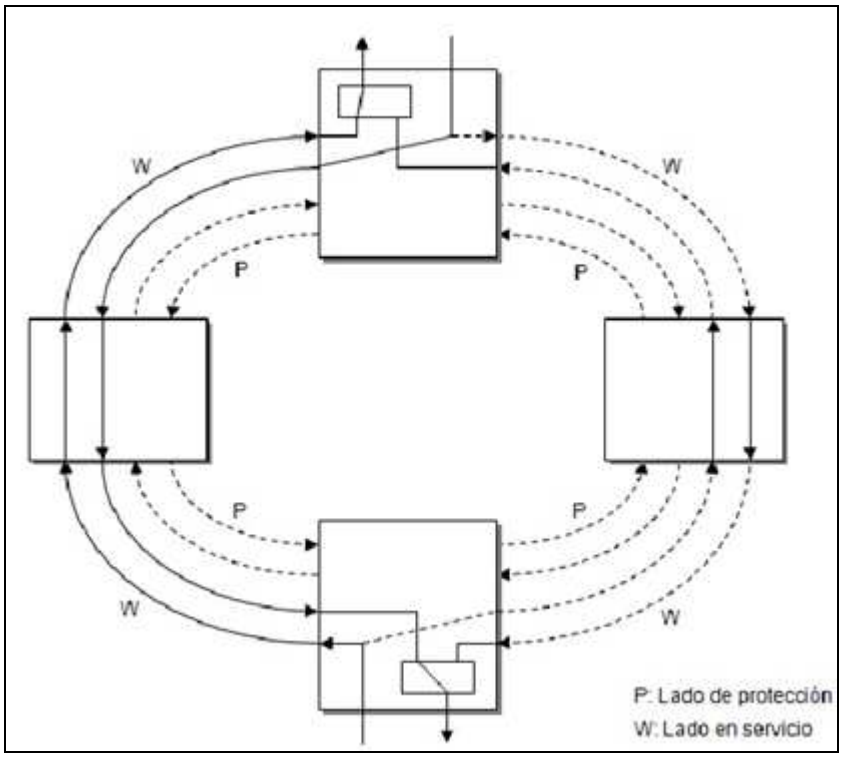

Figura 2.2 SNCP con modo de protección en línea.

Cabe destacar que ambos esquemas, protección de camino punto a punto y camino de subred pueden ser aplicados tanto para caminos de alto orden como de bajo orden (tanto para VC-4 como para VC-12).

1.1.8 Protección de Línea de la Sección de Multiplexación MSP

Este procedimiento opera con una sección de tráfico ubicada entre dos nodos adyacentes. Entre estos dos nodos hay dos enlaces separados o dos diferentes fibras: la operativa y la de protección. Ante un evento de fallo del enlace, la señal entrante debe ser conmutada de la fibra activa a la de protección.

Hay dos tipos diferentes de protección de Sección de multiplexación (MSP):

Protección 1:1 es un esquema de doble extremo. El tráfico es inicialmente enviado por el enlace activo únicamente. Se detecta un fallo en el extremo contrario cuando no recibimos tráfico por un periodo prolongado de tiempo. Una señal es enviada al extremo transmisor que dispara las conmutaciones de protección, enviando el tráfico hacia la línea de back-

up en ambos extremos. Esto significa que tráfico de baja prioridad puede ser portado por el canal de protección mientras el tráfico viaje por el canal operativo. Este tráfico se perderá cuando se inicia un proceso de conmutación de protección.

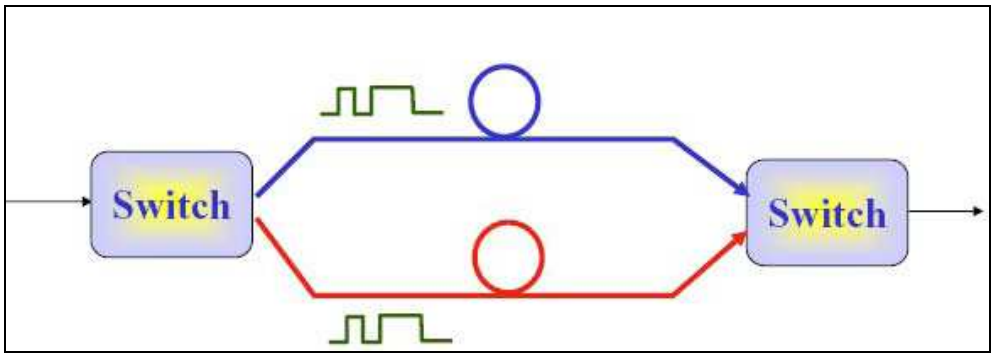

Figura 2.3 Esquema de protección 1:1.

Protección 1:n es similar al tratado 1:1 con la excepción de que varios canales operativos pueden ser protegidos por un único canal de back-up.

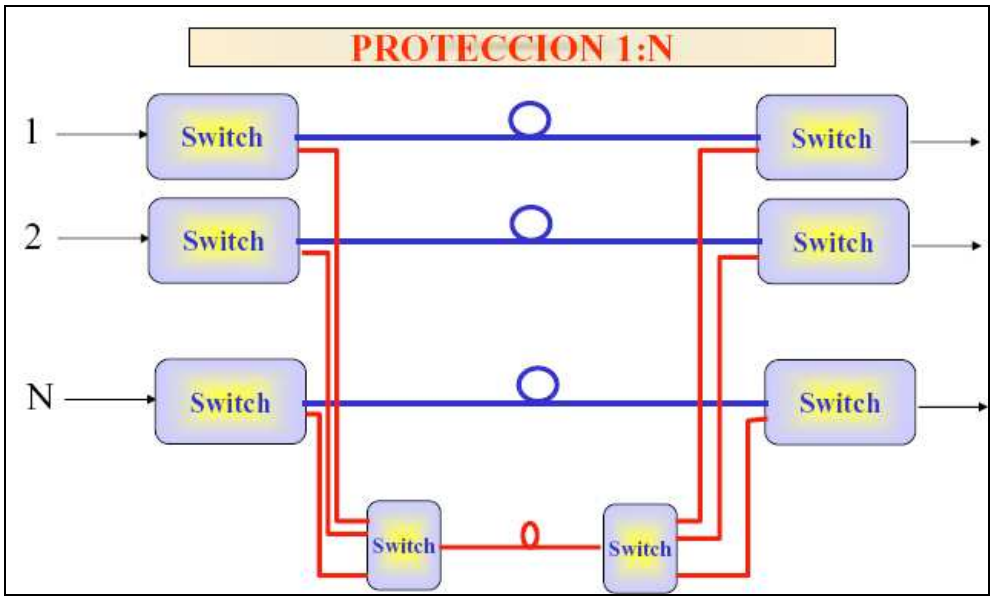

Figura 2.4 Esquema de protección 1:n.

Protección 1+1 MSP donde el tráfico es inicialmente enviado tanto por la ruta activa como por la ruta de protección. Si se detecta una pérdida de tráfico, en el extremo receptor se comienza un proceso de conmutación hacia el camino de protección. No hay necesidad de enviar señalización

hacia atrás, aunque de todos modos, la sección de standby no puede ser utilizada para otro tráfico presentando unos altos requerimientos de capacidad de fibra.

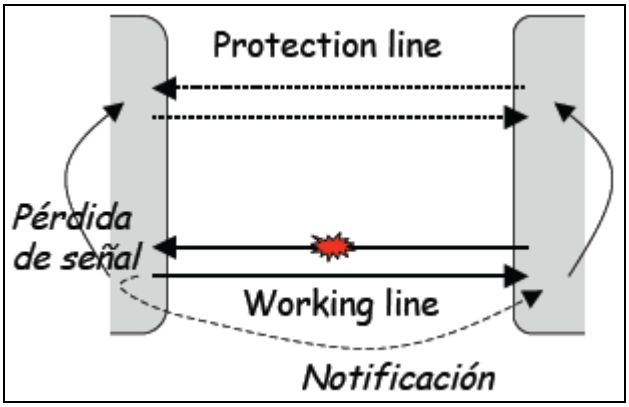

Figura 2.5 Esquema de protección 1+1 MSP.

MSP protegen tráfico entre dos elementos de red adyacentes, pero únicamente el enlace entre esos dos nodos, no aportando protección ante un fallo total de un elemento de red. Otra limitación es que requiere de diversos caminos físicos para fibra activa y de protección. Si ambas fibras se encuentran en la misma conducción y ésta es dañada, los dos caminos, el operativo y el de protección, se perderían.

Dos rutas alternativas deben ser dispuestas entre dos nodos adyacentes. Estas consideraciones se han de tener en cuenta cuando desplegamos este tipo de esquema de protección.

La protección lineal de la sección de multiplexación es típicamente usada para redes lineales malladas. Los diversos caminos físicos son, sin embargo, requeridos haciendo que la malla sea incrementalmente más compleja a medida que crece. Ante la escasez de fibra convertida en una situación crítica muchos operadores han optado por el despliegue de anillos. Los anillos aseguran que entre cada par de nodos hay un camino físico diferente que puede ser usado como ruta de protección.

1.1.9 Anillos Auto-Recuperables

Los procedimientos de protección de anillos auto-recuperables se están convirtiendo rápidamente en comunes, porque proporcionan diversas rutas de protección y por tanto, un uso eficiente de la fibra. Hay diferentes tipos de esquemas de anillos de protección, los cuales pueden ser divididos en los que protegen la capa de sección y los que protegen la capa de camino. A su vez, estos pueden ser subdivididos en esquemas Uni-direccionales y Bi-direccionales. Dos tipos de mecanismos de anillos auto-recuperables serán considerados, puesto que son los más comúnmente desplegados en el mercado ETSI:[5]

Anillos bidireccionales de protección de camino (anillos de protección dedicada o anillos de protección de caminos)

Anillos bidireccionales de protección compartida (SPRings)

Los anillos de protección dedicada son un tipo de protección de camino dedicado, aplicado a un anillo. Al entrar el tráfico al anillo por un nodo A es enviado simultáneamente por ambas direcciones en torno al anillo. Una dirección puede ser considerada como camino de trabajo "w" y la otra dirección el camino de protección "p".

El nodo receptor seleccionará la señal de mayor calidad. Por ejemplo asumimos que la mejor calidad es la de la señal "w"; ante un evento de rotura de fibra óptica entre A y B en "w", B seleccionará el tráfico del camino "p".

1.1.10 Anillos de Protección Compartida de la Sección de Multiplexación

Los anillos de protección compartida de la sección de multiplexación, comúnmente llamados "MS-SPRing" son unos mecanismos de protección de anillo. A diferencia del anillo de protección dedicado, el tráfico es enviado solo por una ruta en torno al anillo. No existe un camino de protección dedicado por cada

[5] Instituto Europeo de Normas de Telecomunicaciones

ruta en producción, en cambio esta reservada capacidad del anillo para protecciones y esta puede ser compartida para la protección de diversos circuitos en producción. La conmutación de protección es iniciada a nivel de sección de modo similar a la protección lineal para de la sección de multiplexación; ante un evento de fallo, todo el tráfico de la sección es conmutado. Este mecanismo se puede llevar a cabo salvando una importante cantidad de capacidad frente al mecanismo de anillo de protección dedicado, permitiendo al operador incrementar el número de circuitos activos en el anillo.

La ventaja en capacidad que se puede conseguir con MS-SPRing con respecto a un anillo con protección de ruta dedicada no es obvia hasta que no se analiza un ejemplo simple con diferentes caminos de tráfico sobre el anillo, como vamos a pasar a presentar. Tomaremos como ejemplo un anillo con seis nodos con una capacidad STM-16, equivalente a 16 STM-1´s. Considerando un patrón de tráfico uniforme en el cual el tráfico entrante sale del anillo en el nodo adyacente.

Si todo el tráfico existente y entrante a los nodos es posible que disponga de rutas activas entre todos los nodos adyacentes, esto es, ocho STM-1´s son usados para tráfico activo girando en torno a todo el anillo y en cada sección otros ocho STM-1´s estarán aún disponibles para la protección compartida para estas rutas de trabajo.

Así, es posible tener rutas activas en cada una de las secciones (w1-w6) y que existan ocho canales STM-1 para cada sección, consiguiendo un total de 48 rutas (ocho canales por seis secciones) a establecer, comparados con los 16 que obteníamos con el anillo de protección dedicada.

Este patrón de tráfico no es típico, pero si los cálculos son realizados para un patrón de tráfico uniforme, el cual es típico para circuitos entre grandes ciudades o redes de datos metropolitanas, entonces SPRings puede doblar la capacidad con respecto a un anillo de protección dedicada.

SPRings puede también incrementar la capacidad en fibras mediante la reutilización de canales reservados para protección. En muchas redes hay demanda de servicios de tráfico de gran ancho de banda de bajo coste donde el coste es prioritario sobre la disponibilidad como es por ejemplo el tráfico IP. En un SPRing el ancho de banda protegido es establecido dinámicamente ante una rotura de fibra. Esto significa que no se usa permanentemente gran cantidad de ancho de banda innecesariamente para protección y se encuentra disponible para algo de tráfico añadido a la carga completamente protegida. Esto proporciona una sencilla manera de integrar SPRings con esquemas de protección punto a punto donde la protección para el tráfico del camino protegido es portada en los canales de tráfico extra compartiendo ancho de banda de protección entre la SPRing y la red de camino protegido.

De este modo protegiendo contra el fallo de un enlace, SPRings protege contra el fallo de algún nodo de la red, caso no posible con la protección MSP lineal.

ANÁLISIS COMPARATIVO ENTRE LOS DIVERSOS TIPOS DE PROTECCIONES PARA LA RED DE TRANSPORTE SDH

1.1.11 Comparación entre Esquemas de Protección

Como se puede apreciar en la Tabla 2.1, los esquemas de protección varían significativamente en sus características. No hay un óptimo esquema de protección. La elección puede ser determinada por el diseño de la red, por ejemplo, SPRings tiende a ser usado en una topología de anillo mientras que la restauración se emplea en redes malladas de alto nivel con gran cantidad de cross-conexiones.

Esquema de Protección	Qué Protege	Dónde aparece la Protección	Es un esquema selectivo a nivel de VC	Estandarizado	Topología	Tiempo Típico de Conmutación
MS-SPRing	Todo el trafico de la sección	Cualquier nodo en el anillo	NO	SÍ	Anillo	<50ms
1+1 MSP	Todo el tráfico de la sección	Nodos Adyacentes	NO	SÍ	Lineal/ Mayada	<50ms
Ruta Dedicada	VC individual	Nodo del extremo final del anillo	SÍ	SÍ	Mixta	<50ms
SNCP	VC individual	Nodo final o intermedio de la ruta	SÍ	SÍ	Mixta	<50ms
Restauración	VC individual	No hay conmutación de protección.	SÍ	NO	Mayada	>1min

Tabla 2.1 Tabla comparativa entre Sistemas de Protección

La elección del esquema de protección puede ser también determinada por el nivel de red al cual el tráfico es portado. En las capas de backbone la tasa de transmisión es muy alta, del orden de STM-16 o STM-64, así que la acumulación de tráfico portado en cada fibra es mucho mayor en enlaces de menor nivel. Una rotura de esta fibra tendría un impacto mucho mayor que una pérdida de señal en una fibra de bajo nivel. El backbone, por tanto, tiene justificado un esquema de protección completa como el MS-SPRing o el 1+1 MSP.

Los patrones de tráfico varían dependiendo del nivel de red en el que nos encontremos. En la capa de backbone el tráfico es típicamente uniforme, portándose entre ciudades grandes, redes metropolitanas o redes de datos. En esta situación, una SPRing puede proveer una ventaja de capacidad sobre la ruta de protección. La reutilización de capacidad reservada para protección es también una consideración importante, como si fuera un tráfico de anillo extra. En capas de backbone, la fibra puede ser escasa y es crítico hacer un óptimo uso del ancho de banda disponible.

En capas inferiores de la red, el tráfico es típicamente portado a un punto central que lo recolecta y lo transporta al siguiente nivel. Esto es conocido como tráfico concentrado. En esta situación las ventajas de SPRings no son grandes y la necesidad de proteger cada fibra no es crítica. Esquemas de protección de ruta selectiva como VC-Trail y protección SNCP son más comunes en esta situación. Por ejemplo, un cliente puede solicitar la protección de sus líneas de 2 Mbps, por lo que estos caminos VC-12 han de ser selectivamente protegidos con rutas de protección.

Esta ruta está protegida a nivel VC-12 a través de toda la red. Si esta ruta estuviera solamente protegida a nivel de circuito de alto nivel, es decir, a nivel de VC-4, por MSP o MS-SPRing y hubiera una ruptura en una fibra de bajo nivel, este VC-12 se perdería. Un circuito VC-4 completo, de este modo, no se perdería, solo que el mecanismo de protección a nivel de VC-4 no detectaría el fallo. Un operador, por tanto, no debe considerar únicamente como trabaja su esquema de protección, sino como se interconexiona con los adyacentes.

Un despliegue efectivo de subredes es interconectando subredes protegidas SNCP y subredes protegidas MS-SPRings. Por ejemplo, una subred MS-SPRings es ideal para el núcleo de la red, pudiendo ser conectada con redes locales o regionales donde la protección de camino de subred estuviera usándose para aplicar protección selectiva al tráfico.

1.1.12 Interconexión de Esquemas de Protección

A medida que el tamaño y la demanda de tráfico de una red se incrementan, también lo hace su complejidad. Un anillo simple o una conexión en cadena raramente serán implementados. Las redes se constituyen a base de un número de subredes y cada una puede tener su propio esquema de protección. Con la gran cantidad de operadores existentes, la interconexión de redes entre diferentes operadores se convierte en una difícil cuestión. Estos factores junto con el objetivo de una mayor resistencia de la red, significan que el hecho de la interconexión de varias subredes individualmente protegidas es de gran importancia.

La interconexión de protecciones es donde un esquema de protección trabaja sobre una única conexión a lo largo de la red. Un simple esquema de protección puede no proporcionar la actuación adecuada, y por tanto, puede ser mejor implementar una protección basada en subredes, pero entonces, la interconexión de estos esquemas ha de ser considerada.

1.1.13 Directivas para Interconexión de Esquemas de Protección

1. **Maximizar la disponibilidad de tráfico**: Disponibilidad fue definida previamente como la probabilidad de que una conexión extremo a extremo esté funcionando. En una red de varias subredes interconectadas se podría asegurar que la red podría sobrevivir a no solamente fallos en una única red, sino también a fallos concurrentes, es decir, en diferentes subredes interconectadas. Otra consideración es el enlace o enlaces donde estas subredes están interconectadas. Éste debe ser tan robusto como cualquier otro punto de dichas subredes.

2. **Mantener independencia de protecciones**: Las fronteras entre subredes pueden representar fronteras administrativas o de mantenimiento. Es deseable que un fallo en una subred no influya en la conmutación de protección en una subred interconectada. Por ejemplo, un trabajo de mantenimiento en una subred no debería efectuar conmutación en una subred interconectada, particularmente si está gestionada por otro operador.

3. **Subredes interconectadas protegidas a diferentes niveles**: Un operador puede adoptar una aproximación multicapa mediante la cual haya separado las capas de backbone, tráfico regional y tráfico local, cada uno de los cuales consistirá en una subred diferente. La administración en cada capa puede diferir, por ejemplo el tráfico en un circuito administrado a nivel de VC-4, y en el nivel regional administrado en forma de VC-12. La interconexión de tráfico y los esquemas de protección de interredes ha de ser considerado.

4. **Redes interconectadas usando diferentes esquemas de protección**: Un camino extremo a extremo probablemente transitará por varias subredes y en cada una puede tener un esquema de protección diferente. Para asegurar que este circuito extremo a extremo está protegido estos esquemas deben trabajar conjuntamente. Esto es particularmente importante en países donde hay varios operadores y los circuitos cruzan fronteras entre operadores.

1.1.14 Tipos de Protecciones Interconectivas

Cuando una simple conexión extremo a extremo pasa a través de diferentes redes interconectadas, hay dos tipos de esquemas de protección conjunta que pueden operar: concatenación (encadenado) o anidamiento.

Concatenación: La conexión extremo a extremo es protegida mediante el encadenado de varias subredes protegidas independientemente, esto es conectando las subredes en series. En cada subred, un mecanismo de

protección diferente puede operar en la conexión. Esto es más fácil de comprender y gestionar que el anidamiento donde la protección es modular. Los mecanismos de conmutación no interactúan y su gestión es simple.

Anidamiento: En este tipo de dominio de protecciones, se producen las superposiciones de esquemas, de modo que dos mecanismos actuarán simultáneamente en una única porción de la conexión.

1.1.15 Tipos de Interconexión

Hay diferentes modos de interconectar subredes. Consideremos un esquema concatenado. La interconexión de nodo dual indica que dos nodos en cada subred están conectados. Dos caminos están establecidos entre cada dos subredes y por tanto una conexión punto a punto es protegida contra fallos en una de las subredes. Un nodo interconectado es protegido contra un simple fallo en un nodo o la pérdida de uno de los enlaces interconectados. El esquema de interconexión de un simple nodo introduce un punto singular de fallo en la red. Si el enlace interconectado falla o uno de los nodos interconectados falla el tráfico se perderá. Incluso si se emplea 1+1 MSP en el enlace de interconexión, los dos nodos podrían ser puntos singulares de fallo.

Dentro de la interconexión dual tenemos dos modalidades

Anillo virtual: Los caminos operativos y de protección son físicamente diferentes. Pueden estar dos nodos interconectados en cada subred o la interconexión de nodos puede ser compartida a través de subredes. Este mecanismo es tan robusto como una subred simple, porque hay dos caminos entre las subredes y no un punto singular de fallo, si hubiera fallos en subredes en cada lado de la interconexión, no obstante, el tráfico podría perderse.

Extracción y continuidad (Nodos igualados): Ésta es una forma más robusta de interconexión dual. El tráfico del primer nodo A es pasado a la

segunda subred vía nodo B, pero también continúa a C y es pasada a D, por lo que dos copias del tráfico son pasadas a la segunda subred. Ante un evento de fallo concurrente en cada una de las subredes, el tráfico no se pierde.

Este último método es también deseable porque la independencia entre subredes se mantiene, lo cual no es el caso de los anillos virtuales. En subredes donde las fronteras representen fronteras administrativas entre regiones o diferentes operadores de red, esta interconexión previene fallos y ante trabajos planeados en una subred la protección afectada es conmutada en la subred vecina.

Extracción y continuidad es un esquema de interconexión dual que puede ser usado para las siguientes combinaciones de subredes:

Subred SNCP con subred SNCP
MS-SPRing con MS-SPRing
MS-SPRing con subred SNCP
MS-SPRing con Anillo de protección dedicada MS
Anillo de protección dedicada MS con subred SNCP

De estas combinaciones, las dos últimas no están recogidas en los marcos de directrices ETSI.

ANÁLISIS DE LAS RECOMENDACIONES UIT-T RESPECTO AL USO DE SISTEMAS DE PROTECCIONES PARA REDES SDH

1.1.16 Recomendación UIT-T G.841

Tipos y características de las arquitecturas de protección para redes de la jerarquía digital síncrona

Esta Recomendación proporciona las especificaciones necesarias en materia de equipos para implementar diferentes tipos de arquitecturas de

protección para redes de la jerarquía digital síncrona (SDH, *synchronous digital hierarchy*). Las entidades protegidas pueden ir desde una sola sección de multiplexación (SDH) (por ejemplo, protección de sección de multiplexación lineal) hasta una parte de un trayecto de extremo a extremo SDH (por ejemplo, protección de conexión de subred) o hasta un trayecto entero de extremo a extremo SDH (por ejemplo, protección de camino de contenedor virtual lineal de orden superior/inferior).

Las implementaciones físicas de estas arquitecturas de protección pueden incluir anillos o cadenas lineales de nodos. Cada clasificación de la protección incluye directrices sobre objetivos de red, arquitectura, funcionalidad de las aplicaciones, criterios de conmutación, protocolos y algoritmos.

La presente Recomendación describe los distintos mecanismos de protección para las redes de la jerarquía digital síncrona (SDH, *synchronous digital hierarchy*), sus objetivos y sus aplicaciones.

Los esquemas de protección se clasifican de la siguiente manera:

Protección de camino SDH (en la capa de sección o de trayecto), y;

Protección de conexión de subredes SDH (con supervisión intrínseca, supervisión no intrusiva y supervisión de subcapa).

Los casos de interfuncionamiento de protección (incluida la jerarquía de conmutación) y de interconexión están estudiándose en el marco de la recomendación UIT-T G.842 descrita a continuación en esta sección. No se describen aquí la arquitectura de sincronización ni la protección de la sincronización.

1.1.17 Recomendación UIT-T G.842

Interfuncionamiento de las arquitecturas de protección para redes de la jerarquía digital síncrona

Esta Recomendación proporciona las especificaciones para el interfuncionamiento de arquitecturas de protección de redes. Tiene un tratamiento especial la interconexión de nodo único y de nodo doble entre anillos de protección compartida de sección de multiplexión (MS) y anillos de protección de conexión de subred (SNCP) de tipos iguales o distintos.

Esta Recomendación describe los mecanismos para el interfuncionamiento entre arquitecturas de protección de redes. Las arquitecturas de protección de redes se describen en la Recomendación G.841. La descripción del interfuncionamiento se hace para la interconexión de nodo único y de nodo doble para el intercambio de tráfico entre anillos. Cada anillo puede ser configurado para protección compartida de MS o para protección SNCP.

1.1.17.1 Criterios y Objetivos de Interfuncionamiento

Las arquitecturas de protección para redes SDH en interfuncionamiento tienen por objeto proporcionar un grado de protección aún mayor dentro de una red. Algunos factores en relación con los criterios de interfuncionamiento son como sigue:

Los requisitos de disponibilidad de extremo a extremo
La solidez frente a los diversos eventos de fallo
La complejidad y los costes de la implementación

Lo siguiente es una lista de objetivos del interfuncionamiento:

1. El interfuncionamiento de anillos deberá acomodarse de tal manera que si dos anillos están conectados en más de un nodo cada uno de ellos, el fallo de uno de estos nodos no provoque la pérdida de ningún servicio.

2. De ser posible evitar la propagación de la conmutación entre anillos en interfuncionamiento.

3. El anillo deberá ser capaz de sustraer tráfico en múltiples nodos, es decir, que el tráfico de servicio puede ser sustraído en dos o más nodos de un anillo sin comprometer la capacidad de restablecimiento del tráfico que sea bicabecera (o de cualquier otro tráfico).

4. La interconexión de anillos puede producirse entre múltiples anillos. Los límites de la interconexión deberán ser los mismos para todos los casos similares de interfuncionamiento entre dos tipos de anillo.

CAPÍTULO III

ANÁLISIS DE LA RED ACTUAL DE TRANSPORTE SDH DE CELEC EP - TRANSELECTRIC

CARACTERÍSTICAS GENERALES

CELEC EP – TRANSELECTRIC, cuenta con servicios de portador de telecomunicaciones y de valor agregado para brindar transmisión de datos e Internet, a través de la red de fibra óptica en diferentes Subestaciones y Puntos de Presencia (PDP´s) a nivel nacional. Las capacidades que se ofrecen parten de la unidad de un E1 (2,048 Mbps) hasta capacidades de un STM-64 (equivalente a 4032 E1´s = 10 Gbps).

Actualmente, la red de CELEC EP – TRANSELECTRIC cuenta con varias tecnologías para la transmisión de datos que se detallan a continuación:

PLC	Power Line Carrier
DPLC	Digital Power Line Carrier
PDH	Plesiochronous Digital Hierarchy
SDH	Synchronous Digital Hierarchy
DWDM	Dense Wavelength Division Multiplexing
IP	Internet Protocol

Las actuales necesidades de comunicación y los requerimientos de alta disponibilidad, demandan la utilización de nuevas tecnologías en la transmisión de la información, es por esto que se ha implementado nuevas técnicas y nuevos equipamientos como parte de la operación de la red.

En la Figura 3.1 se muestra la red de fibra óptica de CELEC EP – TRANSELECTRIC instalada, así como, la fibra óptica a instalar hasta finales de 2011 que comprende un tramo de 700 Km. en la parte Oriental del territorio Ecuatoriano.

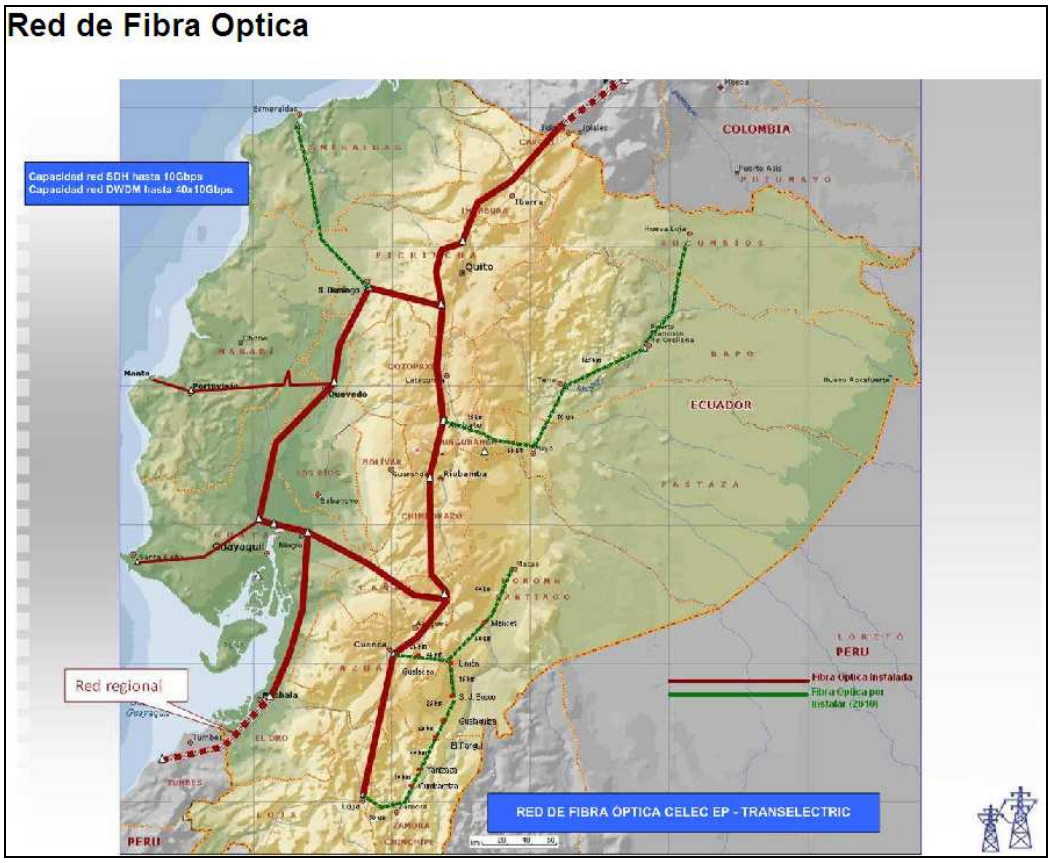

Figura 3.1 Red de fibra óptica de CELEC EP – TRANSELECTRIC

Las rutas internas del país tienen una capacidad de STM-16 (red CELEC EP - TRANSELECTRIC) y la ruta de salida internacional hacia Colombia es de STM-64 (red TRANSNEXA). También esta puesta en marcha la integración a la red regional que une los países de Venezuela, Colombia, Ecuador, Perú y Chile y posteriormente Argentina y Brasil. Para esto la red tiene una interconexión con Perú con una capacidad de 2 STM-16 y un STM-64 (red TRANSNEXA).

La red de trasporte consta con un Centro de Gestión que opera los 365 días del año las 24 horas de forma continua para garantizar la disponibilidad de la red. La disponibilidad de la red de CELEC EP - TRANSELECTRIC para el servicio portador es del 99,8% y para el servicio de valor agregado es del 99,6%.

EVALUACIÓN DE LA TECNOLOGÍA SDH

1.1.18 Servicios disponibles para Clientes

Los servicios que ofrece son de dos tipos:

1.1.18.1 Servicio Valor Agregado

Características:

Desde el año 2007, CELEC EP – TRANSELECTRIC cuenta con la licencia para brindar este servicio.

El medio físico es una red de fibra óptica.

El nodo de conexión se encuentra en Quito, con salidas internacionales por Colombia y Perú.

Este servicio se brinda a empresas del Sector Eléctrico.

La disponibilidad que se ofrece es del 99,6 %.

Conexión:

Se conecta a través de un enrutador IP-v4 cuyo protocolo de enrutamiento es BGP[5]-v4.

Las interfaces de conexión son ópticas y eléctricas. Las interfaces eléctricas son E1, DS3[6], STM-1 y Fast Ethernet que se basan en las normas UIT-T

[5] Border Gateway Protocol.
[6] Digital Signal 3.

G.703[7] e IEEE 802.3.[8] Las interfaces ópticas que se utilizan son Gigabit Ethernet cuya norma es la 802.3u[9].

1.1.18.2 Servicio Portador

Características:

Desde el año 2003, CELEC EP – TRANSELECTRIC cuenta con la licencia para brindar este servicio.

El medio físico es una red de fibra óptica que permite la conexión entre los nodos de la red de transporte.

La transmisión de datos se realiza por la red de transporte que cuenta con tecnologías SDH y DWDM por la cual el cliente puede enviar el tipo de información que se ajuste a sus requerimientos (voz, datos, video e internet).

Conexión:

Las interfaces de conexión son ópticas y eléctricas. Las interfaces eléctricas son E1, DS3, STM-1 y Fast Ethernet que se basan en las normas UIT-T G.703 e IEEE 802.3. Las interfaces ópticas que se utilizan son STM-1, STM-4, STM-16, STM-64, Gigabit Ethernet, 10 Gigabit Ethernet (norma es la 802.3u).

Es importante mencionar que no brinda el servicio de última milla hacia los clientes.

[7] Estándar de la UIT-T que define las características físicas y eléctricas de la interfaz para transmitir voz o datos sobre canales digitales.
[8] 10 BASE5 10 Mbit/s sobre coaxial grueso (thicknet). Longitud máxima del segmento 500 metros.
[9] 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet a 100 Mbit/s con auto-negociación de velocidad.

DESCRIPCIÓN DE LA RED SDH DE CELEC EP – TRANSELECTRIC

1.1.19 Servicios disponibles para CELEC EP – TRANSELECTRIC

Canales de voz
Datos en tiempo real (FRONT ENDS)
Teleprotección
Red Corporativa
Videoconferencia.
Gestión remota de los sistemas de control y protecciones.
Acceso a los servidores de aplicaciones como son: Correo, Intranet, Apipro, Sistema Integrado de Información, E -Business, etc.

1.1.20 Situación Actual de la Red en cada Nodo de la Red SDH

1.1.20.1 Estructura de la Red

La red de transporte de CELEC EP - TRANSELECTRIC que maneja altas capacidades y cuenta con tecnologías SDH Y DWDM.

La red actual presenta una topología anillada con radiales cubriendo las ciudades de: Quito, Guayaquil, Cuenca, Santo Domingo, Quevedo, Manta, Santa Elena, Machala, Tulcán, Riobamba, Ambato y Loja, en algunas de las ciudades mencionadas se cuentan con varios nodos lo cual se detallará posteriormente.

En esta red cabe señalar que existen dos tipos de nodos en las ciudades antes mencionadas.

Un nodo corresponde propiamente a la red de transporte de CELEC EP - TRANSELECTRIC que opera en las subestaciones del SNT (Sistema Nacional de Transmisión).

Y el otro nodo conocido como Punto de Presencia (PDP), que está ubicado en sitios más centrales en varias ciudades del país.

En la actualidad se encuentra en marcha el proyecto para unir a las ciudades de la Región Oriental como Macas, Puyo, Tena, Coca y Baños a la red de transporte, utilizando la misma metodología de nodos antes mencionados.

1.1.20.2 Topología de la Red SDH

En la Figura 3.2 se detalla los equipos que se encuentran instalados en los diferentes nodos de la red SDH.

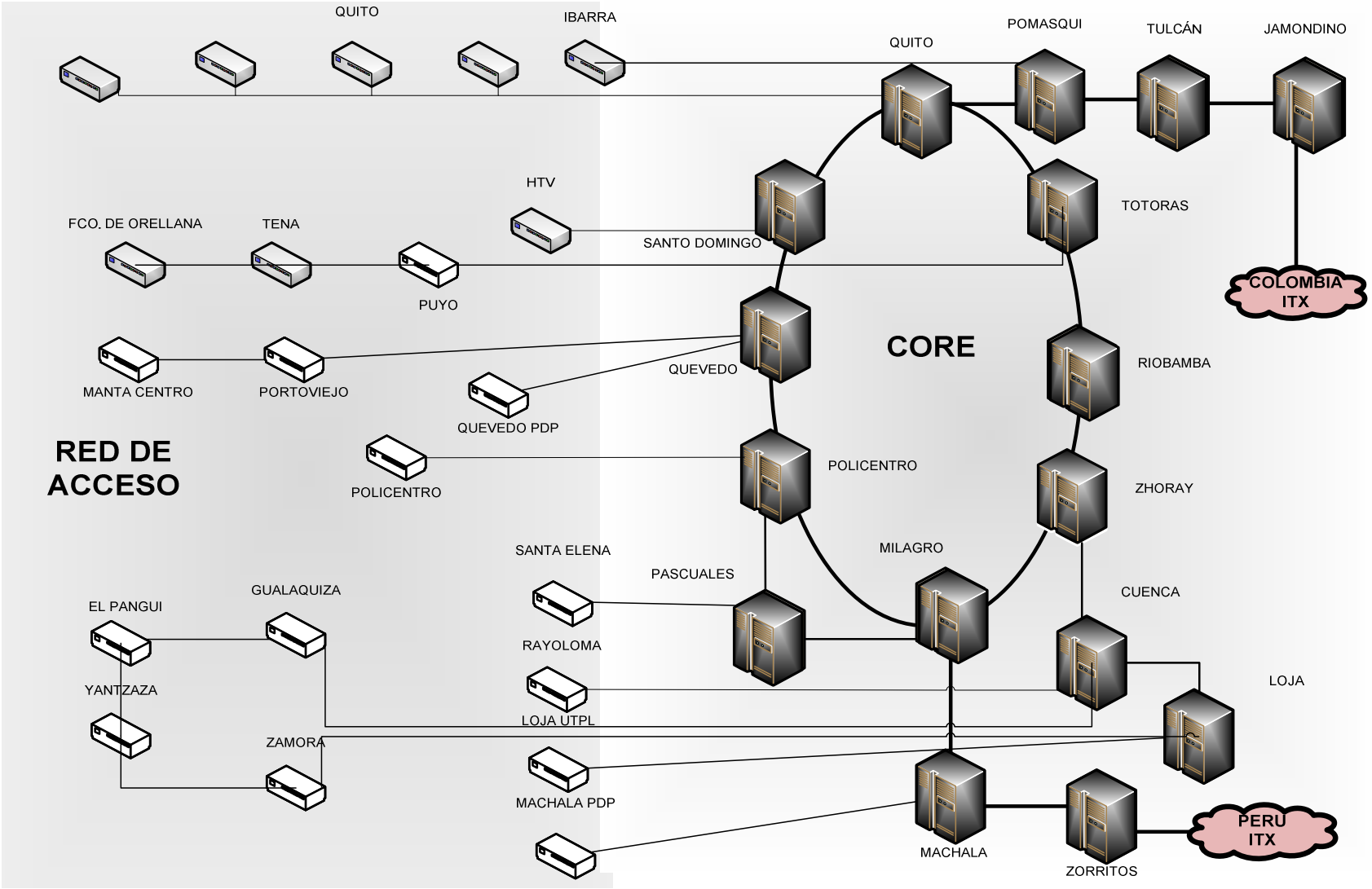

Figura 3.2 Red SDH CELEC EP – TRANSELECTRIC

1.1.21 Tráfico y Capacidades de la Red

1.1.21.1 Tráfico Interno (Nacional)

Capacidad SDH

En las rutas internas entre las principales ciudades, se encuentra operando una capacidad física de:

Cantidad	Capacidad	Capacidad en Mbps	Capacidad Total en Mbps
8	STM-1	155,52	1244,16
3	STM-4	622,08	1866,24
22	STM-16	2488,32	54743,04
5	STM-64	9953,28	49766,40
TOTAL			107619,84

Tabla 3.1 Capacidad total SDH

Las capacidades tanto operativa, disponible y total por tramos se encuentran detalladas en la Tabla 3.2

NE A	NE B	Capacidad Instalada	Cantidad de enlaces a nivel STM-N
STO. DOMINGO SMA	QVDO SMA	STM-16	1
QVDO SMA	POLICENTRO SMA	STM-16	1
POLICENTRO SMA	PASCUALES SMA	STM-1	2
PASCUALES SMA	POLICENTRO DC	STM-1	1
PASCUALES SMA	MILAGRO DC	STM-1	1
TE SC	TE SMA	STM-1	4
TE SC	TE DC	STM-16	2
TE DC	STO. DOMINGO DC	STM-16	1
STO. DOMINGO DC	QVDO DC	STM-16	1
QVDO DC	POLICENTRO DC	STM-16	1
POLICENTRO DC	MILAGRO DC	STM-16	4
MILAGRO DC	MACHALA DC	STM-16	3
MACHALA DC	ZORRITOS	STM -16	2
MACHALA DC	ZORRITOS	STM - 64	1
MILAGRO DC	ZHORAY SMA	STM-16	1
ZHORAY SMA	CUENCA SMA	STM-16	1
ZHORAY SMA	RIOBAMBA SMA	STM-4	1
CUENCA SMA	LOJA SMA	STM-4	2
TE DC	POMASQUI HUA	STM-64	1
TE DC	TOTORAS OSN	STM-16	1
TOTORAS OSN	RIOBAMBA OSN	STM-16	1
ZHORAY OSN	RIOBAMBA OSN	STM-16	1
MILAGRO DC	RIOBAMBA OSN	STM-16	1
POMASQUI OSN	TULCAN OSN	STM-64	1
TULCAN OSN	JAMONDINO OSN	STM-64	1
JAMONDINO OSN	ITX OSN	STM-64	1

Tabla 3.2 Capacidad por tramos de la Red SDH

1.1.22 Plataformas de Gestión de la Red SDH

1.1.22.1 Descripción de los Equipos del Core

Siemens Surpass hiT7070

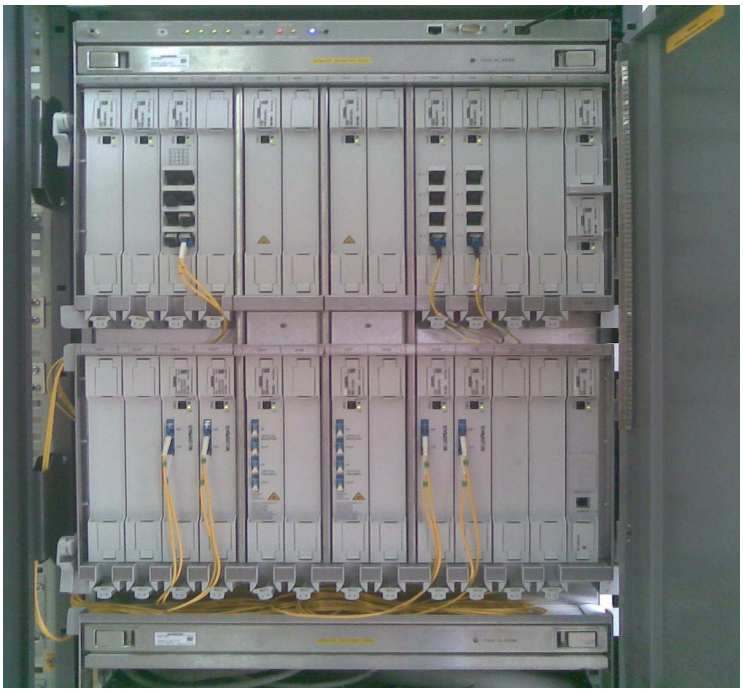

Figura 3.3. Fotografía equipo Siemens Surpass hiT7070

Unidad de conmutación de 160G para capacidades de alto orden y 10G para capacidades de bajo orden.

Funcionalidad (Resilient Packet Ring RPR, Multiprotocol Label Switching MPLS) realiza conmutación de capa 2.

Variedad de interfaces STM-64 incluyendo DWDM.

Conserva las funciones de protección SDH (SNCP, MSP, BSHR, Hardware)

Integrable con el sistema de gestión de altas prestaciones TNMS-Core de Siemens.

Es posible la interconexión para anillos en todos los puertos de tráfico.

Parada automática en caso de una interrupción del enlace de acuerdo con UIT-T G.664.[10]

Equipamiento sencillo y modular.

Posee dos núcleos de operación, llamados single y dual core. Cada una de estas capas maneja sistemas tributarios de alto y bajo orden SDH.

Siemens SMA16

Figura 3.4. Fotografía equipo Siemens SMA 16

Protección 1+1 para interfaces ópticas STM-1/4/16.

[10] Procedimientos y requisitos de seguridad óptica para sistemas ópticos de transporte.

Huawei OSN 3500

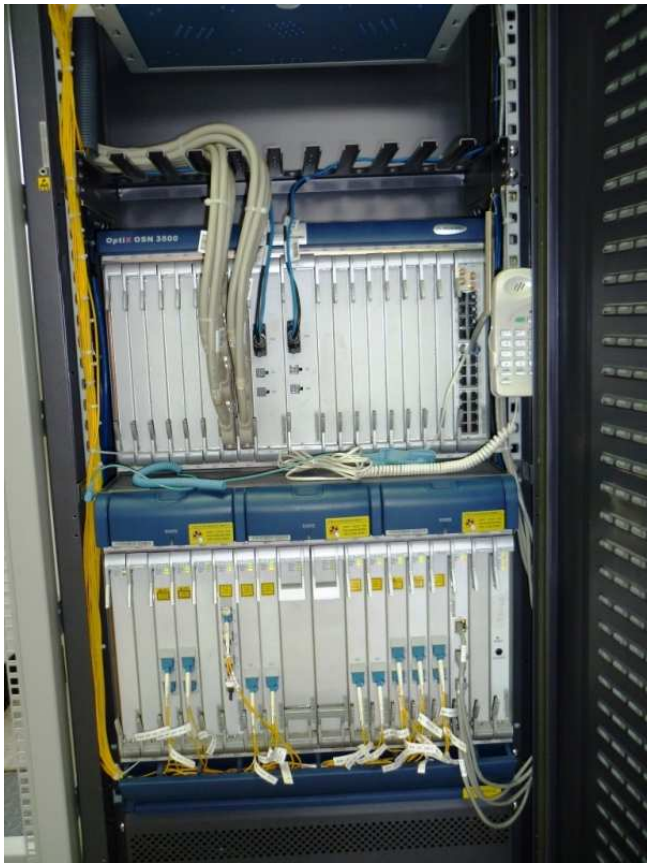

Figura 3.5. Fotografía equipo Huawei OSN 3500

Compatibilidad con STM-64/16/4/1.

Provisión multiservicio en interfaces: STM-1 (Óptico/Eléctrico); STM-4/16/64 estándar o concatenados; E1/T1/E3/T3/E4; ATM; y otros.

Provisto de protocolo GMPLS para servicios end-to-end.

Tecnología WDM incorporada.

Completos mecanismos de protección de red: Protección SDH (1+N).

Soporta 2F/4F MSP, SNCP, DNI, también comparte fibra para protección virtual.

Soporta protección en anillo RPR y STP (spanning tree protection).

Huawei OSN 7500

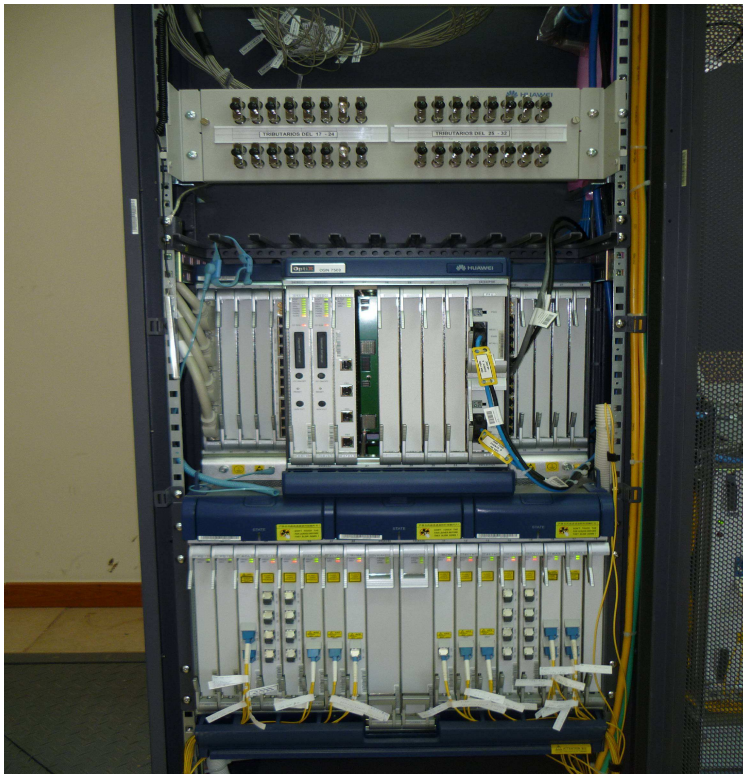

Figura 3.6. Fotografía equipo Huawei OSN 7500

Incorpora las siguientes tecnologías: SDH, PDH, Ethernet, ATM, SAN,[11] WDM,[12] DDN,[13] ASON.[14]

Compatible con sistemas STM-64.

MSTP[15] Network.

Protecciones SNCP[16] y MSP.[17]

[11] Storage Area Network.
[12] Wavelength Division Multiplexing.
[13] Digital Data Network.
[14] Automatically Switched Optical Network.
[15] Multi-Services Transmission Platform.
[16] Subnetwork Conection Protection.
[17] Multiplex Section Protection.

1.1.23 Sistemas de Gestión SIEMENS y HUAWEI

1.1.23.1 Sistema de Gestión Huawei T2000

Huawei T2000 System Manager (Huawei T2000) se utiliza para administrar dispositivos de Huawei de transporte, tales como SDH / SONET y multiplexación por división de longitud de onda (DWDM). Huawei T2000 también administra las conexiones topológicas entre los dispositivos y conexiones de subred. Huawei T2000 utiliza el Common Object Request Broker Architecture (CORBA) hacia el norte de interfaz que se ajusta plenamente a TMF 814 v2.1.

Cuando la integración de Network Manager Edition Transmisión con Huawei T2000, los datos de la interfaz CORBA se utiliza en todas las funciones de Network Manager Edition de transmisión, tales como el descubrimiento de elementos de red, la votación de los activos, y realización de encuestas de conexión de red.

Características

Poderosa red de gestión de la capa.
Alarma de la correlación y la supresión de la pantalla de alarma.
Alarma automática, la función de alerta temprana.
Topología de la red de auto-descubrimiento y de negocios.
ASON funciones de gestión de red, la tradicional red SDH y ASON red integrada de gestión.
Interfaz abierta hacia el norte y pre-integración.
Soporta hasta 32 usuarios del cliente.
Descentralización (NAD), Fenwick (FAD) de gestión.
Cliente de control de la dirección IP.
Poderosa red la capacidad de gestión.

Características y ventajas

Característica	Beneficio
Elemento de red a nivel de gestión de red con capacidades de gestión de pequeñas y medianas empresas de la red	Elemento de red a nivel de gestión de red a la parte de inversión de la red de acceso de nivel a las funciones de gestión de la red, el ahorro de la inversión del usuario
De extremo a extremo la gestión empresarial, incluyendo SDH, WDM, Ethernet, ASON.	Fácilmente administrar, supervisar todos los servicios de red
Apoyo a la correlación de alarmas	El no asistir al personal de mantener a encontrar rápidamente la fuente
Programa integral de seguridad, incluyendo controles de acceso de cliente, la separación de poderes Fenwick, SSL	Eficaz combinación de varios mecanismos de seguridad, para garantizar plenamente el funcionamiento seguro de la gestión de la red
Programas integrales de seguridad, incluyendo copia de seguridad de doble disco, la protección de DCN, automatizado de datos de elementos de la red de sincronización	A través de la copia de seguridad de datos, protección, etc, para mejorar la fiabilidad de la red, reducir las pérdidas de la red causada por la falla inesperada
ASON de gestión de red, incluida la integración de las redes SDH y de gestión de red ASON	Un sistema de gestión de dos redes, una gestión más conveniente, ahorro e inversión
Una variedad de interfaz abierta hacia el norte con otros fabricantes para lograr sistemas de alta dirección y de acoplamiento	Buen sistema de red abierta, eficaz para acortar el ciclo de la construcción, ahorrando el costo de la inversión
Y la planificación de sistemas de simulación (OptiX MDS 6600) con la planificación de la red y la simulación	Para ayudar a comprender los cuellos de botella de la red actual de recursos, los parámetros de fiabilidad de la red, rápido y razonable para completar la planificación de nuevas redes y planificación de la expansión

Tabla 3.3 Características y ventajas

1.1.23.2 Sistema de Gestión Siemens TNMS

El sistema de gestión TNMS, es el producto de TMN de próxima generación para implementar una gestión integrada de la totalidad de la red óptica, incluyendo sistemas DWDM, (NG) SDH, IP, SAN, PDH/Acceso, así como soportar (ASTN).[18] La familia de productos TNMS Core provee una serie de funcionalidades de gestión que abarcan todos los aspectos necesarios para un eficiente control de las redes de transporte:

Configuración
Fallas
Performance
Seguridad

El TNMS Core/CDM ofrece una nueva dimensión operativa a través de excelentes características de visibilidad de red y facilidades de navegación intuitivas, basadas en un entorno Microsoft-Windows, que ha probado su enorme valor en más de 200 instalaciones alrededor de más de 40 países. El sistema operativo a utilizar es Windows 2000 para las versiones de TNMS-Core mencionadas en esta propuesta.

A través de sus interfaces abiertas y de la ejecución de la interfaz NML-EML basada en CORBA, se puede integrar con gran facilidad en otras capas TMN y permite la gestión centralizada de redes multifabricante. El TNMS es altamente escalable y evoluciona a medida que lo hace la red del operador.

Además de las funcionalidades generales de gestión definidas en ITU-T M.3010, el TNMS Core/CDM ofrece las siguientes funcionalidades:

Soporte de elementos de red y funcionalidades de capa de red y de servicios, en una única plataforma.

[18] Automatic Switched Transport Network.

Gestión de redes multitecnología, que incluyen sistemas DWDM, (NG) SDH, PDH, IP y SAN.

Gestores de elemento de red integrados que otorgan el mismo ambiente de trabajo que la Local Craft Terminal (LCT).

Arquitectura de HW y SW escalable para ser aplicable a redes desde pequeñas hasta extra grandes.

Procesamiento optimizado de bases de datos de alta performance.

Amigable interfaz de usuario gráfica (GUI) basada en tecnología Microsoft.

Interfaces northbound y southbound basadas en standards (TMF CORBA, SNMP) para ambientes de gestión multivendor.

Conformidad con los standards internacionales (ITU-T, ETSI, TMF).

CAPÍTULO IV

DISEÑO Y PRUEBAS DE LAS PROTECCIONES EN LA RED SDH DE CELEC EP – TRANSELECTRIC

DISEÑO DE LA RED CON LOS DIFERENTES TIPOS DE PROTECCIONES SDH

CELEC EP – TRANSELECTRIC es una empresa líder en telecomunicaciones, frente a la necesidad de una red segura que cuente con un sistema de protección a nivel SDH, ha decidido aprovechar la infraestructura actual instalada en su red de core y diseñar una red con diferentes sistemas de protección para la red con tecnología SDH en todos sus niveles STM-n, la misma que permitirá tener un transporte de datos seguro, una alta disponibilidad y además la posibilidad de un crecimiento a futuro si la demanda así lo requiere.

El disponer de una red alternativa SDH como protección de la red principal de core permitirá una mayor confiabilidad en la conexión, la cual planteará una disminución de indisponibilidad en la red.

La red de transporte SDH de CELEC EP – TRANSELECTRIC consta de nodos a nivel de las tres regiones del Ecuador en los cuales se tiene diferentes marcas de multiplexores que operan en conjunto. Sus capacidades a nivel de SDH van desde STM-1, STM-4, STM-16 y STM-64 dando lugar a una red de alta capacidad en lo que a manejo de tráfico se refiere.

La Figura 4.1 y 4.2 muestra el estado actual de la Red de Transporte SDH.

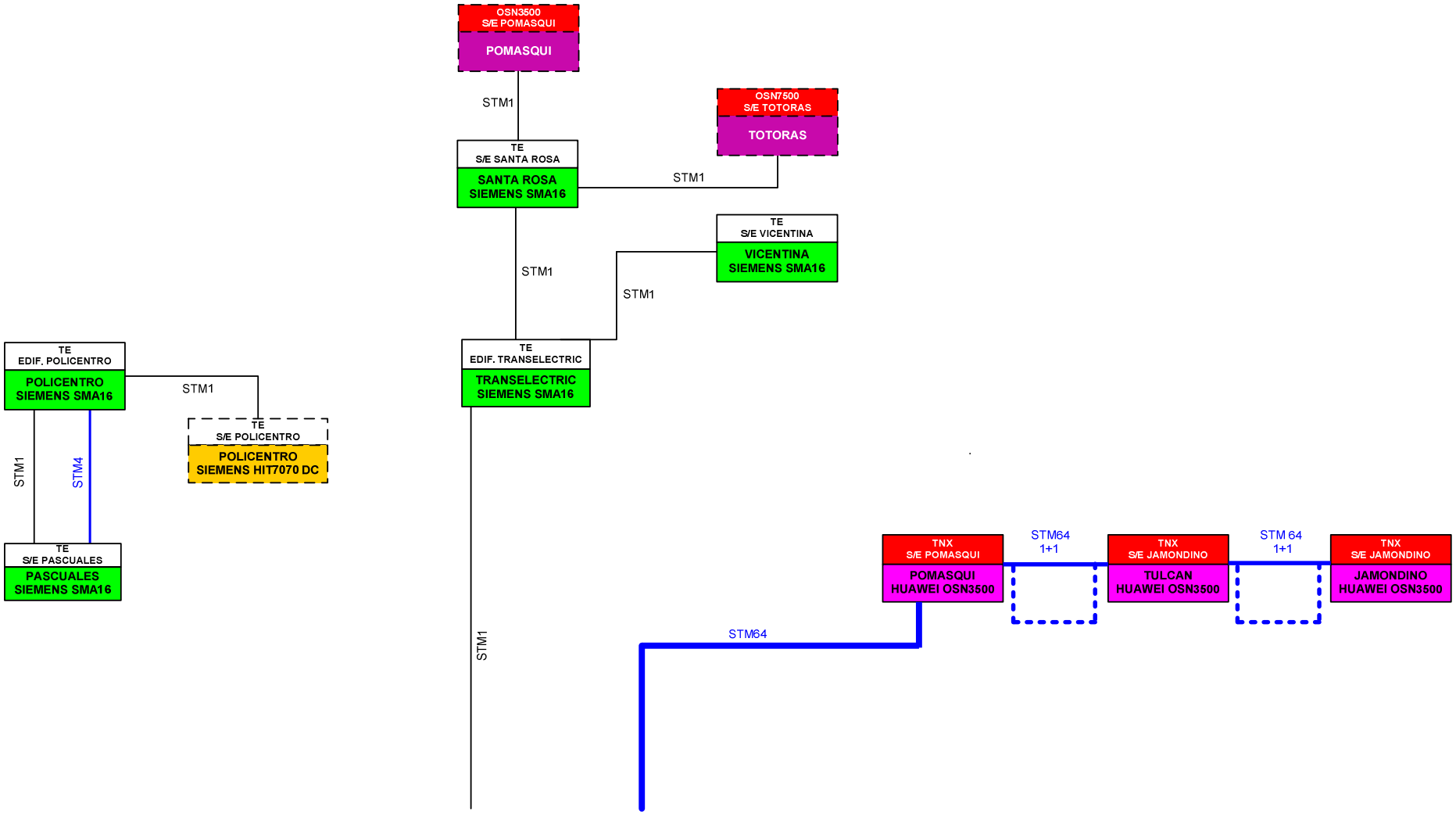

Figura 4.1 Estado actual de la red SDH de CELEC EP – TRANSELECTRIC (Parte 1)

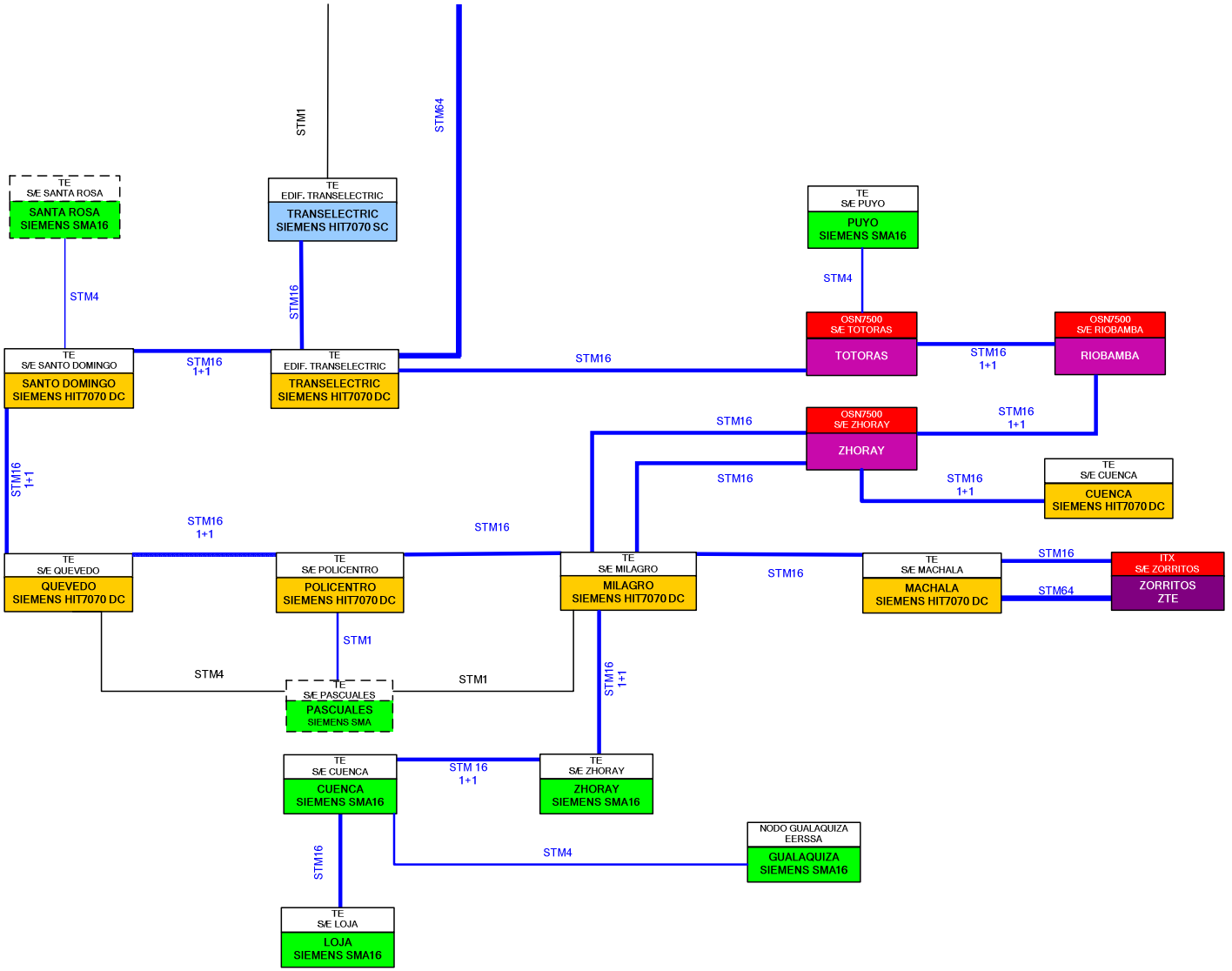

Figura 4.2 Estado actual de la red SDH de CELEC EP – TRANSELECTRIC (Parte 2)

El continuo crecimiento de las telecomunicaciones en el país ha llevado a que CELEC EP – TRANSELECTRIC realice incrementos de capacidades (enlaces STM-N) y aumento de número de nodos en su red de transporte, tratando con esto de mantener una alta disponibilidad en servicios a clientes; es por eso que han implementado esquemas de protección tanto en anillo como lineales.

El siguiente diseño para protección de la red SDH es creado en base a las necesidades y capacidad de tráfico que se tiene en la red de transporte de CELEC EP – TRANSELECTRIC, pretendiendo como resultado una topología más robusta, y con esto disminuir el tiempo de indisponibilidad que se pueda producir frente a una falla en tiempo real.

La Figura 4.3 y 4.4 muestran el Diseño de la Red de Transporte SDH con los diferentes esquemas de protección a implementarse.

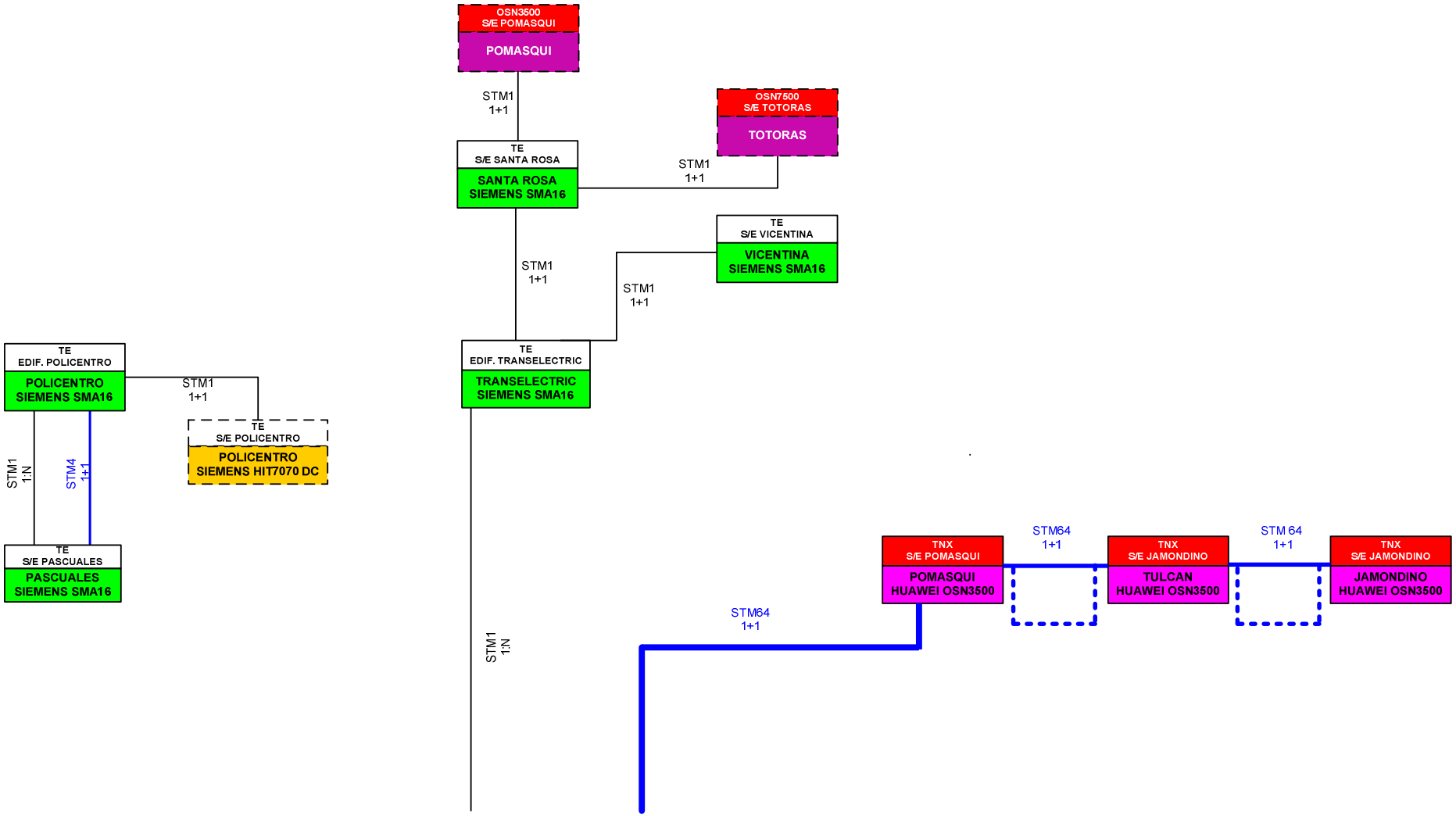

Figura 4.3 Diseño con sistema de protecciones para la red de transporte SDH de CELEC EP – TRANSELECTRIC (parte 1)

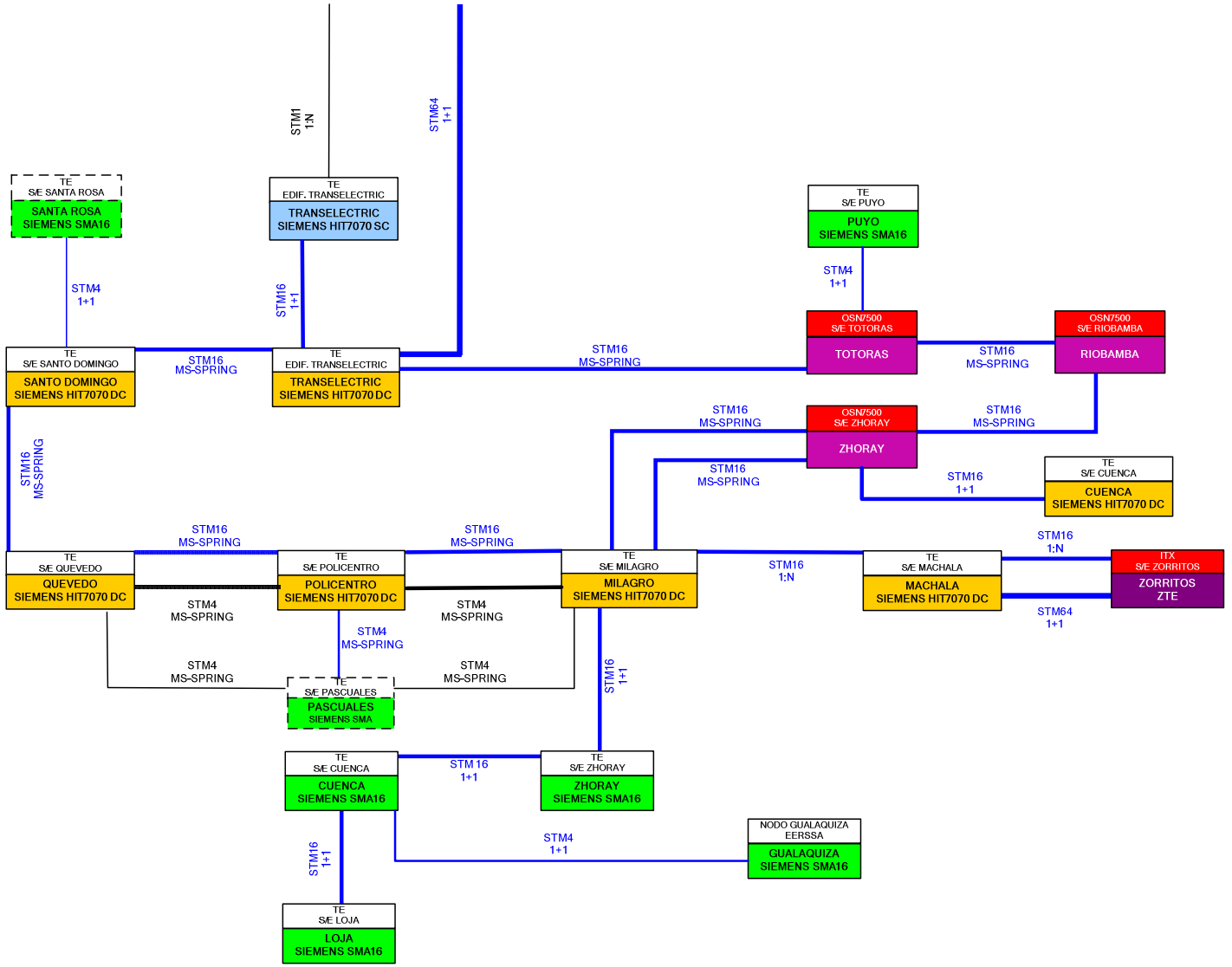

Figura 4.4 Diseño con sistema de protecciones para la red de transporte SDH de CELEC EP – TRANSELECTRIC (parte 2)

El diseño de la red de protección SDH fue basada en necesidades reales de acuerdo a la topología actual tanto en anillo, lineal y radial.

Las protecciones a utilizarse son:

1+1 MSP[19] y 1:N MSP, para tramos lineales y radiales.
MS-SPRING[20] para las topologías en anillo.
SNCP[21] a nivel de servicio.

Las capacidades a nivel STM-N a protegerse son STM-1, STM-4, STM-16 y STM-64 las cuales forman parte de la topología de la red de transporte SDH.

1.1.24 Nodos y sus Protecciones

Protección 1+1 MSP donde el tráfico es inicialmente enviado tanto por la ruta activa como por la ruta de protección. Si se detecta una pérdida de tráfico, en el extremo receptor de la ruta alterna se produce un proceso de conmutación hacia el camino de protección.

Lineal: Transelectric (Siemens SMA 16), Santa Rosa (Siemens SMA 16) y Pomasqui (Huawei OSN 3500). Capacidad STM-1.

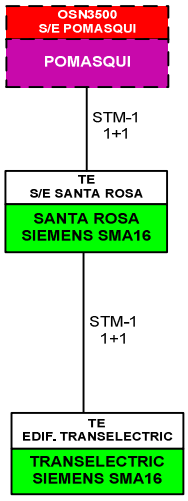

Figura 4.5 Configuración Lineal a nivel STM-1

[19] Multiplex Section Protection
[20] Multiplex Section-Shared Protection Ring
[21] Subnetwork Connection Protection

Lineal: Transelectric (Siemens HiT7070 DC), Pomasqui (Huawei OSN 3500), Tulcán (Huawei OSN 3500) y Jamondino (Huawei OSN 3500). Capacidad STM-64.

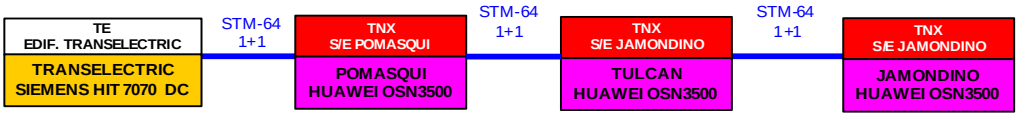

Figura 4.6 Configuración Lineal a nivel STM-64

Lineal: Milagro (Siemens HiT7070 DC), Zhoray (Siemens SMA 16), Cuenca (Siemens SMA 16) y Loja (Siemens SMA 16). Capacidad STM-16.

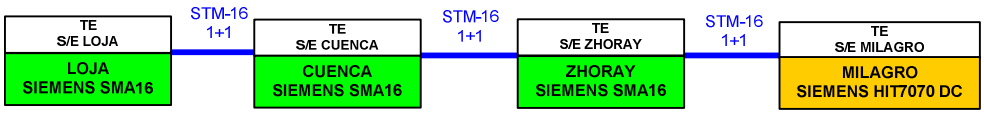

Figura 4.7 Configuración Lineal a nivel STM-16

Radial: Transelectric (Siemens SMA 16) y Vicentina (Siemens SMA 16). Capacidad STM-1.

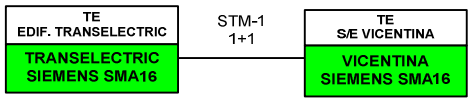

Figura 4.8 Configuración Radial a nivel STM-1

Radial: Santa Rosa (Siemens SMA 16) y Totoras (Huawei OSN 7500). Capacidad STM-1.

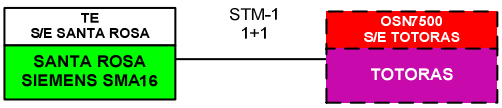

Figura 4.9 Configuración Radial a nivel STM-1

Radial: Santo Domingo (Siemens HiT7070 DC) y Santa Rosa (Siemens SMA 16). Capacidad STM-4.

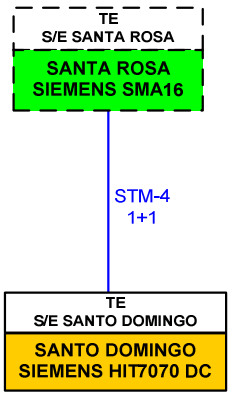

Figura 4.10 Configuración Radial a nivel STM-4

Radial: Puyo (Siemens SMA 16) y Totoras (Huawei OSN 7500). Capacidad STM-4.

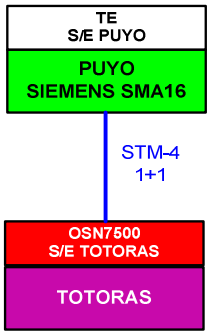

Figura 4.11 Configuración Radial a nivel STM-4

Radial: Zhoray (Huawei OSN 7500) y Cuenca (Siemens HiT7070 DC). Capacidad STM-16.

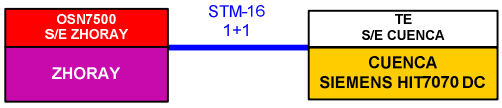

Figura 4.12 Configuración Radial a nivel STM-16

Radial: Machala (Siemens HiT7070 DC) y Zorritos (ZTE). Capacidad STM-64.

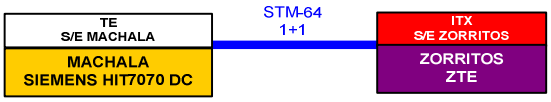

Figura 4.13 Configuración Radial a nivel STM-64

Radial: Cuenca (Siemens SMA 16) y Gualaquiza (Siemens SMA 16). Capacidad STM-4.

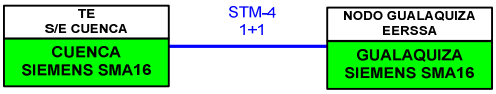

Figura 4.14 Configuración Radial a nivel STM-4

Protección 1: N MSP es similar al tratado 1:1 con la excepción de que varios canales operativos pueden ser protegidos por un único canal de respaldo.

Radial: Milagro (Siemens HiT7070 DC), Machala (Siemens HiT7070 DC). Capacidad STM-16.

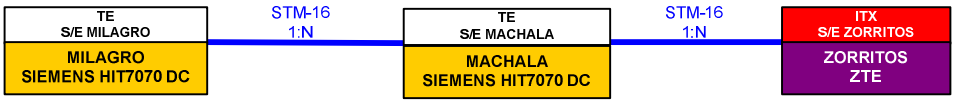

Figura 4.15 Configuración Radial a nivel STM-16

Protección MS-SPRing es un mecanismo de protección de anillo, el tráfico es enviado por una ruta en torno al anillo.

Anillo Central: Transelectric (Siemens HiT7070 DC), Santo Domingo (Siemens HiT7070 DC), Quevedo (Siemens HiT7070 DC), Policentro (Siemens HiT7070 DC), Milagro (Siemens HiT7070 DC), Zhoray (Huawei OSN 7500), Riobamba (Huawei OSN 7500) y Totoras (Huawei OSN 7500). Capacidad STM-16.

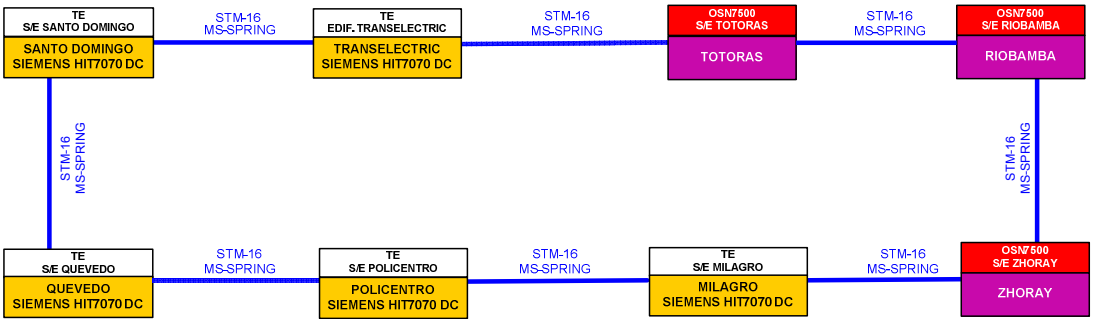

Figura 4.16 Configuración en Anillo a nivel STM-16

Protección SNCP es similar a la protección MSP, pero en la cual, la conmutación SNCP puede ser iniciada en un extremo de la ruta y llegar hasta un nodo intermedio. La red puede ser descompuesta con un número de subredes interconectadas. Con cada protección de subred se proporciona un nivel de ruta y la conmutación automática de protección entre dos caminos es proporcionada en las fronteras de subred.

El esquema de protección SNCP involucra la protección de contenedores virtuales individuales a través de una ruta punto a punto. Si existe un evento de fallo, únicamente el contenedor virtual en cuestión es conmutado a una ruta alternativa, así que la protección individual para un único VC es posible.

Cabe mencionar que el camino de subred puede ser aplicado tanto para caminos de alto orden como de bajo orden (tanto para VC-4 y VC-3 como para VC-12).

Las pruebas para este tipo de protección se realizaron en un anillo a nivel de servicio con un VC-12 entre los siguientes nodos: Transelectric (Siemens HiT7070 DC), Policentro (Siemens HiT7070 DC), Totoras (Huawei OSN 7500), Riobamba (Huawei OSN 7500), Zhoray (Huawei OSN 7500) y Milagro (Siemens HiT7070 DC). Capacidad VC-12.

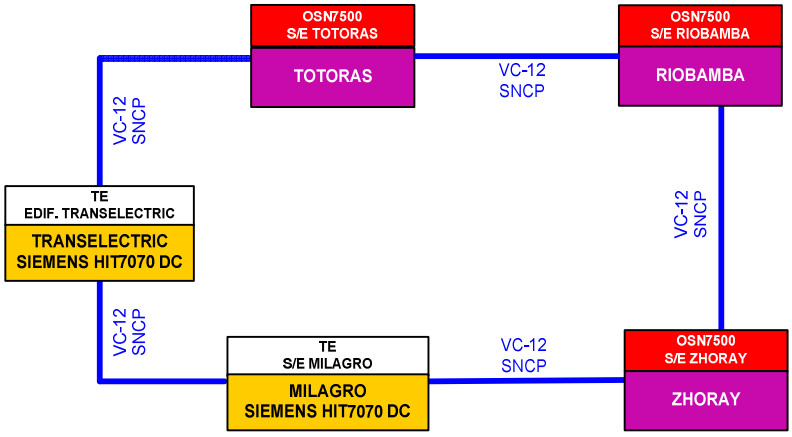

Figura 4.17 Configuración en Anillo a nivel VC-12

DESCRIPCIÓN Y JUSTIFICACIÓN DE LAS PROTECCIONES SDH UTILIZADAS

Las modernas redes de telecomunicaciones deben proporcionar capacidad y ancho de banda suficiente para soportar el tráfico, pero además deben tener la capacidad de protegerse y recuperarse de forma robusta, de una manera eficiente frente a la aparición de fallos. A mayor cantidad de tráfico transportado, más importante es el efecto causado por un fallo en la red.

En general, la selección y evaluación de un mecanismo se basa en el uso entre los recursos utilizados y/o reservados para la protección y la minimización del tiempo necesario para restaurar la conectividad en caso de fallo. Por ejemplo, los mecanismos con un tiempo mínimo de restauración suelen necesitar el aprovisionamiento de recursos dedicados y en consecuencia un uso menos eficiente de los recursos de la red.

El objetivo del nuevo diseño de la red de transporte SDH de CELEC EP - TRANSELECTRIC es probar la interoperabilidad de los sistemas de gestión con la que está implementada, y analizar los diferentes mecanismos por los que se puede recuperar los servicios una vez ocurrida una falla en función de las topologías de red sobre las que trabaja y en los protocolos en los que se apoya para realizar su función.

Los procedimientos de protección de red son empleados para auto-recuperarse de fallos. Los esquemas de protección a utilizarse comprobarán que un elemento de red al detectar un fallo o una pérdida de tráfico iniciará acciones correctivas sin involucrar al sistema de gestión de red o peor aún al tráfico que circule por el mismo. La protección requiere la reserva previa de recursos (típicamente se requiere un 100% de redundancia de recursos) y está diseñada para reaccionar ante fallos rápidamente, el tiempo de respuesta en mecanismos de este tipo es, en el peor de los casos, inferior a 50 ms.

Dentro de los mecanismos de protección se diseñó la red de transporte SDH con los siguientes esquemas: 1:N MSP, 1+1 MSP, MS-Spring y SNCP.

Las protecciones utilizadas en el diseño de la red de transporte SDH de CELEC EP – TRANSELECTRIC fueron establecidas de acuerdo a las necesidades de la red.

Cada tramo, topología, capacidad a nivel STM-n y sistema de protección se ha diseñado para cumplir el nivel de disponibilidad establecido para cumplir con el Acuerdo de Nivel de Servicio (SLA) ofertado a clientes.

Se dividió la red en tramos lineales, Radiales y en anillo, dando lugar a la utilización de sistemas de protecciones 1:N MSP, 1+1 MSP, MS-SPRING y SNCP para con esto mejorar la robustez de la red y disminuir tiempos de indisponibilidad.

La descripción y justificación de los Sistemas de Protecciones a utilizar se detalla a continuación:

1.1.25 Sistema de Protección 1+1 MSP

El tráfico se transmite simultáneamente sobre el enlace principal y sobre la protección de línea.

Tipo de conmutación: unidireccional o bidireccional.

Tipo de operación: reversible o no reversible.

Este esquema de protección es implementado con la idea de utilizar este mecanismo de protección como redundancia. El hecho de enviar la información por dos caminos distintos hace que si en cualquiera de los dos ocurren fallos, tengamos siempre un camino de respaldo.

La red de transporte SDH tiene enlaces radiales y lineales, que dependiendo de las necesidades y configuración de la misma, es necesario implementar un sistema de protección que, teniendo dos caminos activos, sea cual sea el que falle, tenga una manera de recuperarse. La mayor desventaja de este sistema es que en funcionamiento normal, que es la mayor parte del tiempo, estamos consumiendo el doble de recursos de los necesarios.

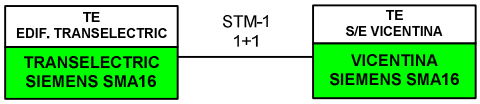

Figura 4.18 Tramo radial Transelectric - Vicentina con protección 1+1 MSP

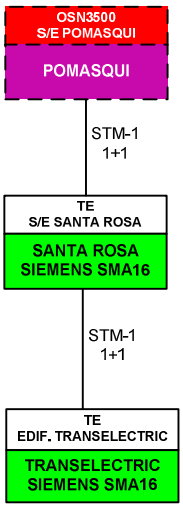

Figura 4.19 Tramo lineal Transelectric - Santa Rosa - Pomasqui con protección 1+1 MSP

1.1.26 Sistema de Protección 1:N MSP

El esquema de protección 1:N tiene N canales de tráfico y 1 canal de protección. Cuando la red no tiene fallas, N canales principales pueden transmitir el tráfico normal mientras que el canal de protección transmite tráfico extra o simplemente no transmite tráfico.

Tipo de conmutación: bi-direccional.
Tipo de operación: reversible.

El continuo crecimiento de la red de transporte SDH de CELEC EP - TRANSELECTRIC ha hecho que se establezcan esquemas de protección como el 1:N MSP en la red, donde la disponibilidad de tarjetas y el número de enlaces de línea en el tramo a ser protegido son un factor importante para levantar un Sistema de Protección de estas características. El reducido número de slots libres es otro factor el cual se debe tomar en cuenta a la hora de escoger un esquema de protección, como es el caso de los tramos protegidos con Sistemas 1:N MSP, en donde los equipos multiplexores que comprenden estos tramos ya no tienen slots disponibles, y por ahora el número de tarjetas en stock es reducido.

Todos estos factores hacen que en ciertos tramos de la red de transporte SDH, el esquema de protección implementado y probado fuese el 1:N MSP, dando con esto, a pesar de las limitaciones antes expuestas, un Sistema de Protección robusto y con un alto porcentaje de disponibilidad.

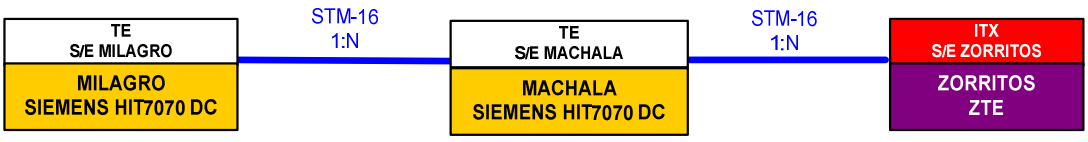

Figura 4.20 Tramo lineal Milagro - Machala - Zorritos con protección 1:N MSP

1.1.27 Sistema de Protección MS-SPRING

Para el diseño de la red de transporte SDH se utilizó el mecanismo de anillo de protección compartida de la sección de multiplexación, comúnmente llamados "MS-SPRing".

El esquema de protección MS-SPRings tiende a ser usado en una topología de anillo mientras que la restauración se emplea en redes malladas de alto nivel con gran cantidad de cross-conexiones. Este tipo de protección protege a nivel de anillo todo el tráfico, si el anillo se compone de 16 hilos de fibra, 8 serán de trabajo y 8 de protección.

El tráfico es enviado por una sola ruta en torno al tramo a protegerse. No existe un camino de protección dedicado por cada ruta activa. La conmutación del enlace de protección es iniciada a nivel de sección de modo similar a la protección lineal de la sección de multiplexación; ante un evento de fallo, todo el tráfico de la sección es conmutado. Este mecanismo se puede llevar a cabo salvando una importante cantidad de capacidad frente al mecanismo de anillo de protección dedicado.

La ubicación de las tarjetas dentro del multiplexor, sea cual fuere su marca, tiene un papel importante dentro del desarrollo o no del esquema de protección. Las pruebas del esquema de protección MS - SPRING no pudieron llevarse a cabo de manera práctica y fueron realizadas de manera lógica utilizando herramientas, dentro del mismo software del multiplexor, que simularon escenarios reales a condiciones reales.

La ejecución de las pruebas de manera práctica para este esquema de protección implicaban reubicar tarjetas dentro del multiplexor, migrar tráfico y con esto provocar tiempo de indisponibilidad en los enlaces, por lo que se procedió a realizar pruebas de manera lógica utilizando una herramienta de ensayo llamada TEST RING, la cual permitió realizar una simulación del Sistema de Protección ante un evento de falla real utilizando una topología en anillo compuesta de nodos

previamente definidos. Para estas pruebas se utilizó un canal STM-16 llevando a cabo una simulación de una falla real con capacidad de 2.5 Gbps.

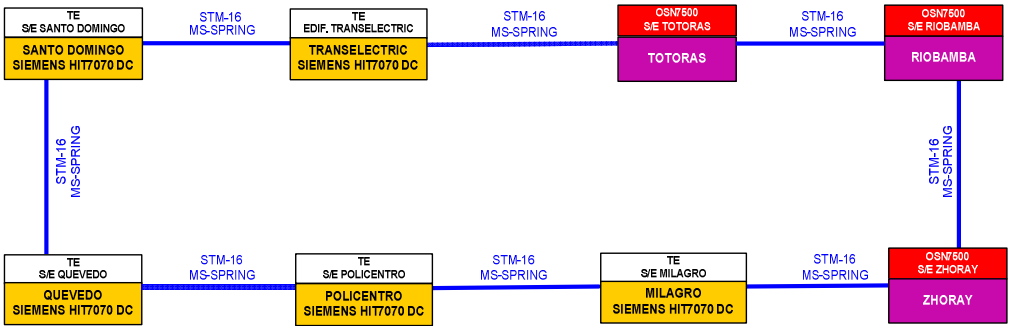

Figura 4.21 Anillo a nivel STM-16 Transelectric – Santo Domingo – Quevedo – Policentro – Milagro – Zhoray – Riobamba – Totoras con protección MS - SPRING

1.1.28 Sistema de Protección SNCP

En telecomunicaciones, la protección de la subred de conexión, o SNCP, es un tipo de mecanismo de protección asociados a las redes ópticas síncronas como jerarquía digital síncrona. SNCP is a dedicated (1+1) protection mechanism for SDH network spans which may be deployed in ring, point to point or mesh topologies.SNCP es un mecanismo dedicado de protección para tramos en una red SDH que puede ser configurado en anillo, punto a punto o topologías de malla.

SNCP is a 1+1 protection scheme (one working and one protection transport entity).Es un esquema de protección 1 +1 (una ruta principal y una ruta de protección de transporte).Input traffic is broadcast in two routes (one being the normal working route and the second one being the protection route). El tráfico de entrada se transmite en dos vías (una siendo la ruta principal y la segunda como ruta de protección).

La selección de la señal de mayor calidad se realiza, no únicamente por el elemento de red en el extremo del camino, sino que también en nodos intermedios a la salida de cada subred que es atravesada por la ruta.

La idea de tener una red protegida no solo a nivel de trayecto ha hecho que se escoja un esquema de protección por subred siendo éste Sub Network

Conection Protection (SNCP), el cual genera una alta disponibilidad para la conexión con relación al camino dedicado, ya que SNCP permite a la red sobreponerse a dos fallos simultáneos cosa que el camino de protección no permite y aun así, es requerido un complejo control que asegure realmente diversas rutas.

SNCP trabaja especialmente bien sobre anillos, porque se aseguran diversas rutas de enlaces.

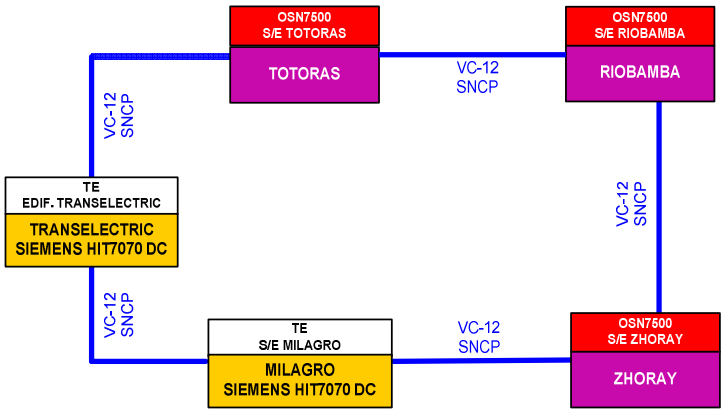

Figura 4.22 Anillo a nivel STM-16 Transelectric – Milagro - Zhoray – Riobamba – Totoras con protección en anillo SNCP

PRUEBAS DE INTEROPERABILIDAD ENTRE SISTEMAS DE GESTIÓN SIEMENS Y HUAWEI EN LA RED SDH

El interés de la Gerencia de Telecomunicaciones de CELEC EP – TRANSELECTRIC es el que se realice pruebas de interoperabilidad entre equipos multiplexores SIEMENS y HUAWEI por lo menos de uno de los siguientes esquemas de protección: 1 + 1 MSP, 1:N MSP, MS – SPRING, SNCP.

Las dos pruebas de los esquemas de protección 1+1 MSP y 1:N MSP fueron realizadas con trafico real a nivel STM-16, sin afectación alguna. Se realizaron pruebas del esquema de protección SNCP con un VC – 4 Server Trail, pero simulando un canal de capacidad VC-12, o que es los mismo, 1 E1. Dicha prueba de protección de servicio fue exitosa.

Para complementar el estudio se añadió la prueba de protección en anillo a nivel STM-16 con el sistema de protección MS-SPRING en los equipos multiplexores HUAWEI, y con esto culminar las pruebas a nivel de protección en anillo y protección de línea.

1.1.29 Sistema de Protección 1:N MSP

La Figura 4.10 muestra el diagrama empleado para las pruebas de protección realizadas con el esquema 1:N MSP, en la cual se comprobó la interoperabilidad entre equipos multiplexores SIEMENS y HUAWEI cuyos resultados fueron satisfactorios.

Los nodos que se utilizaron para las pruebas de interoperabilidad de la protección 1:N MSP fueron Zhoray con multiplexores HUAWEI (OSN 7500) y Milagro con multiplexores SIEMENS (HiT7070).

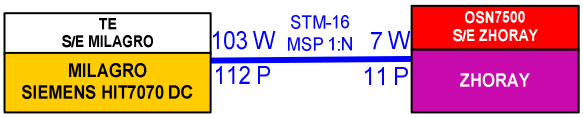

Figura 4.23 Puntos de prueba para sistema de protección 1:N MSP

Sistema de Gestión HUAWEI, multiplexor OSN 7500:

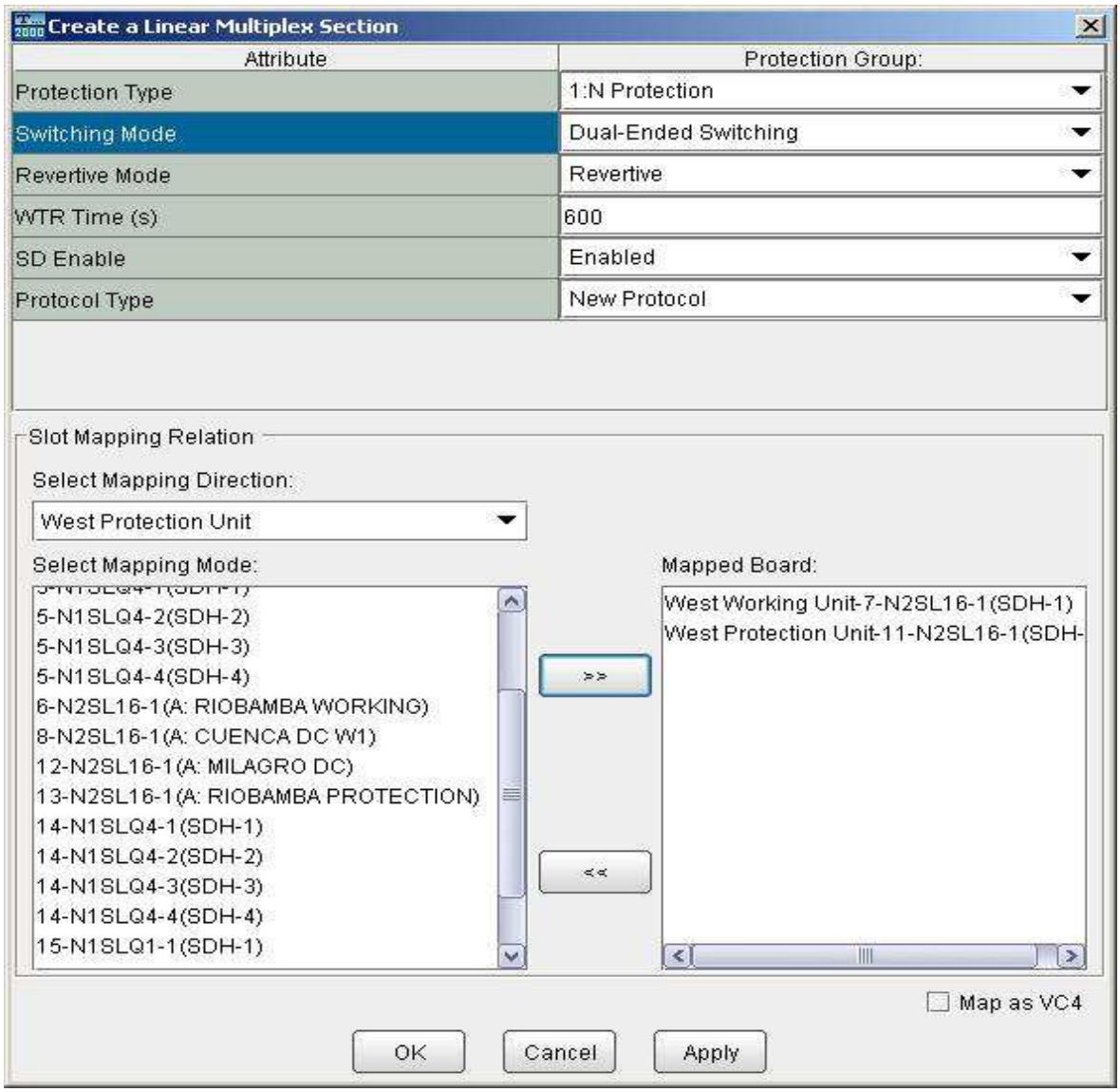

Figura 4.24 Creación de la protección 1:N MSP en el multiplexor HUAWEI del nodo Zhoray (OSN 7500)

La protección creada es 1:N MSP en la Subestación Zhoray donde se tiene un multiplexor HUAWEI OSN 7500, en donde está activo el modo reversible y el tiempo de verificación del estado del enlace es de 600 s. Las tarjetas utilizadas están ubicadas en los slots 7 como principal y 11 como protección, el cual se indica en la Figura 4.11.

Sistema de Gestión SIEMENS, multiplexor HiT7070:

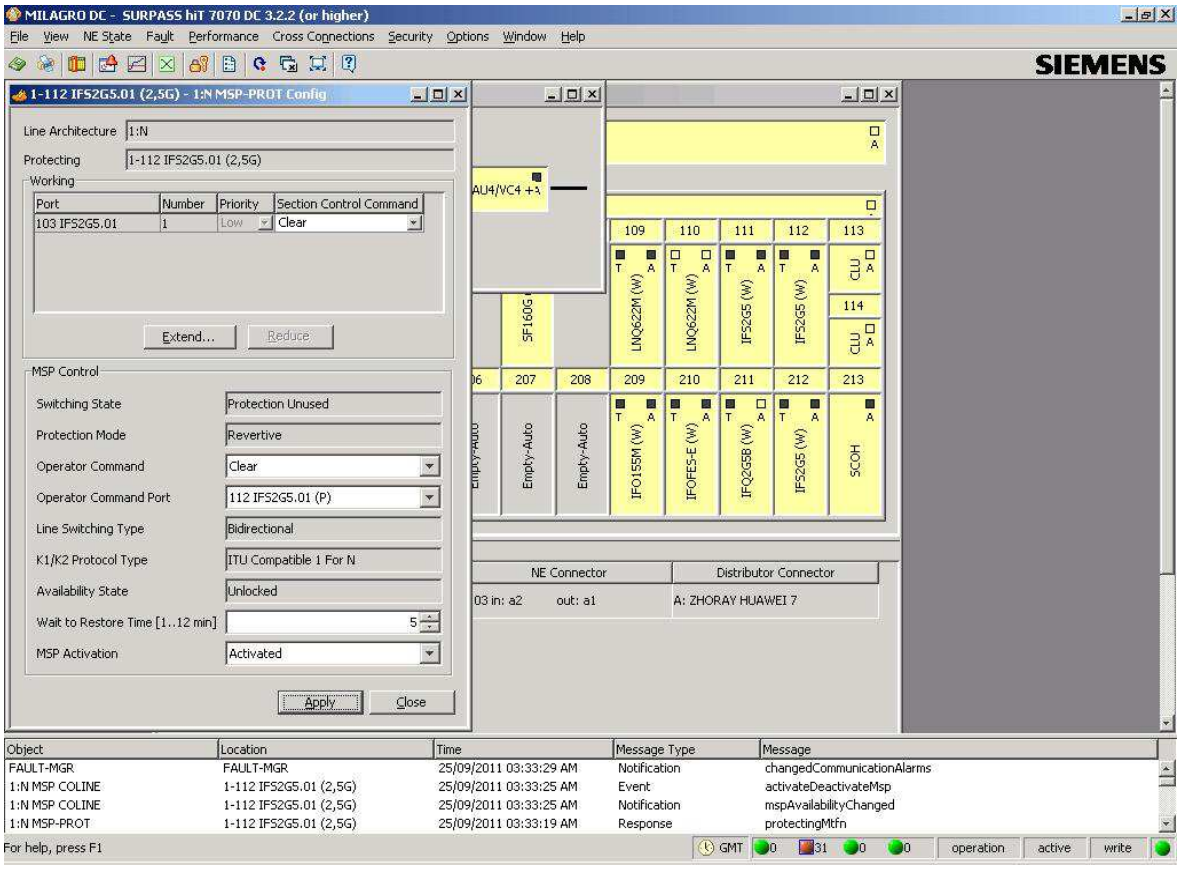

Figura 4.25 Creación de la protección 1:N MSP en el multiplexor SIEMENS del nodo Milagro (HiT7070)

La configuración del sistema de protección utilizado como se puede observar en la Figura 4.12 es 1:N MSP en donde la tarjeta 112 puerto 1 es la protección y la tarjeta 103 puerto 1 es el camino principal, configurado en modo de protección reversible, el cual indica que al momento de concluida la falla el enlace conmutará nuevamente a su línea de camino principal.

Se comprueba antes de realizar las pruebas, que el *MSP Activation* esté en estado “Activated”, que indica que la protección ha sido aceptada y está habilitada para ser utilizada en cualquier momento.

Con esto se demuestra que la protección MSP 1:N ha sido aceptada por ambas marcas de multiplexores dando lugar a que la interoperabilidad se compruebe mediante las siguientes pruebas:

Sistema de Gestión HUAWEI, multiplexor OSN 7500:

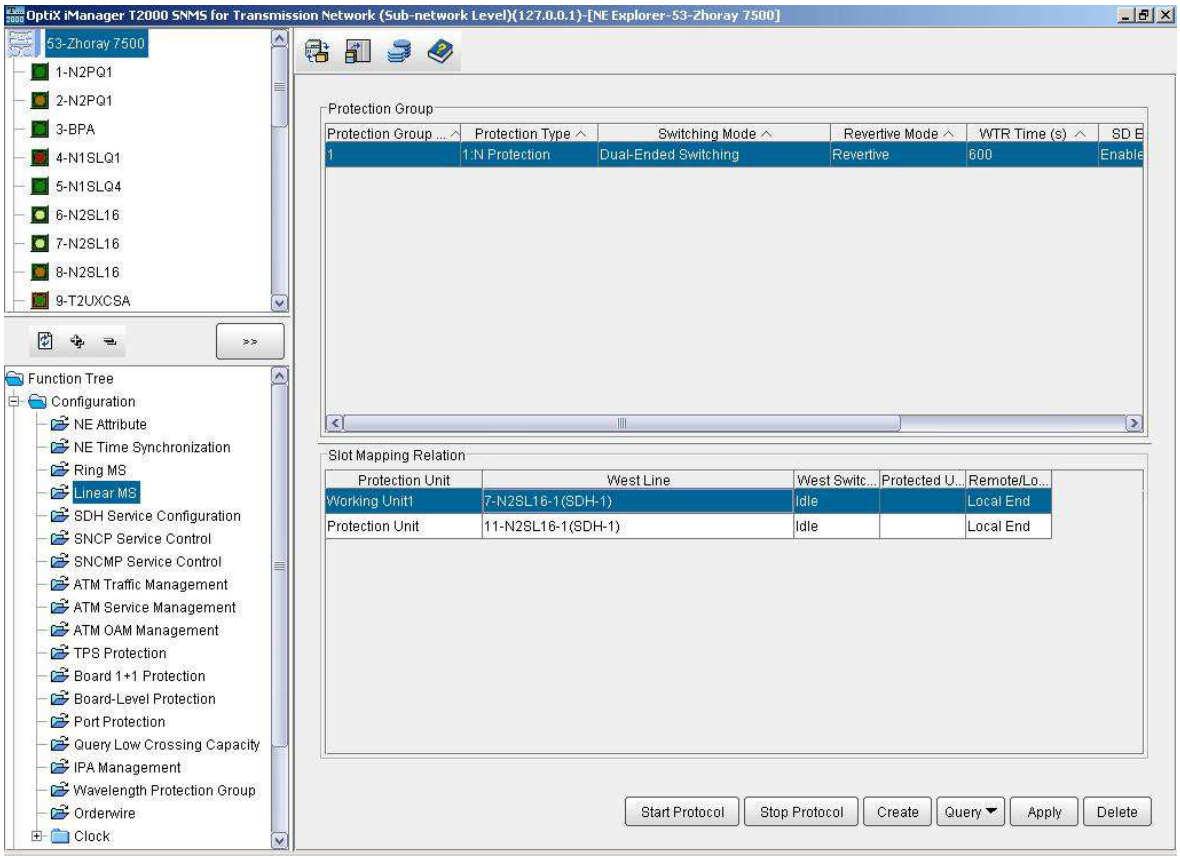

Figura 4.26 Subestación Zhoray sistema de protección 1:N MSP

Para la protección 1:N MSP a nivel de línea se utilizó la tarjeta N2SL16 slot 11 y como principal a la tarjeta N2SL16 slot 7.

El tipo de protección es 1:N MSP, el modo de conmutación es “Dual-Ended Switching” lo que significa que en cualquiera de los dos puntos, tanto en la subestación Zhoray como en la subestación Milagro puede conmutar a la protección o retornar al camino principal debido a que está activo el modo Reversible, lo que permite que la protección se normalice al trayecto principal cuando este esté en servicio nuevamente después de 600 segundos del Wait To Restore, que es el tiempo de verificación de inestabilidad en el enlace.

Tanto el trayecto principal como su protección esta en modo de espera habilitado, lo que implica que los dos caminos están como enlaces levantados y

que la protección está lista para ser utilizada en cualquier momento que se presente una falla.

La Figura 4.14 muestra el resultado de apagar el láser de la tarjeta IFS2G5 en el slot 103 del equipo multiplexor SIEMENS HiT7070 en la Subestación Milagro. Por lo tanto, la tarjeta N2SL16 del slot 7 del multiplexor HUAWEI, que se encontraba como principal, se alarmó con LOS[22] dando lugar a que el status de conmutación nos arroje un mensaje de alerta en el camino principal (Switch upon signal failure) que significa que existirá una conmutación al camino de protección.

Para el caso de una falla en el camino principal la conmutación al camino de protección es inmediata. Se realizaron pruebas con un servicio activo cuya capacidad de tráfico es de 300 Mbps. Respecto al tiempo de indisponibilidad que la falla podría ocasionar, se tomaron algunas precauciones como control de ping extendido al cliente, permitiendo verificar en las pruebas que no se registraron pérdidas de tráfico, ya que la conmutación al camino de protección fue casi imperceptible.

[22] Loss Of Signal

Sistema de Gestión HUAWEI, multiplexor OSN 7500:

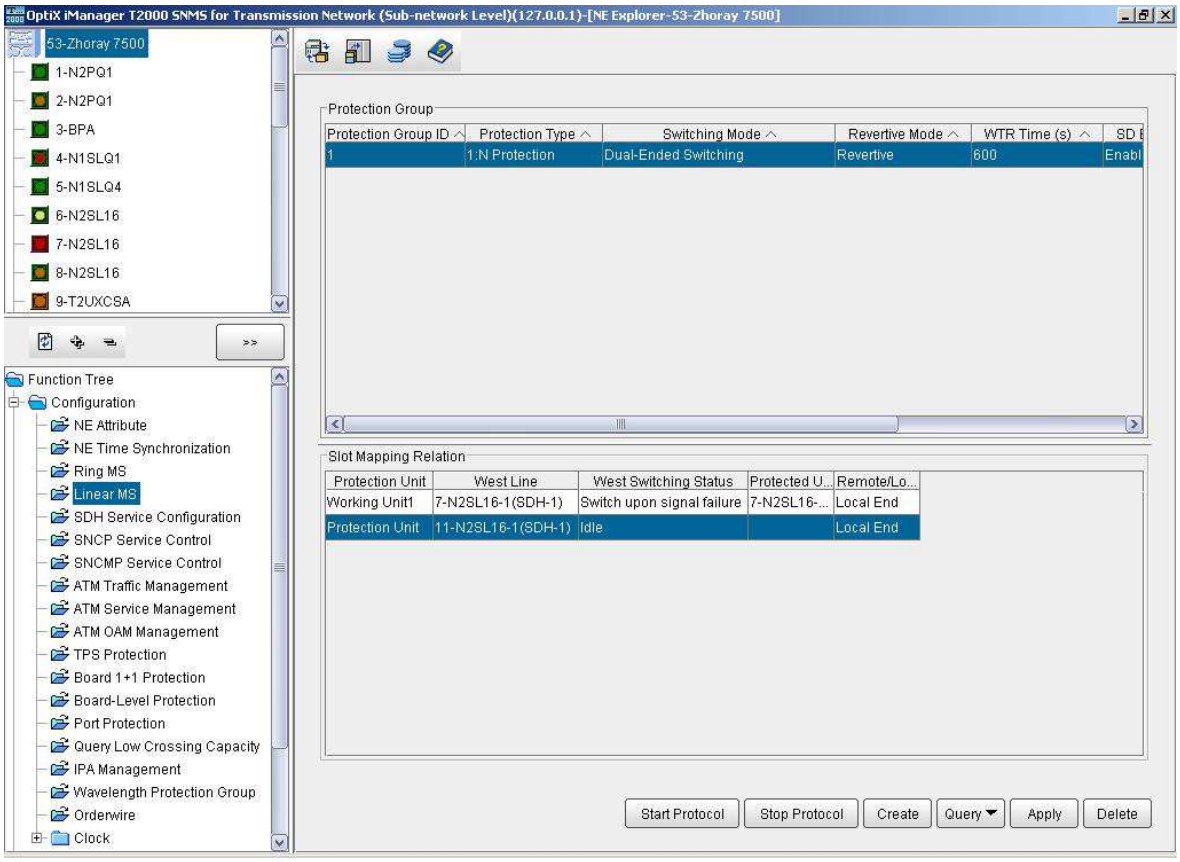

Figura 4.27 Conmutación a la protección en la Subestación Zhoray (HUAWEI OSN 7500)

Como se puede observar en la Figura 4.14, la tarjeta N2SL16 del slot 7 está en color rojo, lo que significa que la misma esta fuera de servicio y alarmada con LOS, esto se debe a que al ser forzado el láser de la tarjeta de Milagro a apagarse no se establezca un enlace óptico con la tarjeta principal de Zhoray.

Sistema de Gestión HUAWEI, multiplexor OSN 7500:

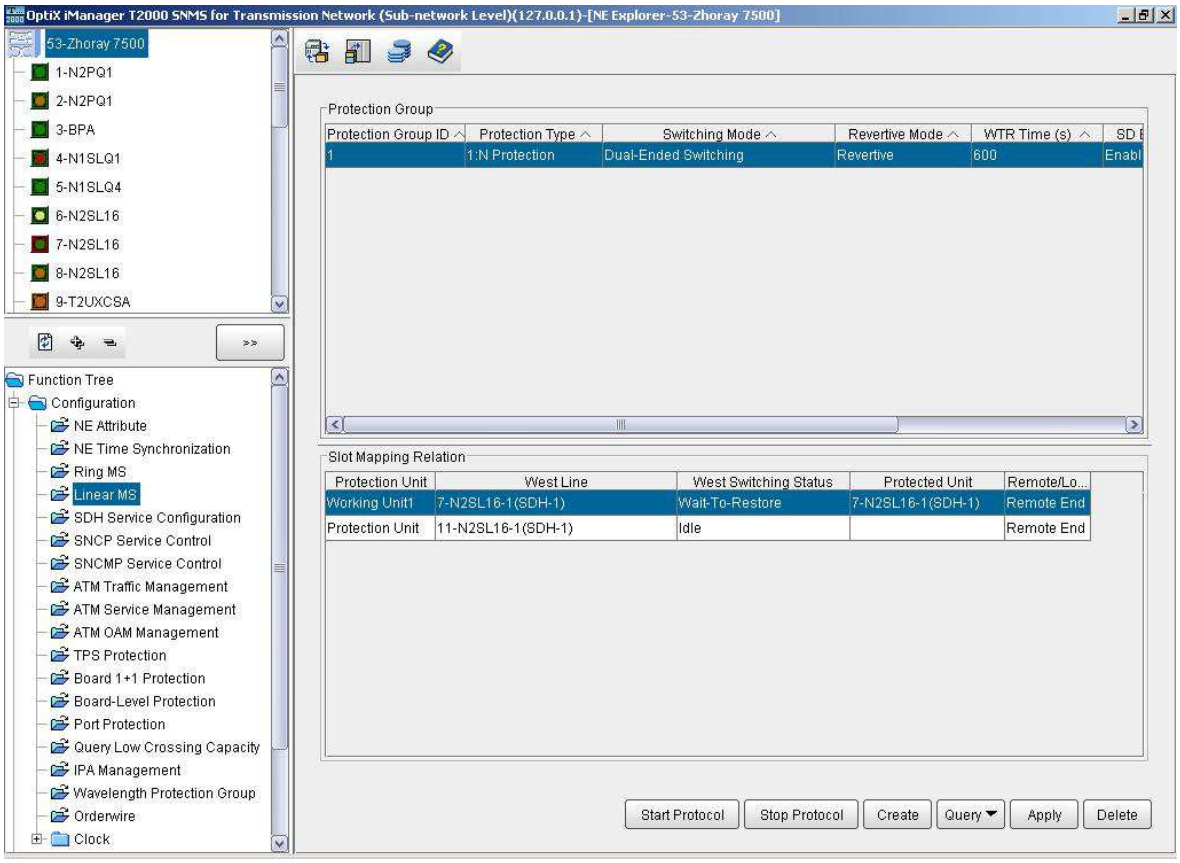

Figura 4.28 Restauración al camino Principal

El tiempo de verificación para que el tráfico conmute nuevamente al camino principal tiene que ser de 600 s, por lo que en este tiempo, como se puede observar en la Figura 4.15, el camino principal, se encuentra con el mensaje *Wait-To-Restore*, dando lugar a que se verifique el estado correcto de la conmutación del servicio al camino principal y posteriormente a la conmutación completa del servicio y flujo normal de tráfico sin perdidas ni tiempo de indisponibilidad.

En las Figuras 4.16 a 4.18 se mostrará un procedimiento similar de conmutación de la protección, que para este caso se forzará la desactivación del láser de la tarjeta N2SL16, en el equipo multiplexor HUAWEI OSN 7500.

Sistema de Gestión SIEMENS, multiplexor HiT7070:

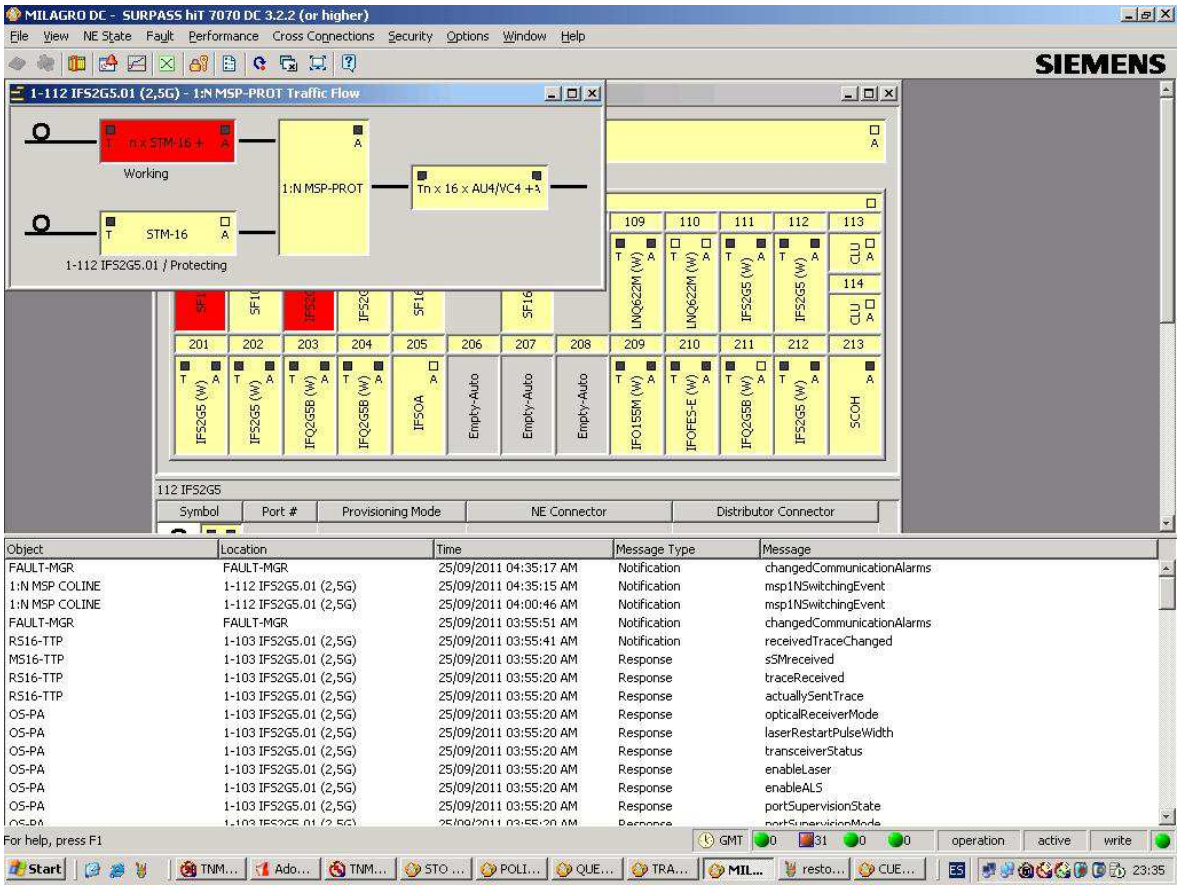

Figura 4.29 Proceso de conmutación del camino Principal al camino de protección en equipo multiplexor SIEMENS

Como se observa en la Figura 4.16, al forzar la desactivación del láser de la tarjeta N2SL16 del equipo multiplexor HUAWEI, indica una notificación en el equipo SIEMENS, en la tarjeta 103 puerto 1, que existe una falla en la comunicación del enlace principal entre Milagro y Zhoray, conmutando inmediatamente a la tarjeta 112 puerto 1 del equipo multiplexor SIEMEN, de esta forma el tráfico opera en el enlace de protección.

El proceso de restablecimiento del enlace de línea se realiza al activar nuevamente el láser óptico en Zhoray, en el multiplexor HUAWEI, slot 7. Cuando la falla se ha superado y el temporizador del Wait-to-Restore (WTR) ha expirado, el enlace óptico debe retomar su camino principal.

A continuación se muestra como se da este proceso en los multiplexores SIEMENS.

Sistema de Gestión SIEMENS, multiplexor HiT7070:

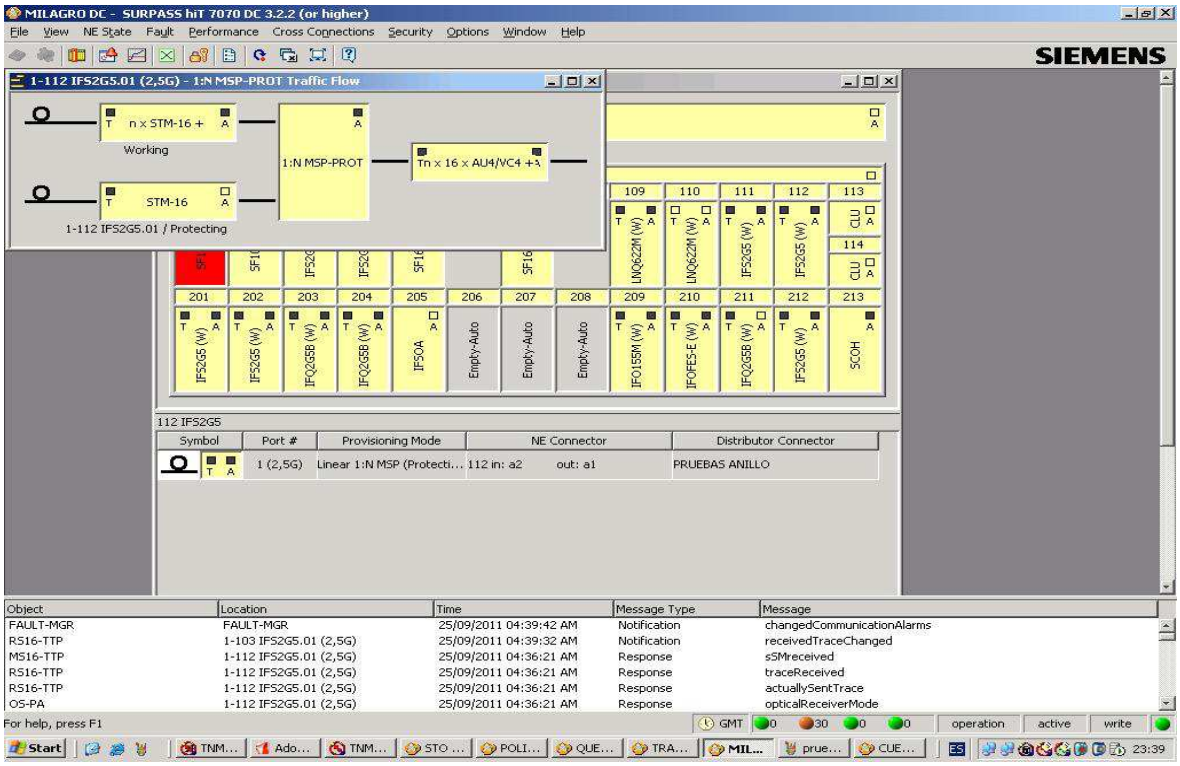

Figura 4.30 Restauración de la señal óptica en relación al camino de Protección, tarjeta 112 puerto 1 multiplexor SIEMENS

En la Figura 4.17, nos muestra como la conmutación del enlace de línea de la señal óptica del camino de protección al camino principal fue exitosa. No se presentaron alarmas ni tiempo de indisponibilidad que pudiera afectar al tráfico por este enlace óptico.

Sistema de Gestión SIEMENS, multiplexor HiT7070:

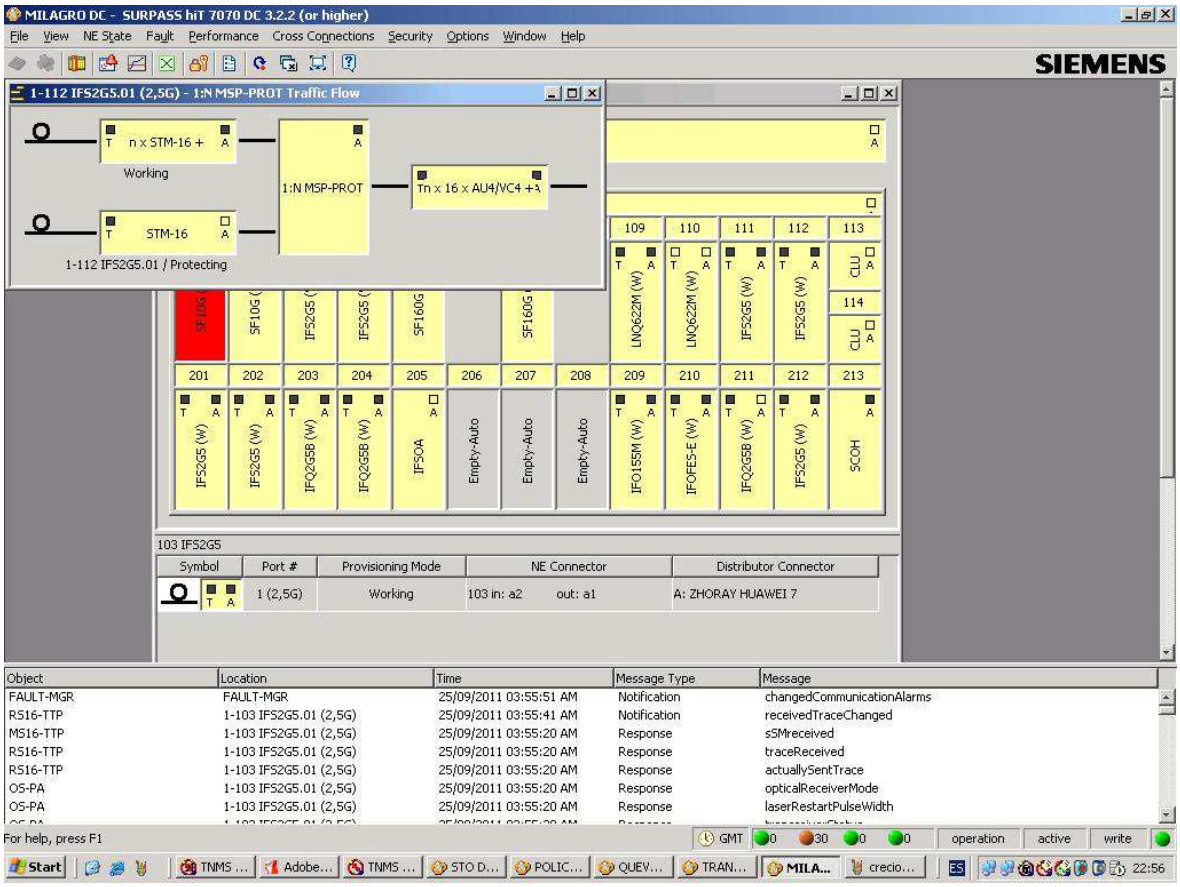

Figura 4.31 Restauración de la señal óptica con relación al camino Principal, tarjeta 103 puerto 1 multiplexor SIEMENS

Con esto queda probada la interoperabilidad del sistema de protección 1:N MSP entre equipos multiplexores SIEMENS y HUAWEI, sin caída ni perdida de paquetes o tiempo de indisponibilidad en el enlace óptico de prueba en el tramo Milagro (SIEMENS HiT7070) y Zhoray (HUAWEI OSN 7500).

1.1.30 Esquema de Protección MS-SPRING

Las pruebas para el sistema de protección MS-SPRING fueron realizadas en el multiplexor HUAWEI en la ruta comprendida entre Totoras (OSN 7500), Riobamba (OSN 7500) y Zhoray (OSN 7500); a dichos nodos se les tomo como tramos de prueba para la creación de un anillo a nivel STM-16 para probar el sistema de protección en anillo compartido MSP.

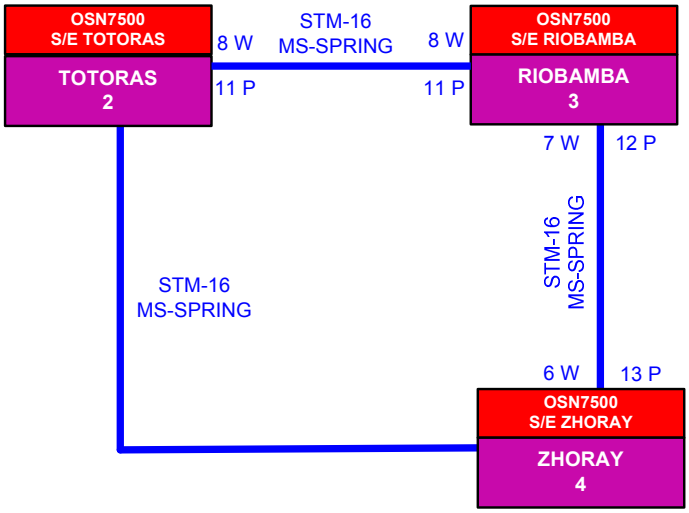

Figura 4.32 Topología en anillo para pruebas MS-SPRING

La topología en anillo fue probada en este tramo para la implementación futura del mismo a nivel STM-16. Con esto se trata de aprovechar las características del Test Ring que posee esta marca de multiplexor.

Cada punto de enlace óptico tiene un ID, los cuales son escogidos por el administrador de la gestión; para este caso de estudio se utilizó los siguientes:

Totoras ID: 2
Riobamba ID: 3
Zhoray ID: 4

Los ID`s se los utiliza para identificar el Local Node, East Node y West Node. El Local Node es el ID de cada punto donde se encuentra un multiplexor, que para este caso sería cada subestación, el West Node y el East Node son los ID`s de los puntos vecinos con relacional al Local Node.

Cada nodo en el anillo debe ser identificado mediante la asignación de un ID de nodo. El número máximo de nodos en el anillo es de 127. El ID de nodo debe ser independiente del orden en que aparecen los nodos en el anillo. El ID de nodo se utiliza para la identidad de los nodos de origen y destino de cada solicitud APS.

Cuando la conmutación de protección no está activa en el anillo, cada nodo debe enviar periódicamente peticiones de APS a los dos nodos adyacentes (Not Request). Cuando un nodo determina que la conmutación de protección se requiere, se deberá enviar una solicitud APS en ambas direcciones.

Bits 4-1 (MSB - LSB)	Condition, State or external Request	Priority
1 1 1 1	Lockout of Protection (LP)	highest
1 1 0 1	Forced Switch (FS)	
1 0 1 1	Signal Fail (SF)	
0 1 1 0	Manual Switch (MS)	
0 1 0 1	Wait-To-Restore (WTR)	
0 0 1 1	Exerciser (EXER)	
0 0 0 1	Reverse Request (RR)	
0 0 0 0	No Request (NR)	lowest

Tabla 4.1 Solicitud de Código APS

Las pruebas que se realizaron fueron satisfactorias y se las detalla a continuación:

Creación del Sistema de Protección anillado MS-SPRING:

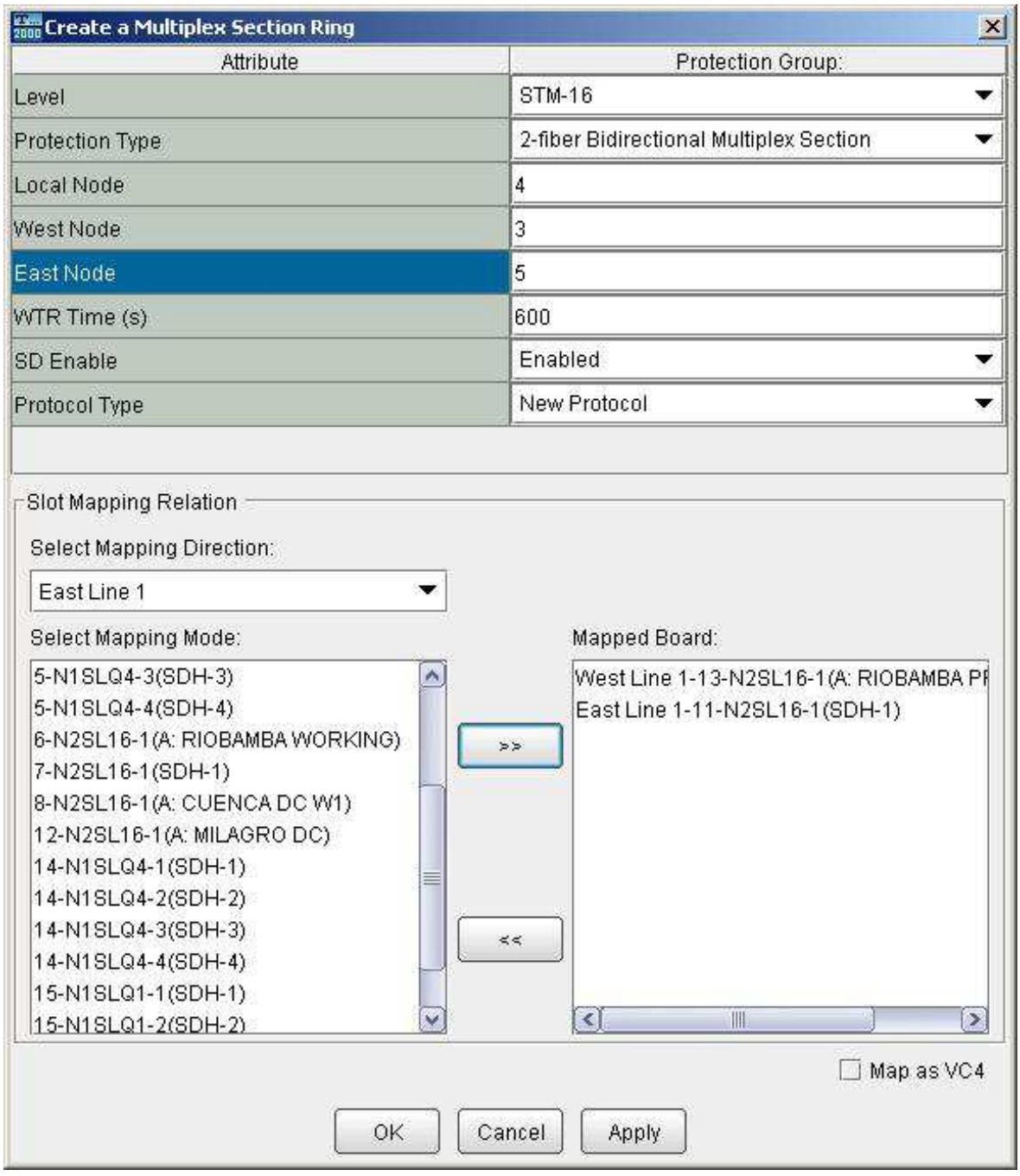

Figura 4.33 Configuración de Sistema de Protección en anillo MSP con 2 fibras

La capacidad escogida para la creación del anillo Multiplex Section Ring fue a nivel STM-16 en donde el tipo de protección creado es a 2-fibras bidireccional dando lugar con esto a que la conmutación sea hacia ambos lados, WEST o EAST. Todo esto dependiendo de la dirección que tiene el tráfico como enlace principal.

Subestación Totoras, multiplexor HUAWEI OSN 7500:

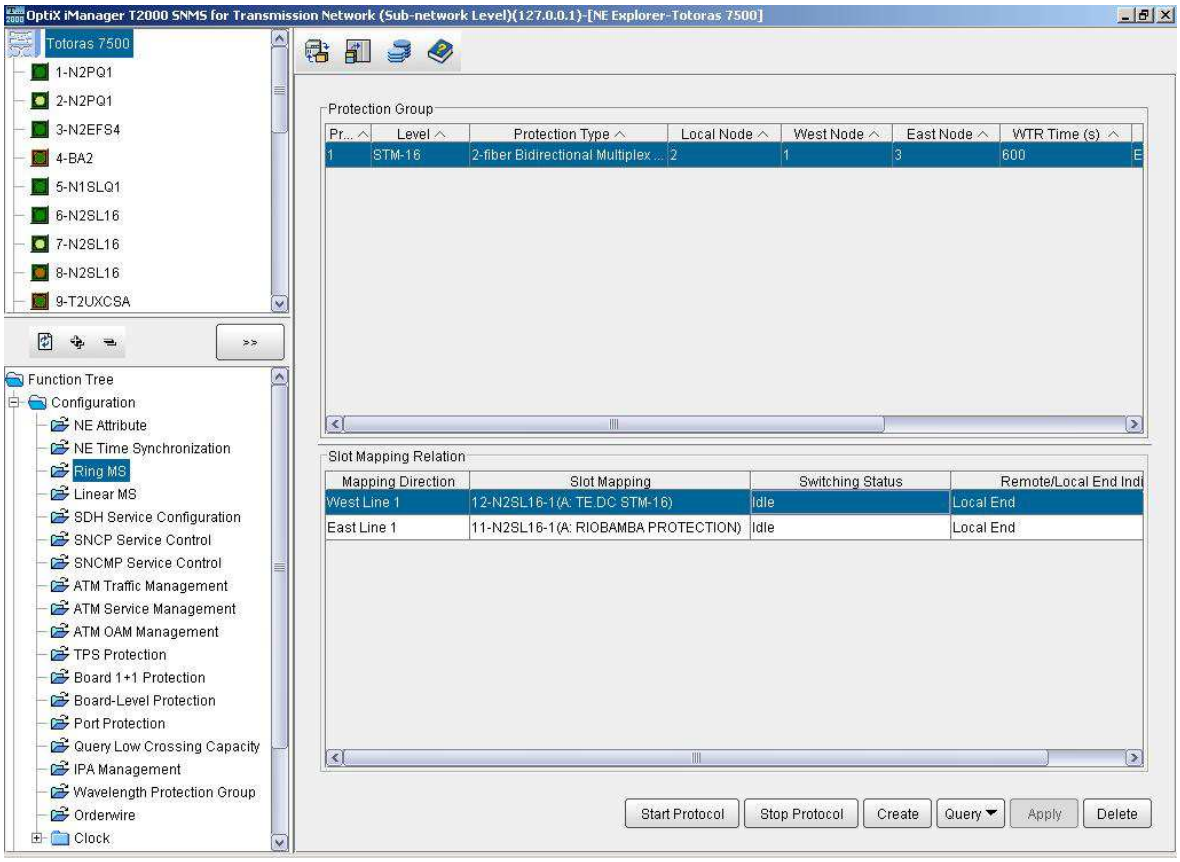

Figura 4.34 Creación de la protección MS-SPRING con 2 fibras

La prueba para el sistema de protección MS-SPRING se las realizó con la herramienta de análisis EXERCISE RING que posee el Sistema de Gestión T2000 de HUAWEI.

El código binario de solicitud de código APS para Exercise Ring es 0011 como se muestra en la Tabla 4.1.

En cada uno de los nodos del anillo se realizaron configuraciones similares.

Subestación Riobamba, multiplexor HUAWEI OSN 7500:

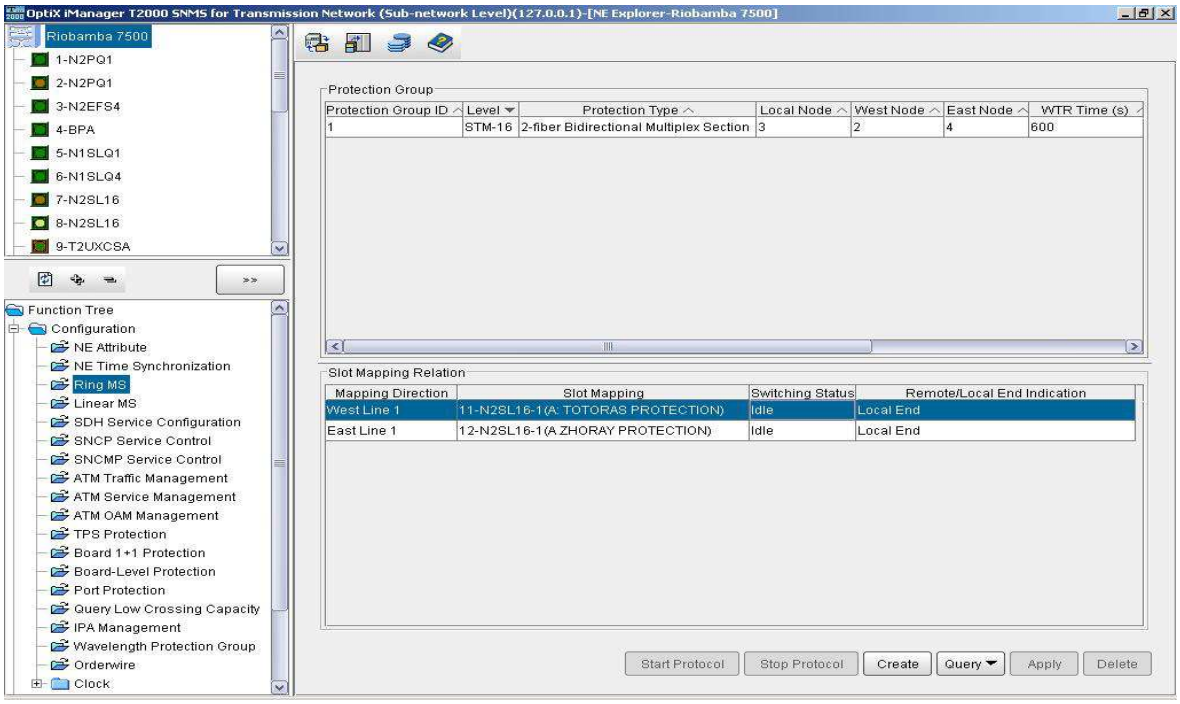

Figura 4.35 Creación de la protección MS-SPRING con 2 fibras.

Subestación Zhoray, multiplexor HUAWEI OSN 7500:

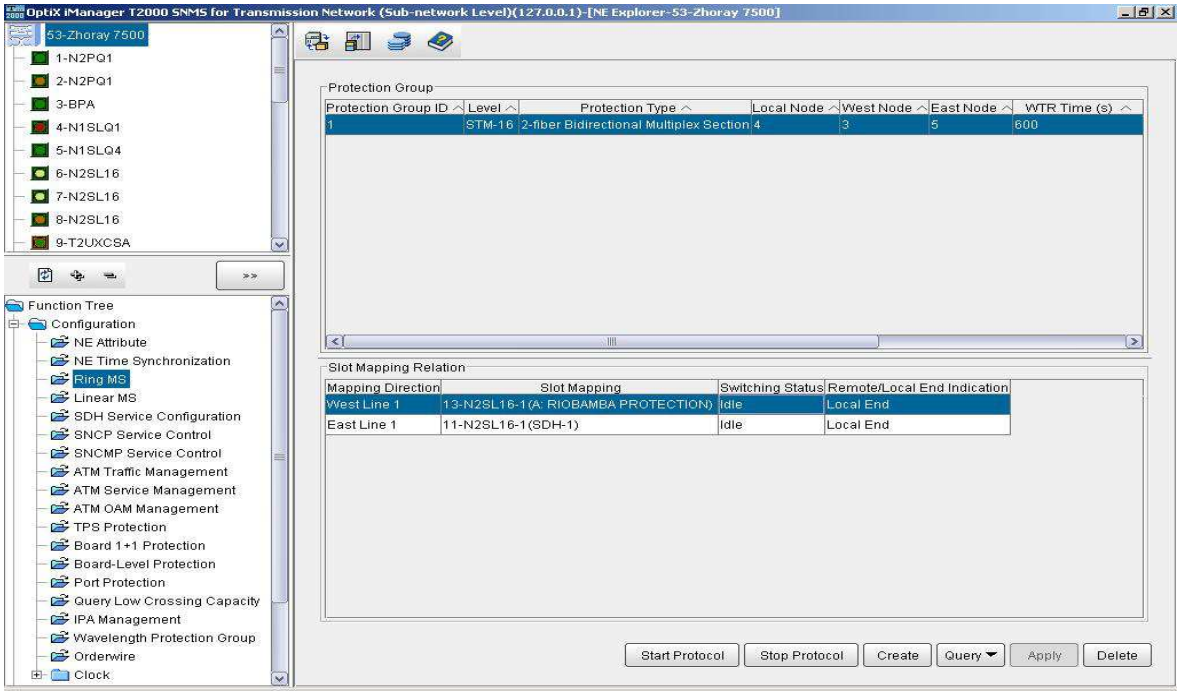

Figura 4.36 Creación de la protección MS-SPRING con 2 fibras.

En necesario tener un orden adecuado con respecto a los Nodos: Local, Este y Oeste, ya que esto determinará la correcta conmutación con respecto al lugar de origen de la falla.

Para las pruebas realizadas en el anillo se utilizó la herramienta EXERCISE RING en el Sistema de Gestión T2000, donde se las efectuó en tiempo real y simulando una capacidad STM-16.

Las pruebas en las 3 subestaciones fueron las siguientes:

Subestación Totoras:

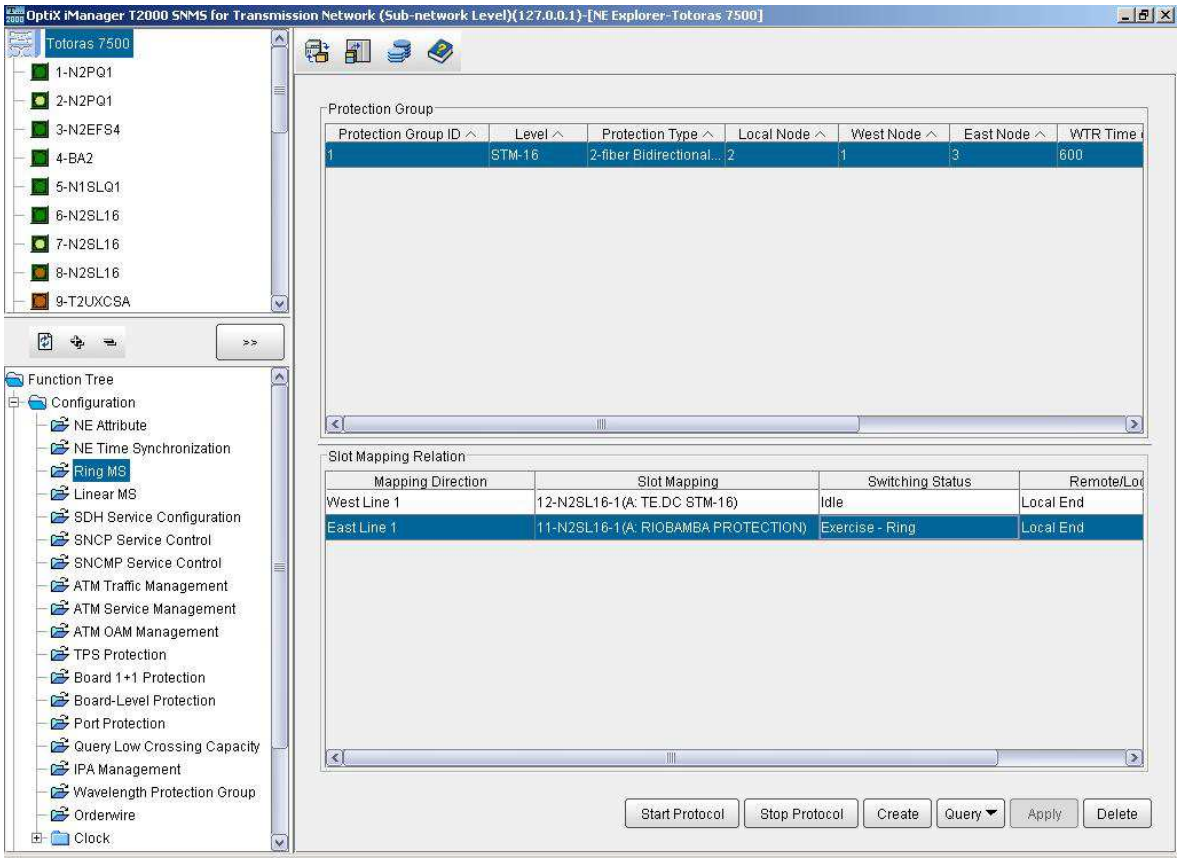

Figura 4.37 Pruebas de sistema de protección MS-SPRING en la Subestación Totoras utilizando la herramienta de prueba Exercise Ring.

Las pruebas realizadas en el Sistema de Gestión T2000 de HUAWEI mediante Exercise Ring, se desarrollaron de tal manera que se simulo un canal real con tráfico existente a nivel STM-16. Las fallas generadas para la

conmutación del tráfico en el anillo MSP son creadas en el *Local End,*[23] esto se puede comprobar en el Status de Conmutación, donde en el trayecto escogido para esta prueba es el East Line en la tarjeta N2SL16 slot 11, en donde se muestra la palabra *Exercise Ring*, que indica que el trayecto está con fallas o perdida de señal óptica y por ese motivo conmutara al siguiente salto, que para este caso sería la S/E Riobamba, teniendo como resultado la conmutación del tráfico hacia la WEST LINE slot 11 tarjeta N2SL16.

Esto de detalla a continuación en la Figura 4.25:

Subestación Riobamba:

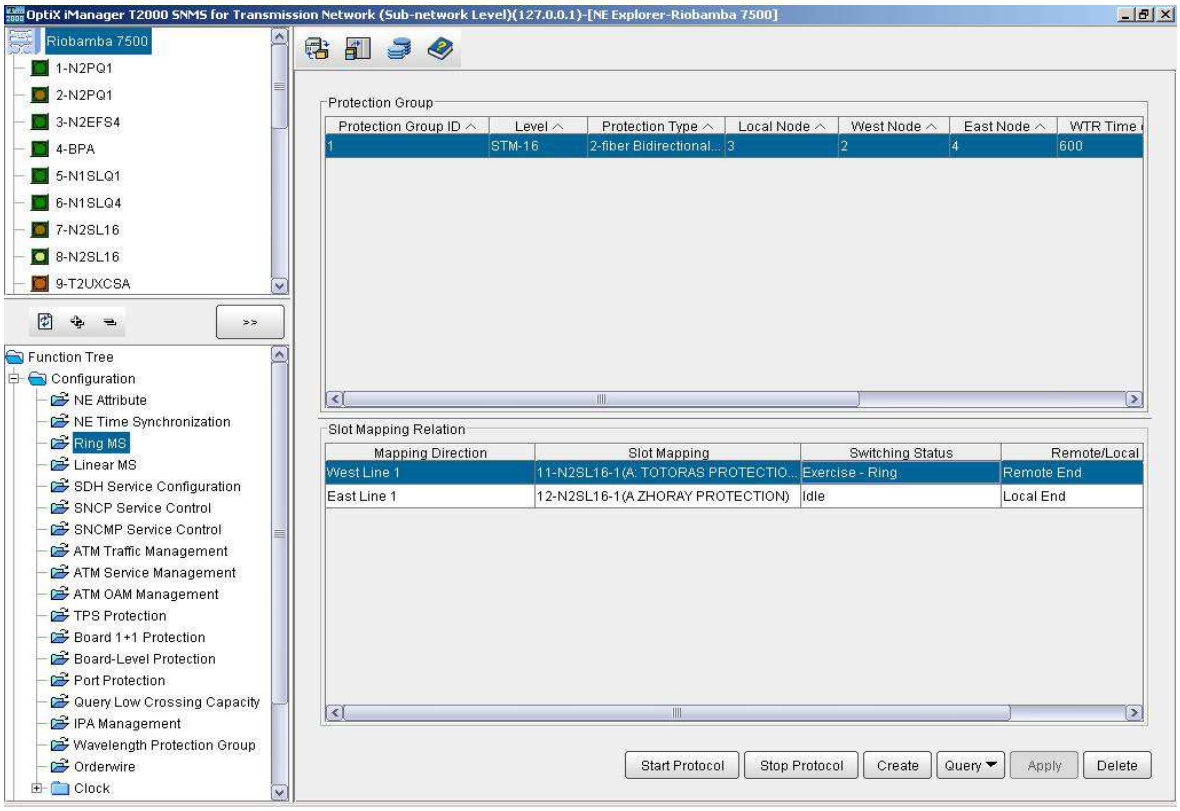

Figura 4.38 Conmutación de tráfico al WEST LINE proveniente de la S/E Totoras.

La conmutación de tráfico al West Line es realizada con éxito, dando lugar a que el mismo continúe su trayecto hacia el siguiente salto sin complicación.

[23] Nodo Local, cuando se genera una falla implica que existe perdidas en el nodo presente.

Para la siguiente prueba se realizó similares configuraciones en el tramo Riobamba – Zhoray, con fallo de señal óptica en la Subestación Riobamba.

Subestación Riobamba:

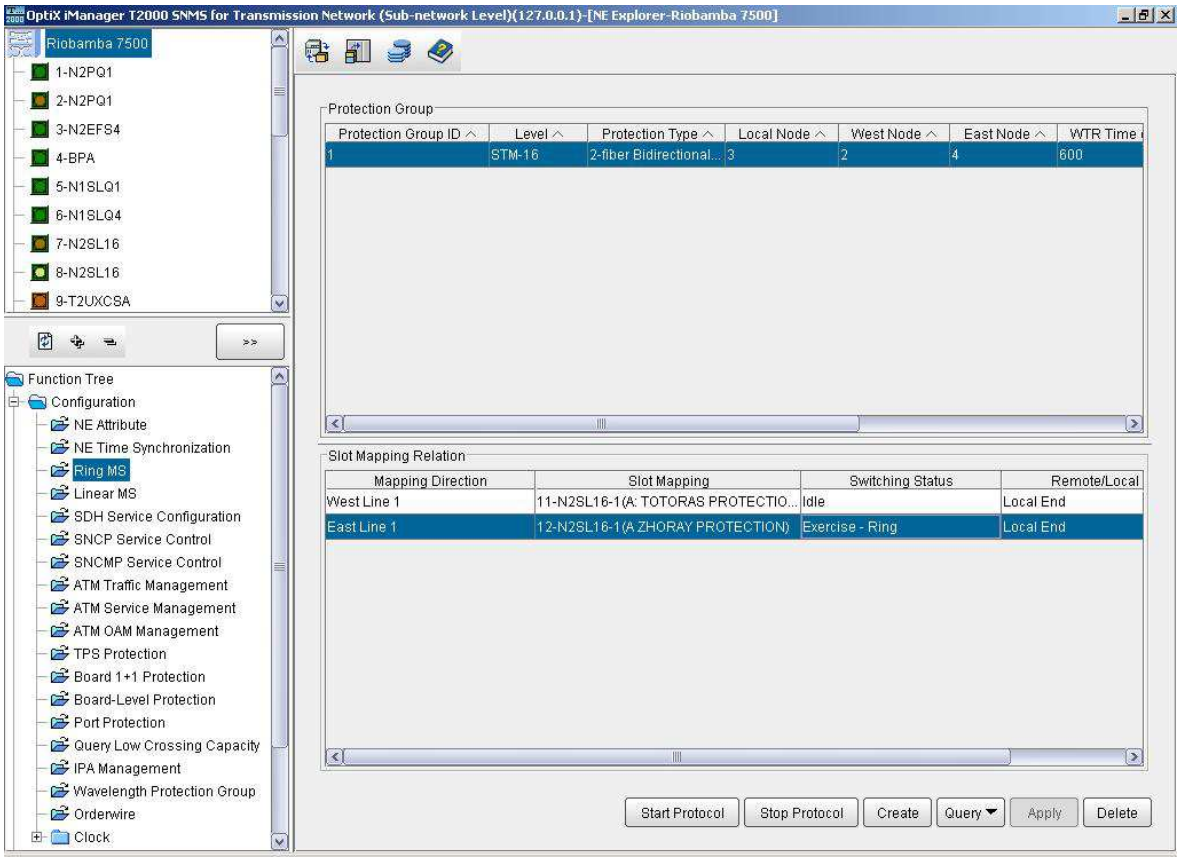

Figura 4.39 Prueba dos de sistema de protección MS-SPRING utilizando herramienta de prueba Exercise Ring

La prueba se efectuó simulando un canal real a nivel STM-16 dando lugar a que la falla o pérdida de señal óptica se de en la East Line de la tarjeta N2SL16 slot 12, en el tramo hacia la protección de Zhoray.

Para el siguiente salto, que para este caso es el nodo ubicado en la Subestación Zhoray, se mostrará en el *Status de Conmutación* un *Remote End* en la West Line de la tarjeta N2SL16 slot 13, lo que indica que el tráfico conmutó a dicha línea y que el mismo proviene del nodo anterior donde existió una falla. Esto se muestra a continuación en la siguiente Figura:

Subestación Zhoray:

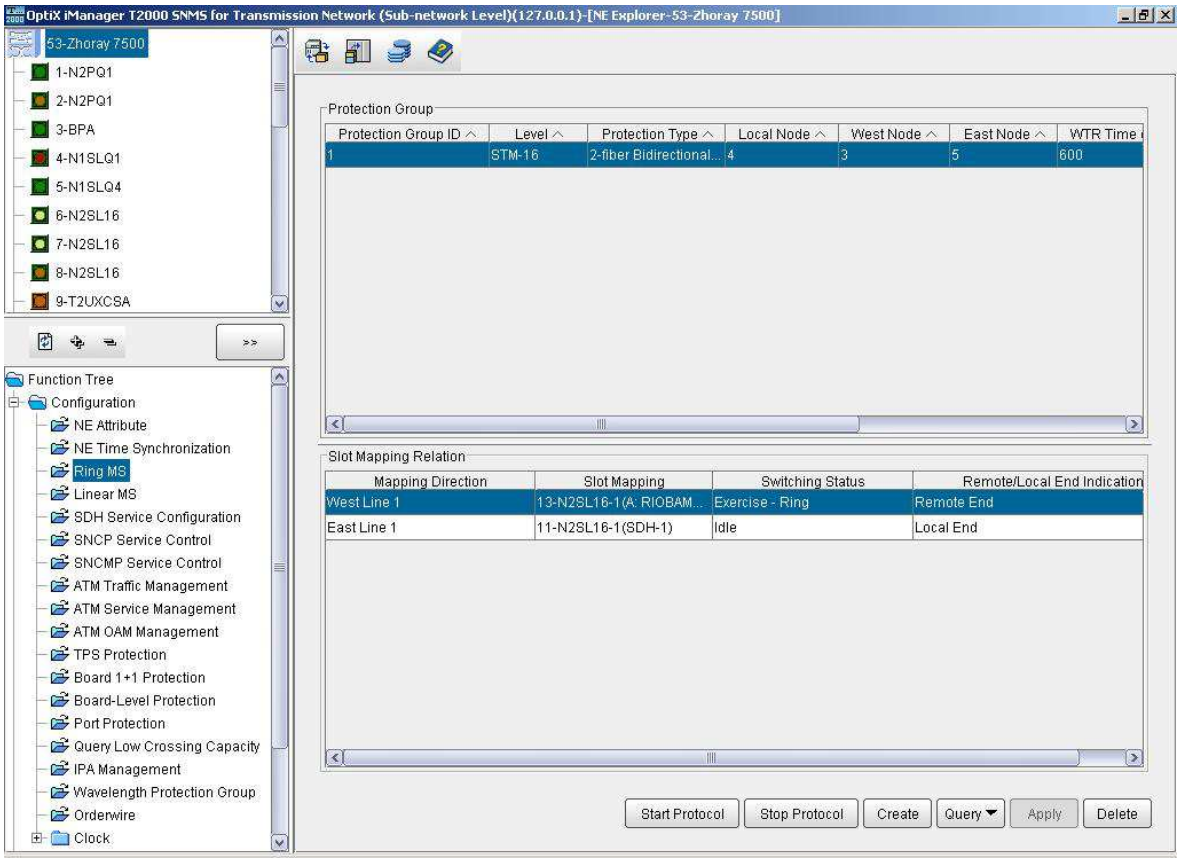

Figura 4.40 Conmutación de tráfico al WEST LINE proveniente de la S/E Riobamba.

Como se observa en la Figura 4.27, el *Status de Conmutación* de la tarjeta N2SL16 slot 13 está en *Exercise Ring* en el *Remote End*, lo que indica que el tráfico conmuto y es proveniente de la falla o perdida óptica en el nodo anterior es decir de la Subestación Riobamba.

Con esto se deja por sentado que las pruebas en anillo Multiplex Section Shared Protection Ring (MS-SPRING) fueron exitosas. El tiempo de indisponibilidad fue mínimo sin afectación de tráfico.

1.1.31 Sistema de Protección Subnetwork Connection Protection SNCP

La topología utilizada para probar el Sistema de Protección SNCP fue en anillos a nivel VC-12. El trayecto escogido para esta prueba comprende los nodos de Transelectric (Siemens HiT7070 DC), Milagro (Siemens HiT7070 DC),

Zhoray (Huawei OSN 7500), Riobamba (Huawei OSN 7500) y Totoras (Huawei OSN 7500) como se muestra en la siguiente Figura:

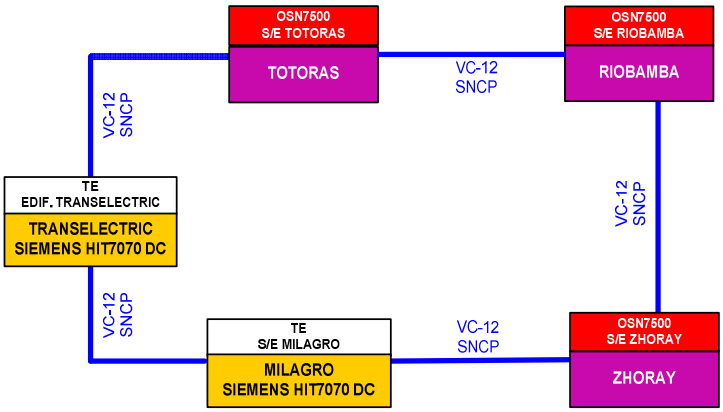

Figura 4.41 Topología en anillo para pruebas de Sistema de protección SNCP.

SNCP trabaja especialmente sobre anillos, porque se aseguran diversas rutas. El hecho de que trabaje sobre nodos intermedios hace que su eficacia sea también buena sobre redes malladas.

La configuración en anillo con Sistema de Protección SNCP se muestra en la Figura 4.29, en donde se detalla las rutas escogidas, tanto principal como de protección.

Sistema de Gestión HUAWEI, multiplexor OSN 7500:

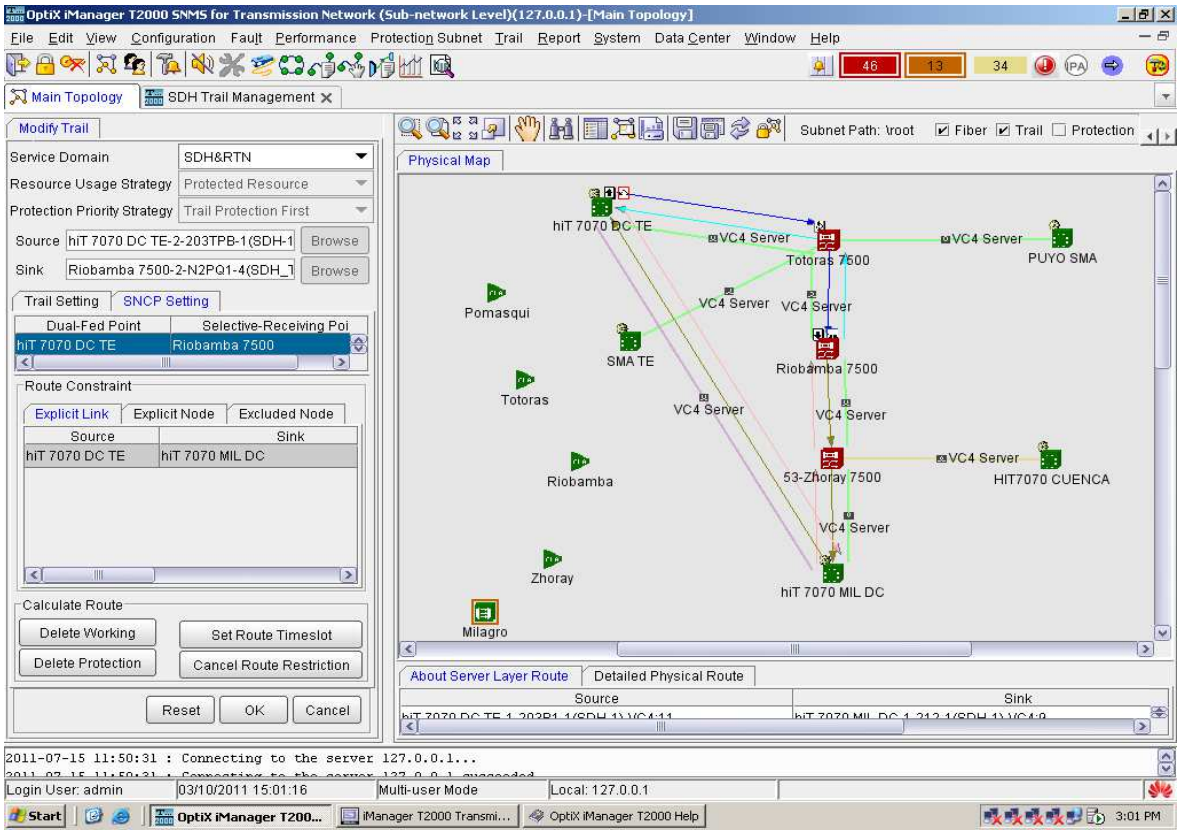

Figura 4.42 Configuración de Sistema de Protección SNCP a nivel de tributario VC-12

Las pruebas realizadas para este anillo con protección SNCP fueron realizadas en base a comprobar la interoperabilidad de las gestiones SIEMENS (HiT7070) y HUAWEI (OSN 7500) dando lugar a que las pruebas sean satisfactorias y que ambas gestiones acepten el Sistema de Protección como tal.

Se ubicó como nodo fuente al equipo Siemens HiT7070 DC del Edificio Transelectric y como nodo destino final al equipo Huawei OSN 7500 de la Subestación Riobamba.

El multiplexor ubicado en el Edificio Transelectric está configurado como nodo principal de conmutación ya que puede conmutar el tráfico hacia cualquiera de las dos direcciones, mientras que el multiplexor ubicado en la Subestación Riobamba está configurado como nodo de recepción, y la dirección del trafico proveniente va a depender de la calidad de la señal, ya que la selección de la señal de mejor calidad se realiza no únicamente por el elemento de red en el

extremo del camino, sino que también en nodos intermedios a la salida de cada subred que es atravesada por la ruta.

La descripción de todas las rutas esta descrita en la Figura 4.30:

Sistema de Gestión HUAWEI, multiplexor OSN 7500:

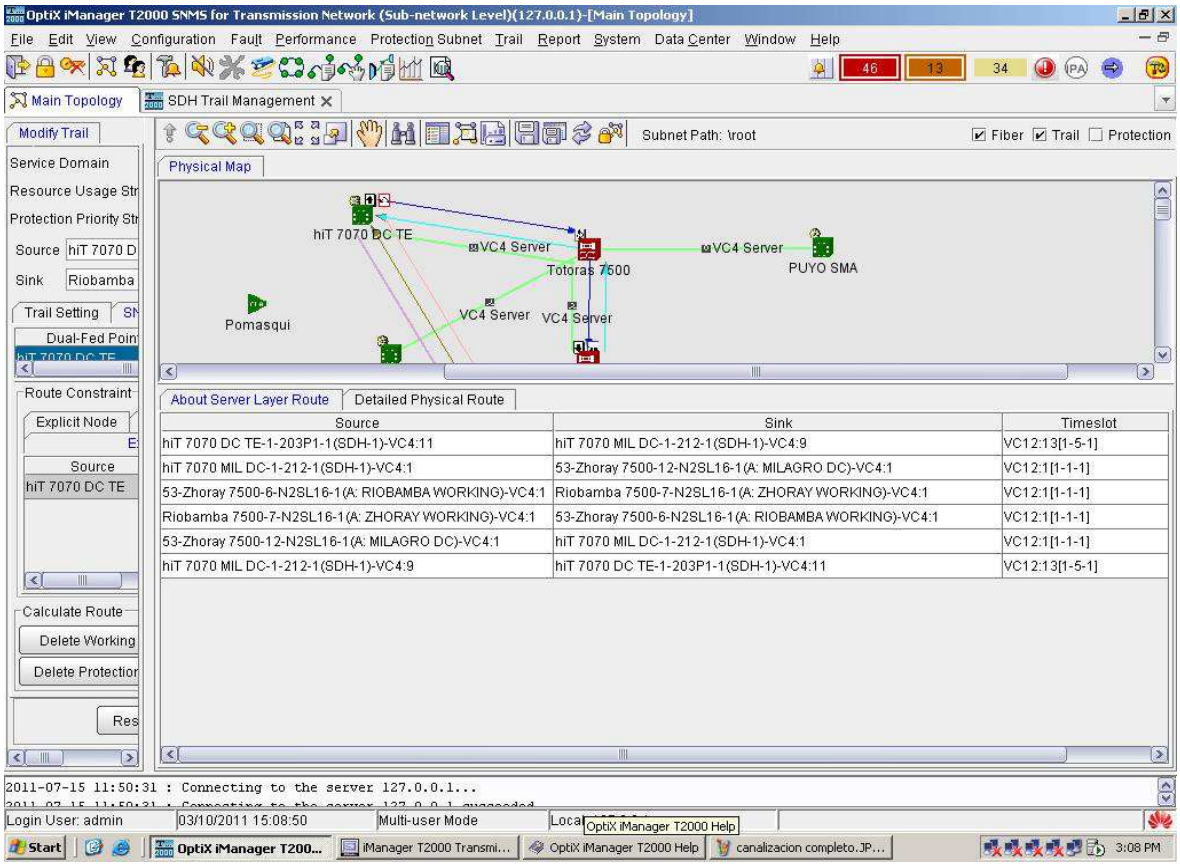

Figura 4.43 Descripción de todas las rutas en el anillo SNCP a nivel VC-12.

Como se puede observar en la Figura 4.30 la capacidad escogida para la prueba fue a nivel tributario, VC-12, ya que este tipo de protección se lo realiza a nivel de servicio mas no a nivel de capacidades de línea; esto involucra la protección de contenedores virtuales individuales a través de una ruta punto a punto. Si existe un evento de fallo, únicamente el contenedor virtual en cuestión es conmutado a una ruta alternativa.

El proceso de conmutación para este tipo de protección se lo puede realizar de dos maneras, Positive Protection o Negative Protection, teniendo el detalle de las rutas en la Figura 4.31.

Sistema de Gestión HUAWEI, multiplexor OSN 7500:

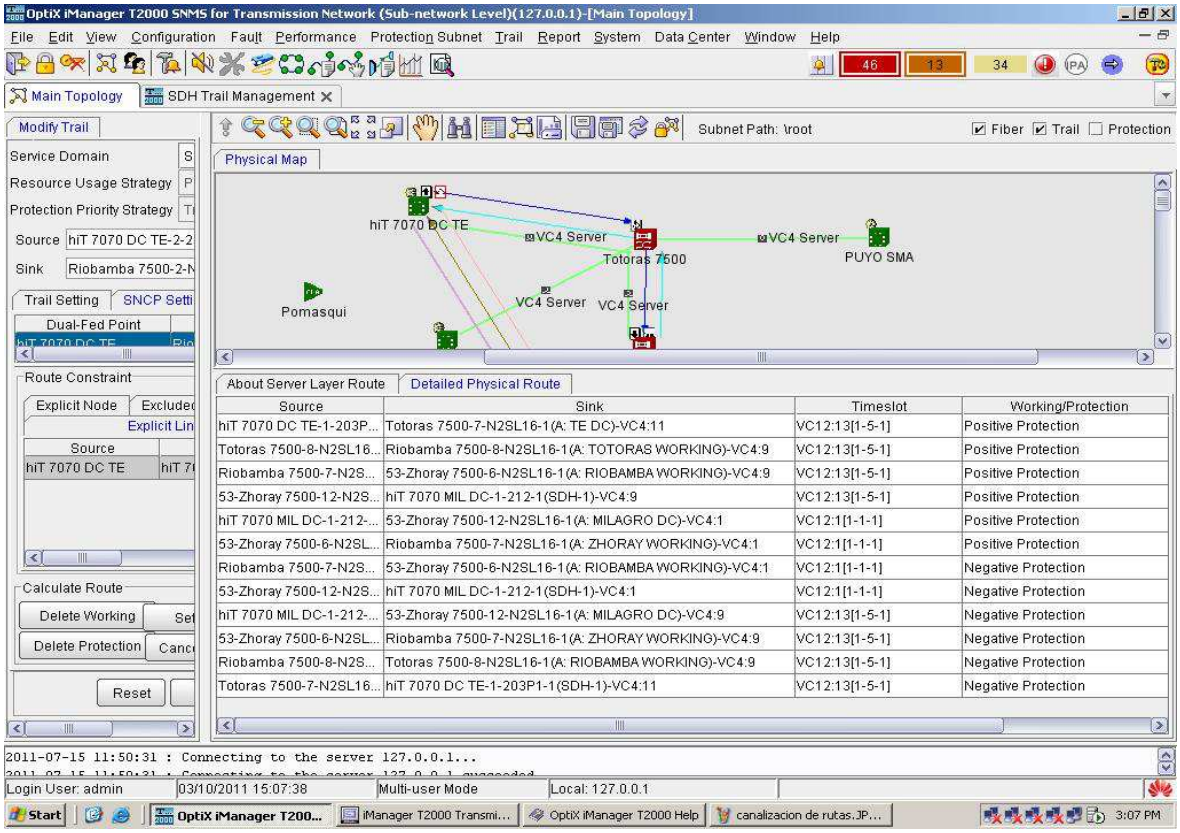

Figura 4.44 Detalle de rutas en el Sistema de Protección SNCP.

La función de protección de trayecto (*Path Protection*) permite ingresar un tributario en ambas direcciones del anillo sobre un equipo ADM y seleccionar en la matriz de conmutación la dirección en mejor estado. En este caso el tráfico de cada tributario ocupa un lugar en ambas ramas del anillo y como se puede observar en la Figura 4.31 esto se representa por *Positive Protection* o *Negative Protection* que es la dirección que puede tomar la conmutación con relación a su origen de falla.

Las opciones de conmutación en SNCP son forzar manualmente conmutando a la protección (*Forze Manual To Protect*) o que conmute por falla en un tramo del anillo.

Para esto se probó forzando un VC-12 manualmente a la protección, dando como resultado la conmutación del tráfico al lado contrario de donde se produjo la falla.

La restauración se basa en encontrar un camino alternativo para la comunicación en caso de fallo. El tiempo de procesamiento necesario para encontrar una ruta de tráfico alternativo se presenta como una dificultad para la rápida restauración del tráfico afectado, ya que en este caso, el tiempo transcurrido entre el fallo y la restauración, puede ser hasta del orden de los 50 ms.

La restauración es iniciada únicamente tras la detección de pérdida de señal por parte del sistema de gestión de red y no cuando el fallo ocurre. Esto lleva a que los tiempos de restauración sean relativamente lentos, del orden de segundos o minutos.

Aun siendo tan versátil este mecanismo, debido a su costo alto y complejidad, solo es recomendable para servicios en los que sea estrictamente necesario que la calidad de la señal sea máxima.

1.1.32 Sistema de Protección 1+1 MSP

Las pruebas para este Sistema de Protección fueron realizadas entre multiplexores SIEMENS HiT7070 en donde el tramo seleccionado para las mismas fue el comprendido entre Transelectric (Siemens HiT7070 DC) y Santo Domingo (Siemens HiT7070 DC) a nivel STM-16. Este análisis se lo realizo a nivel de conexión de línea como se muestra en la Figura 4.32.

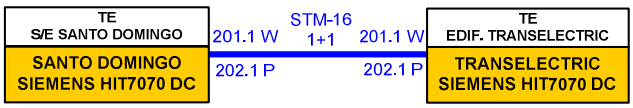

Figura 4.45 Conexión de Línea para las pruebas del Sistema de Protección 1+1 MSP.

La idea que utiliza este mecanismo de protección es la redundancia. El hecho de enviar la información por dos caminos distintos hace que si en cualquiera de los dos ocurren fallos, tengamos siempre un camino de respaldo.

Este mecanismo cuenta, como todos, con ventajas e inconvenientes. Como ventajas podemos citar que teniendo dos caminos activos (Figura 4.32), sea cual sea el que falle, tenemos una manera de recuperarnos. Además, al llegar a recepción la misma información repetida, podemos utilizarlo como método de recuperación de señal.

La mayor desventaja de este sistema es que en funcionamiento normal, que es la mayor parte del tiempo, estamos consumiendo el doble de recursos de los necesarios. En la Figura 4.32 se muestra un nodo en condiciones normales de funcionamiento. El receptor utiliza un conmutador para seleccionar la señal de servicio en condiciones de funcionamiento normales en modo reversible.

Esto se muestra en la Figura 4.33 donde se realiza la configuración del Sistema de Protección 1+1 MSP y su diagrama respectivo.

Sistema de Gestión SIEMENS, multiplexor HiT7070:

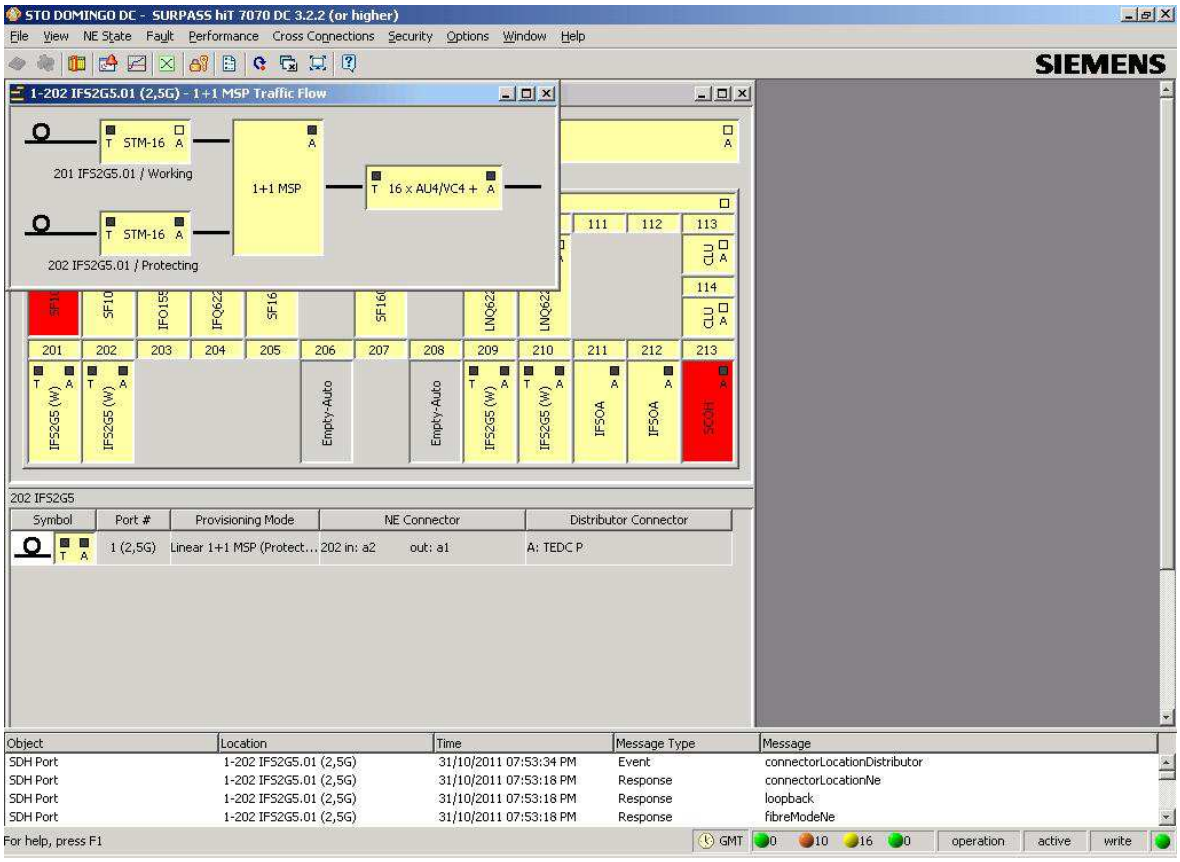

Figura 4.46 Configuración del Sistema de Protección 1+1 MSP en el nodo Santo Domingo DC a nivel STM-16.

El flujo de tráfico está en condiciones normales, es decir por la línea Principal. La configuración del Provisioning Mode es *Lineal 1+1 MSP* con esto queda confirmado que el Sistema de Protección a utilizar es 1+1 MSP y está conectado con la línea que mira hacia Transelectric DC (Protección).

La misma configuración se la realizó para el nodo Transelectric DC con la diferencia de que la protección fue creada de manera inversa, es decir hacia la línea que mira hacia el nodo Santo Domingo DC.

Sistema de Gestión SIEMENS, multiplexor HiT7070:

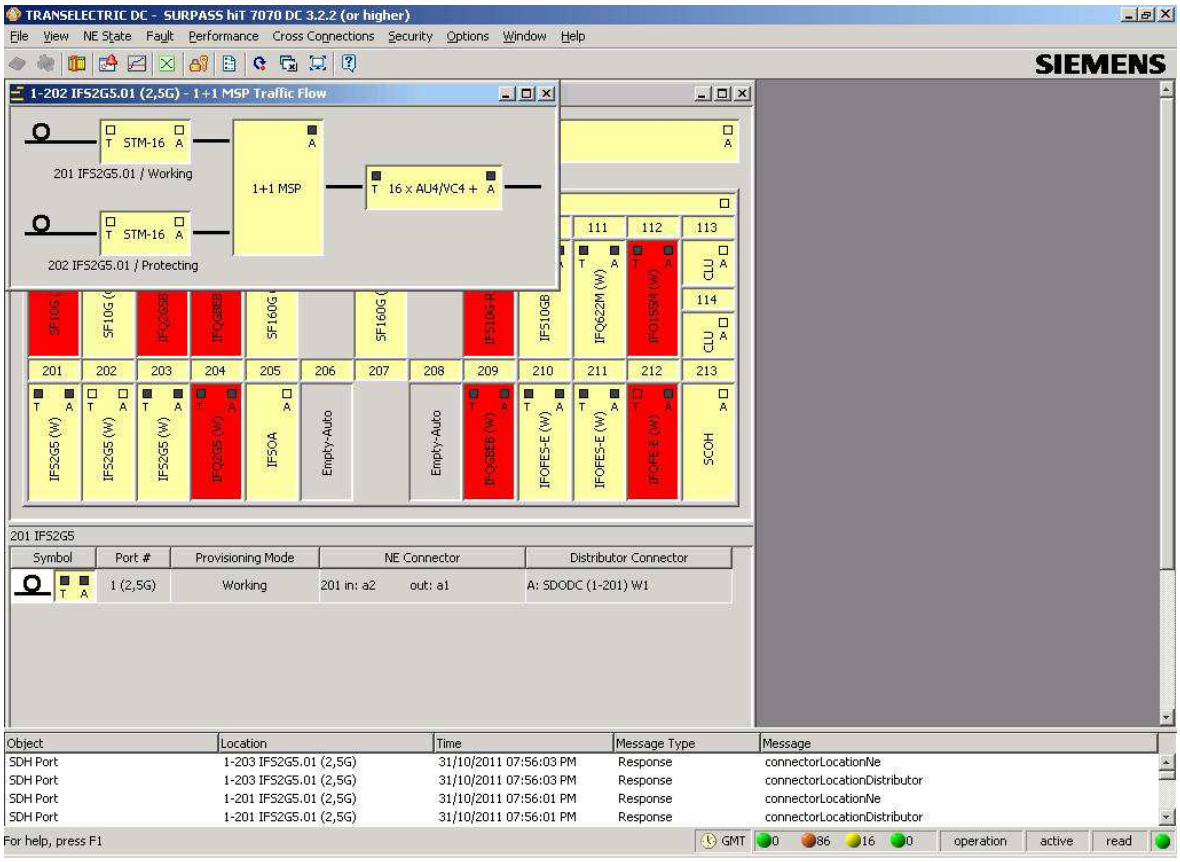

Figura 4.47 Configuración del Sistema de Protección 1+1 MSP en el nodo Transelectric DC a nivel STM-16.

La Figura 4.34 muestra el nodo cuando hay un fallo en el servicio. Para este caso, el receptor detectará la pérdida de señal y conmutará automáticamente a la línea de protección.

El tráfico puede ser restablecido cuando múltiples fallos afectan al tráfico solamente en uno de los caminos (el de servicio o el de protección). Si ambos caminos se ven afectados por determinados fallos, el tráfico no puede ser restablecido.

Esto se demuestra en las siguientes Figuras:

Sistema de Gestión SIEMENS, multiplexor HiT7070:

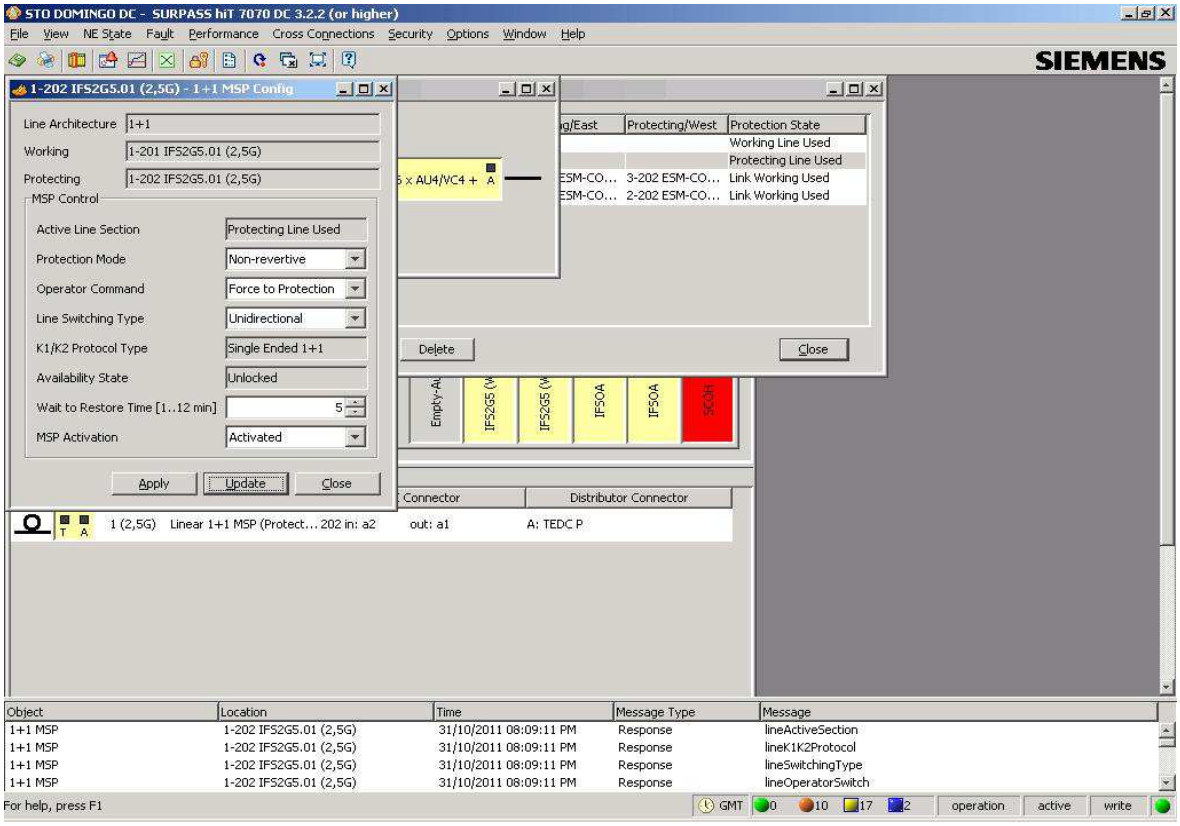

Figura 4.48 Proceso de conmutación en situación de fallo en la línea principal en el nodo Santo Domingo DC.

Como se puede observar en la Figura 4.35 el proceso de conmutación se llevó a cabo, notando esto en Active Line Section, donde se observa que la línea en uso es la de Protección, *Protecting Line Used*, y esto nos indica que la conmutación fue realizada con éxito sin ocasionar tiempo de indisponibilidad o perdidas en el canal gracias a que las dos líneas, tanto la Principal como la de Protección están siempre activas.

Los mismos eventos se produjeron en el nodo Transelectric DC y se muestran a continuación:

Sistema de Gestión SIEMENS, multiplexor HiT7070:

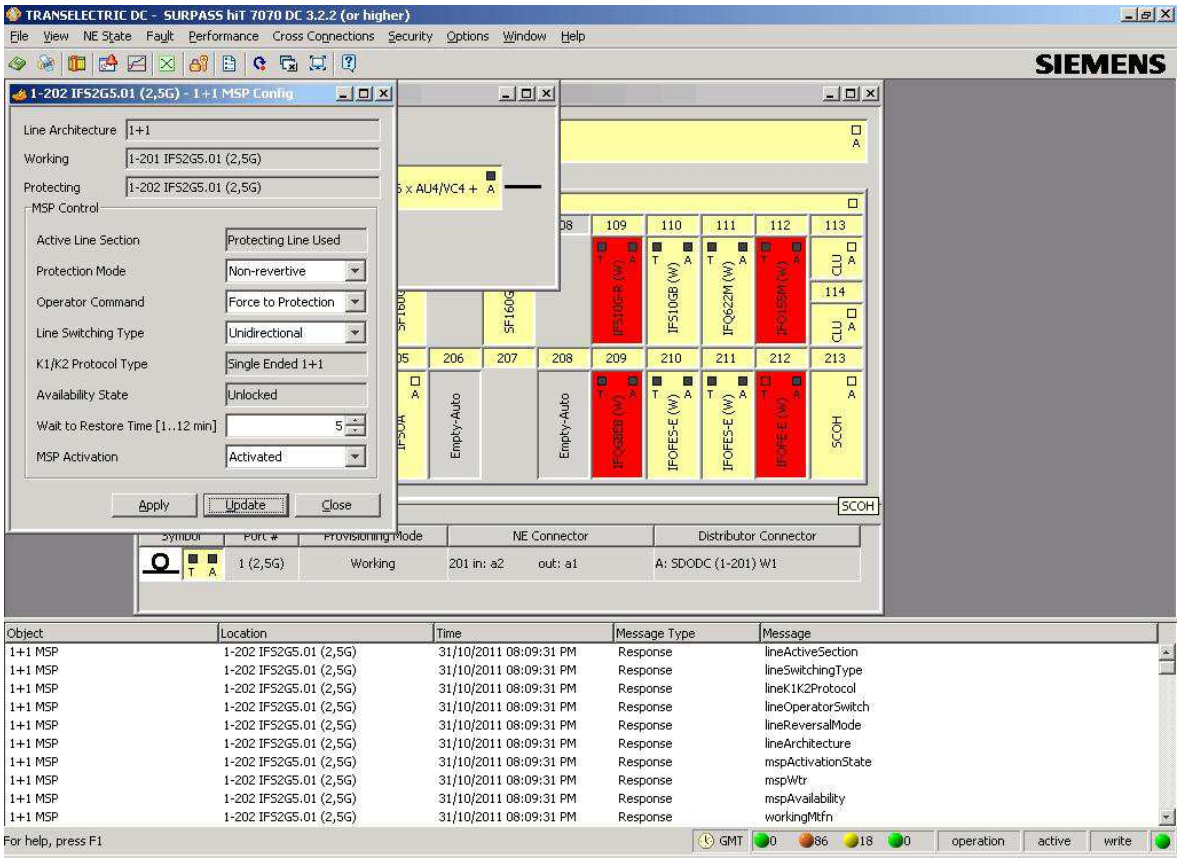

Figura 4.49 Proceso de conmutación en situación de fallo en la línea principal en el nodo Transelectric DC.

Al igual que en el nodo Santo Domingo DC, el sistema de protección es 1+1 MSP. Los eventos que se produjeron en ambos casos fueron la activación MSP con la detección de su respectiva protección, 1+1; activación del Modo de Reversa lo que proporciona seguridad de que si el enlace principal vuelve a su normalidad, conmute hacia él nuevamente. Se activaron los bits de cabecera K1 y K2 de los Protocolos de Línea y con esto la conmutación de la línea principal a la protección, dejando esta última como activa y con tráfico normalizado.

Así se deja ratificado que el Sistema de Protección 1+1 MSP está correctamente implementada y así asegurar una alta disponibilidad en la red de transporte SDH de CELEC EP – TRANSELECTRIC.

CAPÍTULO V

EVALUACIÓN DEL DISEÑO

El análisis de los proyectos constituye una evaluación de los recursos a emplearse, a través de la cual se determinan los beneficios y costos en los que se puede incurrir al pretender realizar una inversión, en donde uno de sus objetivos es obtener resultados que apoyen la toma de decisiones frente a las actividades de inversión.

Al analizar los proyectos de inversión se determinan los costos de oportunidad que incurren al invertir al momento de obtener beneficios, mientras se sacrifican las posibilidades de otras oportunidades, o si es posible privar el beneficio actual para trasladarlo al futuro, al tener como base específica el proyecto a realizarse.

Una de las evaluaciones que deben de realizarse para apoyar la toma de decisiones en lo que respecta a la inversión de un proyecto, es la que se refiere a la evaluación financiera, que se apoya en el cálculo de retorno de inversión que traerá el proyecto para una empresa en general, en este caso para CELEC EP - TRANSELECTRIC.

ANÁLISIS DE DISPONIBILIDAD DEL SISTEMA

Durante los últimos años, la convergencia de servicios ha introducido mayores demandas de los sistemas de transmisión de información. Uno de los mayores interrogantes y punto de gran análisis por el costo que implica, tanto la inversión en capital humano como en recursos económicos, es el tiempo de disponibilidad del servicio brindado al usuario frente al porcentaje mínimo solicitado por los clientes.

La diversidad en equipamiento activo acoplado a los sistemas de transmisión, requiere la implementación de rutas de respaldo para evitar problemas de interrupción del servicio; esto con el objetivo de aumentar la confiabilidad del sistema e incrementar la disponibilidad de la red de transporte.

La disponibilidad de un sistema es usualmente expresada como una relación del tiempo de funcionamiento del servicio en un periodo en valor porcentual.

$$\%d = (td / tp) * 100$$

Siendo *%d* = porcentaje de disponibilidad,

td = tiempo disponible del servicio (tiempo donde el servicio está disponible)
tp **=** tiempo de pérdida del servicio (tiempo donde el servicio no está disponible)

Esta relación es un valor porcentual para así expresar la disponibilidad del servicio.

Los valores más comunes de disponibilidad son:

99.9 % = 2628 segundos/mes, 43.8 minutos/mes u 8.76 horas/año, de afectación total en la red (tres nueves)

99.99% = 268.8 segundos/mes, 4.38 minutos/mes u 52.6 horas/año, de afectación total en la red (cuatro nueves)

99.999% = 26.28 segundos/mes, 0.44 minutos/mes u 5.26 horas/año, de afectación total en la red (cinco nueves)

La disponibilidad ofrecida por CELEC EP - TRANSELECTRIC a los clientes es la siguiente:

99.80% = 268.2 segundos/mes para servicio CLEAR CHANNEL
99.60% = 267.7 segundos/mes para servicio IP

Con este valor medimos de la proporción de tiempo que la red está disponible con los servicios del cliente. La disponibilidad indica la confiabilidad del canal contratado por el cliente y éste se encuentre operativo. Con esto se garantiza que el servicio esté disponible para uso del cliente.

Para conseguir un correcto desempeño de la red y una alta disponibilidad podemos tomar alguna de las siguientes recomendaciones:

Protección de equipamiento: La disponibilidad del equipamiento puede ser implementada mediante aplicación de protecciones locales en el propio elemento de red. Por ejemplo, las alimentaciones, tarjetas de control, o unidades tributarias pueden ser duplicadas. Una tarjeta con problemas será reemplazada por su protección automáticamente donde este esquema de protección esté presente.

Robustez de la red: Para incrementar la supervivencia de la red y por tanto la disponibilidad, los enlaces de red deben ser protegidos. Existen procedimientos que son aplicados para asegurar que el fallo de un enlace de transporte sea reemplazado por otro enlace de protección y/o un camino alternativo ante la presencia de un fallo en un nodo o enlace. Hay dos tipos de mecanismos utilizados de protección.

Restauración: Este es un proceso lento automático o manual el cual emplea capacidad extra libre entre nodos finales para recuperar tráfico después de la pérdida de servicio. Al detectarse el fallo, el tráfico es reenrutado por un camino alternativo. El camino alternativo se encuentra de acuerdo con algoritmos predefinidos y generalmente emplea cross-conexiones digitales. Este proceso puede tomar algunos minutos.

Protección: La protección abarca mecanismos automáticos con elementos de red, los cuales aseguran que los fallos sean detectados y

compensados antes de que ocurra una pérdida de servicios. La protección hace uso de capacidad pre-asignada entre nodos y su uso es preferible a la restauración porque la capacidad de reserva siempre estará disponible en un corto intervalo de tiempo.

La disponibilidad ofrecida a los clientes de CELEC EP – TRANSELECTRIC desde octubre de 2010 hasta septiembre de 2011 se detalla en la Tabla 5.1 de Disponibilidad de la Red.

MES	TIEMPO A CUMPLIRSE (s)	TIEMPO DE INDISPONIBILIDAD (s)	TIEMPO CUMPLIDO (s)	CONFIABILIDAD DEL SISTEMA ACTUAL (%)	CONFIABILIDAD DEL SISTEMA CON IMPLEMENTACIÓN (%)
Oct-10	278.985.600	217.484	278.768.116	99.922	99.990
Nov-10	281.318.400	144.576	281.173.824	99.949	99.990
Dec-10	303.091.200	15.144	303.076.056	99.995	99.990
Jan-11	318.729.600	491.504	318.238.096	99.846	99.990
Feb-11	296.870.400	74.460	296.795.940	99.975	99.990
Mar-11	339.465.600	118.140	339.347.460	99.965	99.990
Apr-11	329.702.400	1.337.256	328.365.144	99.594	99.990
May-11	333.504.000	579.101	332.924.899	99.826	99.990
Jun-11	328.492.800	11.700	328.481.100	99.996	99.990
Jul-11	367.372.800	20.160	367.352.640	99.995	99.990
Aug-11	350.092.800	223.003	349.869.797	99.936	99.990
Sep-11	357.523.200	386.659	357.136.541	99.892	99.990
TOTAL	3.885.148.800	3.619.187	3.881.529.613	99.908	99.990

Tabla 5.1 Disponibilidad de la Red

Para la Tabla 5.1 se tomó la información de: disponibilidad ofertada, indisponibilidad y confiabilidad del sistema, contrastándolo con la confiabilidad del sistema con la implementación del proyecto, teniendo como resultado que la confiabilidad del sistema se mantendrá en un estándar de 99.99 %, es decir cuatro nueves, obteniendo con esto una mayor confiabilidad en el sistema, 0.082 % mas confiable, y eso se verá reflejado en una mayor recaudación por facturación.

Tomaremos en cuenta que el tiempo de funcionamiento y el de disponibilidad no son sinónimos. Un sistema puede estar en funcionamiento pero no disponible los servicios, como en el caso de un fallo de red.

La disponibilidad de red es un aspecto clave para CELEC EP – TRANSELECTRIC puesto que debe mantener altos estándares de calidad en los servicios que brindan y con esto optimizar la confiabilidad en la red.

ANÁLISIS DE RECAUDACIÓN POR SERVICIO

Se realizó una tabla comparativa de montos facturados con la indisponibilidad actual y los montos a facturarse disminuyendo los tiempos de indisponibilidad con la implementación del proyecto. Los valores tomados son desde octubre de 2010 hasta septiembre de 2011 que se presentan en la Tabla 5.2:

MES	MONTO FACTURADO (USD $)	MONTO DE FACTURACIÓN (cumpliendo disponibilidad) (USD $)	MONTO NO FACTURADO POR INDISPONIBILIDAD (USD $)	PORCENTAJE DE PÉRDIDA POR INDISPONIBILIDAD (USD %)	MONTO NO FACTURADO POR INDISPONIBILIDAD CON IMPLEMENTACIÓN (USD $)	PORCENTAJE DE PÉRDIDA POR INDISPONIBILIDAD CON IMPLEMENTACIÓN (USD %)
oct-10	-2.849,18	279.563,26	282.412,44	101,0192	220.281,70	78,7949
nov-10	1.015.402,29	1.015.468,90	66,61	0,0066	51,96	0,0051
dic-10	371.571,81	371.748,32	176,51	0,0475	137,68	0,0370
ene-11	3.580.993,94	3.584.262,94	3.269,00	0,0912	2.549,82	0,0711
feb-11	200.020,24	200.131,49	111,25	0,0556	86,78	0,0434
mar-11	995.011,86	996.058,25	1.046,39	0,1051	816,18	0,0819
abr-11	692.720,88	695.332,88	2.612,00	0,3756	2.037,36	0,2930
may-11	302.852,70	303.273,93	421,23	0,1389	328,56	0,1083
jun-11	362.030,06	363.484,11	1.454,05	0,4000	1.134,16	0,3120
jul-11	250.453,11	252.995,42	2.542,31	1,0049	1.983,00	0,7838
ago-11	401.130,25	417.466,24	16.335,99	3,9131	12.742,07	3,0522
sep-11	367.373,17	367.543,51	170,34	0,0463	132,87	0,0361
TOTAL	8.536.711,13	8.847.329,25	310.618,12	3,5109	242.282,13	
PROMEDIO						2,7385
MONTO PARA EL PROYECTO (USD $)						68.335,98

Tabla 5.2 Montos de facturación

El desarrollo de esta Tabla nos muestra en valores reales el monto facturado con indisponibilidad y el monto facturado sin indisponibilidad, haciendo un contraste con el posible monto de facturación terminada la implementación del proyecto, lo que nos arrojó como resultado un incremento en la facturación del 0.79 % lo que en valor monetario corresponde a USD $ 68.335,98.

Gracias a la implementación del proyecto las perdidas con respecto al monto facturado cumpliendo la disponibilidad se reducirán hasta en un 22 % con relación a las notas de crédito.

ANÁLISIS DE TICKETS DE FALLAS DE LA RED

El siguiente análisis se lo realizó de acuerdo al porcentaje de tickets abiertos por motivos de falla en las protecciones SDH en el Centro de Gestión de Telecomunicaciones de CELEC EP – TRANSELECTRIC, las cuales se muestran a continuación:

Cortes de Fibra: La principal causa de fallo de fibras es el daño causado por factores fuera del alcance del ser humano como rayos, terremotos choques de automotores, avionetas, etc.

Equipamiento puede fallar debido a efectos de desgaste de componentes y tiempo de vida útil.

Fallos de alimentación: ocasionados por problemas en el suministro de energía al sistema de alimentación de -48VDC.

Mantenimientos: no programados y errores realizados durante el trabajo que pueden afectar la disponibilidad del servicio.

Desastres naturales que quedan fuera de control humano y ocasionan interrupción en los servicios.

El 22 % de fallos en la red corresponde a fallas en los sistemas de protecciones, con lo que mediante este proyecto se trata de reducir al máximo este porcentaje y así llegar a una red robusta tanto para beneficio del cliente en aspecto de confiabilidad de la red, como para CELEC EP – TRANSELECTRIC en lo que respecta a recaudación monetaria.

Los datos de tickets abiertos no se pueden mostrar en este proyecto de tesis ya que es información confidencial para la empresa.

ANÁLISIS DE FACTIBILIDAD DEL PROYECTO

El análisis de factibilidad de un proyecto forma parte del proceso de evaluación al cual debe someterse todo proyecto de inversión. En la actualidad en ocasiones se aborda este tema desde un enfoque económico-financiero fundamentalmente, olvidando el enfoque técnico el cual debería ser tratado.

La evaluación de proyectos de inversión constituye hoy en día un tema de gran interés e importancia ya que mediante este proceso se valora cualitativa y cuantitativamente las ventajas y desventajas de destinar recursos a una iniciativa específica. El análisis de factibilidad de un proyecto es un método para presentar el mejor uso o necesidad de los recursos que posee el Área de Administración de Redes y Comunicaciones de CELEC EP - TRANSELECTRIC.

El estudio de factibilidad técnica tiene por objetivo proveer de información para cuantificar el monto de la inversión y los beneficios a conseguir.

Para la implementación del diseño de la red de protecciones se requiere las tarjetas y módulos ópticos descritos en la Tabla 5.3:

TRAMO	TARJETA	MARCA	MODULO	MARCA
TRANSELECTRIC-TOTORAS (120Km)	IFS2G5	SIEMENS	JE-33dB-16.2/3	SIEMENS
	NSL16	HUAWEI	V-16.2JE(BA)	HUAWEI
MILAGRO-ZHORAY (120 Km)	IFS2G5	SIEMENS	JE-33dB-16.2/3	SIEMENS
	NSL16	HUAWEI	V-16.2JE(BA)	HUAWEI
ZHORAY-CUENCA (60 Km)	NSL16	HUAWEI	L-16.2	HUAWEI
	IFS2G5	SIEMENS	L-16.2	SIEMENS
MILAGRO-MACHALA (140 Km)	IFS2G5	SIEMENS	JE-33dB-16.2/3	SIEMENS
	IFS2G5	SIEMENS	JE-33dB-16.2/3	SIEMENS
	IFSOA	SIEMENS		
	IFSOA	SIEMENS		

Tabla 5.3 Requerimiento de Tarjetas

El avance de nuevas tecnologías y actualización de las ya existentes ha hecho que no exista disponibilidad de tarjetas para el equipo multiplexor SDH HiT7070 de la marca SIEMENS. El fabricante nos dio a conocer mediante un comunicado que ya no se están fabricando tarjetas ni equipo de la serie 7070. Por este motivo no es factible realizar un análisis de presupuesto para la implementación del proyecto.

ANÁLISIS DE COSTO-BENEFICIO EN LA IMPLEMENTACIÓN DE LA PROTECCIÓN DE LA RED

El costo-beneficio es una lógica o razonamiento basado en el principio de obtener los mayores y mejores resultados al menor esfuerzo invertido, tanto por eficiencia técnica como por motivación humana.

Se supone que todos los hechos y actos pueden evaluarse bajo esta lógica, aquellos dónde los beneficios superan el coste son exitosos, caso contrario fracasan.

El análisis de costo-beneficio es un término que se refiere tanto a:

Una disciplina formal (técnica) a utilizarse para evaluar, o ayudar a evaluar, en el caso de un proyecto o propuesta, que en sí es un proceso conocido como evaluación de proyectos.

Un planteamiento informal para tomar decisiones de algún tipo, por naturaleza inherente a toda acción humana.

Bajo ambas definiciones el proceso involucra, ya sea explícita o implícitamente, un peso total de los gastos previstos en contra del total de los beneficios previstos de una o más acciones con el fin de seleccionar la mejor opción o la más rentable.

El análisis costo-beneficio es una técnica importante dentro del ámbito de la teoría de la decisión. Pretende determinar la conveniencia de un proyecto mediante la enumeración y valoración posterior en términos monetarios de todos los costes y beneficios derivados directa e indirectamente para este proyecto.

El análisis de costo-beneficio es una herramienta de toma de decisiones para desarrollar sistemáticamente información útil acerca de los efectos deseables e indispensables de los proyectos públicos, para este caso es la "Interoperabilidad de Sistemas de Protecciones entre Equipos Multiplexores en la Red de Transporte SDH de CELEC EP – TRANSELECTRIC, el cual se detalla en la Tabla 5.4.

BENEFICIO	COSTO
Robustez en la red	Aumentar el número de enlaces
Aumentar la disponibilidad de la red 0,082 %	Invertir en compra de tarjetas y módulos ópticos
Aumentar la recaudación 0,72 %	Complejidad de los sistemas de protección
Mejora en calidad de servicio QoS	Reubicación de las tarjetas ópticas en los equipos Siemens HiT7070
Fidelizar a los clientes	Posibles cortes de servicio
Disminuir el índice de fallas en la red	

Tabla 5.4 Costo – Beneficio

Con esto se deja por sentado que el Análisis de Costo – Beneficio arroja que la factibilidad del proyecto es viable.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Se realizó la interoperabilidad de un esquema de protección en anillo y un esquema de protección lineal entre equipos multiplexores SDH marca Huawei modelo OSN7500 y marca Siemens modelo HiT7070 de CELEC EP – TRANSELECTRIC.

Mediante un escenario de pruebas en la red de transporte SDH se comprobó la interoperabilidad de los equipos multiplexores, se analizó los diferentes mecanismos de protección, esquemas de red y los protocolos utilizados para los sistemas de protección.

Se investigó sobre el funcionamiento de la tecnología SDH y sus diferentes tipos de protecciones, de los cuales se comprobó la interoperabilidad de dos sistemas de protección siendo estos los que más se acoplan a la red de transporte SDH de CELEC EP – TRANSELECTRIC.

Se realizó un estudio del estado actual de la red de transporte SDH, el cual arrojó como resultado que solo se manejan sistemas de protecciones lineales 1+1 MSP y 1:N MSP en tramos con equipos del mismo fabricante, siendo esto solo entre equipos multiplexores HUAWEI o solo entre equipos multiplexores SIEMENS, dando como resultado varios tramos sin protección y vulnerables a fallas.

Se realizó un análisis comparativo entre los diversos tipos de protecciones que se pueden utilizar en la red de transporte SDH de CELEC EP – TRANSELECTRIC tomando en cuenta el tráfico y disponibilidad de servicios, obteniendo como resultado que se pueden utilizar esquemas de protección en anillo y a nivel se servicio, siendo estos el MS – SPRING y el SNCP respectivamente y así obtener una red robusta alcanzando, para alcanzar un nivel de disponibilidad deseado.

Se ejecutó mediante pruebas de funcionamiento la interoperabilidad de esquemas de protección lineal y en anillo siendo el 1+1 MSP y 1+N MSP, en lo que respecta a protecciones lineales, y MS – SPRING y SNCP en lo que respecta a protección en anillo y protección de servicio en anillo. De manera general los resultados mostraron un éxito en el 75% de las pruebas tomando en cuenta que la protección MS – SPRING no se la pudo finalizar por factores físicos en el equipo SIEMENS HiT7070, pero si se los realizó de manera lógica simulando un canal real con un software de simulación llamado EXCERCISE RING.

Se probó el sistema de protección 1+1 MSP en el tramo Transelectric (Siemens HiT7070 DC) y Santo Domingo (Siemens HiT7070 DC) a nivel STM-16. Al realizar las pruebas del sistema no hubo afectación en el tramo escogido, es decir no generaron tiempo de indisponibilidad, y las mismas se realizaron entre equipos multiplexores de la misma marca, ya que la organización de las tarjetas dentro del equipo multiplexor es fundamental para implementar este tipo de protección MSP. Este inconveniente se da dentro de los equipos SIEMENS puesto que al querer configurar una tarjeta de protección, ésta necesita ser contigua a la tarjeta a ser protegida, factor que no se da en los equipos HUAWEI. Es por este motivo que no se probó la interoperabilidad entre estas marcas de multiplexores pero si la factibilidad de probar una protección en este tramo entre equipos multiplexores SIEMENS. La mayor desventaja de este sistema es que en funcionamiento normal, que es la mayor parte del tiempo, estamos consumiendo el doble de recursos de los necesarios.

El sistema de protección 1:N MSP fue probado en el tramo Zhoray, con multiplexores HUAWEI (OSN 7500), y Milagro con multiplexores SIEMENS (HiT7070). Las pruebas de interoperabilidad se realizaron con un servicio activo cuya capacidad de tráfico es de 300 Mbps. Respecto al tiempo de indisponibilidad que la falla pudo haber ocasionado, se tomó algunas precauciones como control de ping extendido al cliente, permitiendo verificar en las pruebas que no se registraron pérdidas de tráfico, ya que la conmutación al camino de protección fue casi imperceptible. La disponibilidad de tarjetas y el número de enlaces de línea en el tramo a ser protegido son un factor importante para levantar un Sistema de Protección de estas características.

La topología que se utilizó para probar el Sistema de Protección SNCP fue en anillo a nivel VC-12. El trayecto escogido para esta prueba comprendió los nodos de Transelectric (Siemens HiT7070 DC), Milagro (Siemens HiT7070 DC), Zhoray (Huawei OSN 7500), Riobamba (Huawei OSN 7500) y Totoras (Huawei OSN 7500). SNCP trabaja especialmente sobre anillos, porque se aseguran diversas rutas. El hecho de que trabaje sobre nodos intermedios hace que su eficacia sea también buena sobre redes malladas. Las pruebas realizadas para este anillo con protección SNCP fueron realizadas en base a comprobar la interoperabilidad de las gestiones SIEMENS (HiT7070) y HUAWEI (OSN 7500) dando lugar a que las pruebas sean satisfactorias y que ambas gestiones acepten el Sistema de Protección como tal. Aun siendo tan versátil este mecanismo, debido a su costo alto y complejidad, solo es recomendable para servicios en los que sea estrictamente necesario que la calidad de la señal sea máxima.

La ubicación de las tarjetas dentro del multiplexor, sea cual fuere su marca, tiene un papel importante dentro del desarrollo o no del esquema de protección. Las pruebas del esquema de protección MS - SPRING no se llevaron a cabo de manera práctica y se las realizó de manera lógica utilizando herramientas, dentro del mismo software del multiplexor, que simularon escenarios reales a condiciones reales. La ejecución de las

pruebas de manera práctica para este esquema de protección implicaban reubicar tarjetas dentro del multiplexor, migrar tráfico y con esto provocar tiempo de indisponibilidad en los enlaces, por lo que se realizó pruebas de manera lógica utilizando una herramienta de ensayo llamada TEST RING, la cual permitió realizar una simulación del Sistema de Protección ante un evento de falla real utilizando una topología en anillo compuesta de nodos previamente definidos. Las pruebas para el sistema de protección MS-SPRING fueron realizadas en el multiplexor HUAWEI en la ruta comprendida entre Totoras (OSN 7500), Riobamba (OSN 7500) y Zhoray (OSN 7500); a dichos nodos se les tomó como tramos de prueba para la creación de un anillo a nivel STM-16. Las pruebas en anillo Multiplex Section Shared Protection Ring (MS-SPRING) fueron exitosas. El tiempo de indisponibilidad fue mínimo y sin afectación de tráfico.

RECOMENDACIONES

El número de slots libres es un factor importante que se debe tomar en cuenta para realizar pruebas e implementar un esquema de protección, ya que de la ubicación de las tarjetas dentro del chasis del equipo depende el tipo de protección que se pueda poner en funcionamiento.

Se requiere realizar un análisis de reubicación de tarjetas en los equipos multiplexores SIEMENS y HUAWEI, de tal manera, que en un futuro, se puedan configurar protecciones 1:N MSP y MS - SPRING sin ningún contratiempo.

Dar un mantenimiento cada determinado tiempo a los equipos multiplexores ya que en algunos de los nodos se podía encontrar patch cord de fibra sin utilizar, y esto a la postre puede impedir el manejo adecuado de los equipos de core.

Depurar los equipos multiplexores con relación a los servicios activos y los no activos, ya que al querer levantar los canales de pruebas se pudo

constatar que existían canalización basura lo cual impedía optimizar el tiempo en las pruebas de los sistemas de protección.

Hacer un análisis de ingeniería de tráfico para mediante este poder adquirir nuevos equipos SDH y ampliar la capacidad de la red sin ningún problema de disponibilidad de tarjetas o uso de los enlaces de protección.

REFERENCIAS BIBLIOGRÁFICAS

1. http://arantxa.ii.uam.es/~ferreiro/sistel2008/anexos/Proteccion&restauracion
2. http://es.scribd.com/Protecciones-SDH-Ethernet/d/46779807
3. http://tlm.unavarra.es/~daniel/docencia/rba/rba06_07/slides
4. http://www.ramonmillan.com/tutoriales sdh parte2.php

GLOSARIO DE TÉRMINOS

AIS.- Alarm Indication Signal. Alarma de desconexión proveniente del siguiente salto.

Arquitectura TCP/IP.- Arquitectura de transferencia de paquetes para redes WAN y LAN basado en el modelo OSI, esta arquitectura se basa en tres capas física, red, transporte y aplicación.

Backbone.- Se refiere a las principales conexiones troncales de una red, está compuesta por routers, switchs y medios físicos de comunicación como fibra óptica, etc.

BGP.- Border Gateway Protocol - Protocolo de Puerta de Enlace de Borde.

BIT.- Binary Digit. Digito Binario. Unidad mínima de información, puede tener dos estados "0" o "1".

Carrier.- Operador de Telefonía que proporciona conexión a Internet a alto nivel.

DTE.- Data Terminal Equipment. Equipo Terminal de Datos. Se refiere por ejemplo al computador conectado a un modem que recibe datos de este.

DTMF.- Dual Tone Multifrecuency. Multi frecuencia de doble tono. Son los tonos que se utilizan en telefonía para marcar un número telefónico.

DUPLEX.- Capacidad de un dispositivo para operar de dos maneras. En comunicaciones se refiere normalmente a la capacidad de un dispositivo para recibir/transmitir. Existen dos modalidades HALF-DUPLEX: Cuando puede recibir

y transmitir alternativamente y FULL-DUPLEX cuando puede hacer ambas cosas simultáneamente.

Firewall.- Cortina de Fuego. Router diseñado para proveer seguridad en la periferia de la red. Se trata de cualquier programa (Software) ó router (Hardware) que protege a una red de otra red. El firewall da acceso a una maquina en una red local a Internet pero Internet no ve más allá del firewall.

FTP.- File Transfer Protocol - Protocolo de Transferencia de Archivos.

Full Duplex.- Circuito o dispositivo que permite la transmisión en ambos sentidos simultáneamente.

Intranet.- Red interna o red local.

IP.- Internet Protocol – Protocolo de Internet.

ISP.- Internet Service Provider – Proveedor de Servicio de Internet.

LAN.- Local Area Network - Red de Área Local.

LOS.- Loss of Signal. Alarma de desconexión en el punto presente.

OSI.- Open System Interconnection - Sistema de Interconexión Libre.

OSPF.- Open Shortest Path First - Protocolo de Enrutamiento Jerárquico de Pasarela Interior.

QoS.- Quality of Service - Calidad de Servicio.

RADIUS.- Remote Authentication Access Control System - Sistema de Control de Acceso de Autenticación Remota.

RDI.- Remote Defect Indicator. Alarma remota proveniente de un AIS.

RIP.- Routing Information Protocol – Protocolo de Información de Enrutamiento.

SLA.- Service Level Agreement - Acuerdo de Nivel de Servicio.

SNMP.- Simple Network Management Protocol - Protocolo Simple de Administración de Red.

TACACS.- Terminal Access Controller Access Control System - Sistema de Controlador de Acceso mediante Control del Acceso desde Terminales, protocolo de autenticación remota, propietario de Cisco.

TCP.- Transfer Control Protocol – Protocolo de Control de Transferencia.

UNEQUIPPED.- Conexión sin equipo en el punto remoto o presente.

UTP.- Unshielded Twisted Pair - Par Trenzado No Blindado, tipo de cable que se utiliza principalmente para comunicaciones.

WAN.- Wide Area Network - Red de Área Amplia.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS