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

Santiago Alexis Morales Valencia
santym_06@hotmail.com
Departamento de Eléctrica y Electrónica, Escuela Politécnica del Ejercito. Sangolquí, Ecuador.

Resumen— El estudio del Proyecto contempló un levantamiento y análisis de información sobre del estado actual de la red de transporte SDH de CELEC EP - TRANSELECTRIC, sus nodos y esquemas de protección. El análisis se inició con el sistema actual de la red, las capacidades de tráfico y los enlaces de línea de la red SDH, además de la topología de la misma, los tipos de protección que se pueden utilizar, el software de gestión y la interoperabilidad de los sistemas de protección de los fabricantes SIEMENS y HUAWEI. Para este proyecto se utilizó las recomendaciones de la UIT-T para los estándares de protecciones, que nos permitió realizar un estudio que se ajuste a los requerimientos de la red de transporte SDH.

I. Introducción

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.

II. 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). 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 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.

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.

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

Como se puede apreciar en la Tabla 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**	**Topología**	**Tiempo Típico de Conmutación**
MS-SPRing	Todo el tráfico de la sección	Cualquier nodo en el anillo	Anillo	<50ms
1+1 MSP	Todo el tráfico de la sección	Nodos Adyacentes	Lineal/ Mayada	<50ms
Ruta Dedicada	VC individual	Nodo del extremo final del anillo	Mixta	<50ms
SNCP	VC individual	Nodo final o intermedio de la ruta	Mixta	<50ms
Restauración	VC individual	No hay conmutación de protección.	Mayada	>1min

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.

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

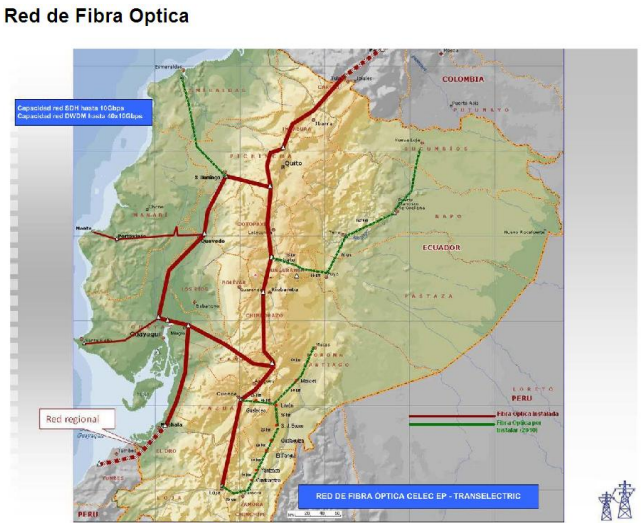
CELEC EP – TRANSELECTRIC, cuenta con servicios de portador de telecomunicaciones y de valor agregado para brindar transmisión de datos e Internet, a través de la red de fibra óptica en diferentes Subestaciones y Puntos de Presencia (PDP´s) a nivel nacional. Las capacidades que se ofrecen parten de la 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.

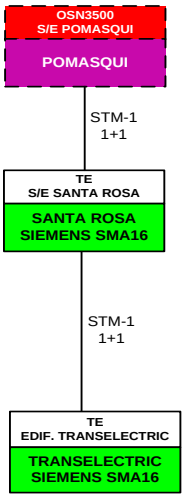
En la Figura se muestra la red de fibra óptica de CELEC EP – TRANSELECTRIC instalada, así como, la fibra óptica a instalar hasta finales de 2011 que comprende un tramo de 700 Km. en la parte Oriental del territorio Ecuatoriano.



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%.

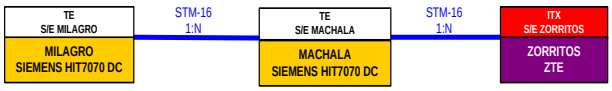
V. DISEÑO DE LA RED CON LOS DIFERENTES TIPOS DE PROTECCIONES SDH

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.



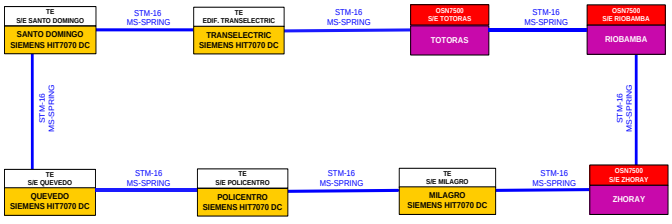
- Lineal: Transelectric (Siemens SMA 16), Santa Rosa (Siemens SMA 16) y Pomasqui (Huawei OSN 3500). Capacidad STM-1.

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.

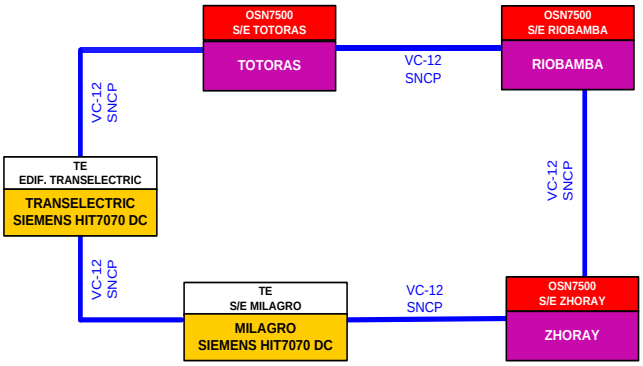
Protección MS-SPRing es un mecanismo de protección de anillo, el tráfico es enviado por una ruta en torno al anillo.



- 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.

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.



- 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.

VI. ANÁLISIS DE COSTO-BENEFICIO EN LA IMPLEMENTACIÓN DE LA PROTECCIÓN EN 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 siguiente Tabla.

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	

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

VII. CONCLUSIONES

- 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 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.

VIII. 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.

- 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.

RECONOCIMIENTO

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.

REFERENCIAS

[1] es.scribd.com/Protecciones-SDH-Ethernet/d/46779807
[2] J. U. Duncombe, “Infrared navigation—Part I: An assessment of feasibility (Periodical style),” IEEE Trans. Electron Devices, vol. ED-11, pp. 34–39, Jan. 1959.
[3] arantxa.ii.uam.es/~ferreiro/sistel2008/anexos/Proteccion&restauracion.pdf
[4] E. H. Miller, “A note on reflector arrays (Periodical style—Accepted for publication),” IEEE Trans. Antennas Propagat., to be published.
[5] tlm.unavarra.es/~daniel/docencia/rba/rba06_07/slides/16-TopologiasSDH.pdf
[6] www.ramonmillan.com/tutoriales sdh parte2.php

Autor:

Santiago Alexis Morales Valencia, nace en la ciudad de Quito el 6 de junio de 1985.
El en año 2003, obtiene el título de Bachillerato Técnico con especialización en Físico-Matemáticas en el Colegio Técnico Experimental de la Aviación Civil.
Actualmente es egresado de la Facultad de Electrónica de la Escuela Politécnica del Ejército y se encuentra presentando su proyecto de grado.
Realizó sus prácticas pre-profesionales y proyecto de grado en CELEC EP – TRANSELECTRIC, donde actualmente se encuentra trabajando, empezó en la Sección de Mantenimiento de telecomunicaciones y en la actualidad labora en la Sección de Operación como personal de turnos rotativos.