U N I V E R S I D A D D E C H I L E
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA

EVOLUCIÓN DE LAS REDES DE TRANSPORTE HACIA LA INTEGRACIÓN DE SERVICIOS: LAS REDES SDH

MEMORIA PARA OPTAR AL TÍTULO DE INGENIERO CIVIL ELECTRICISTA

JORGE ANTONIO POZO PEÑALOZA

PROFESOR GUÍA:
NÉSTOR BECERRA YOMA

MIEMBROS DE LA COMISIÓN:
ALBERTO CASTRO ROJAS
RICARDO BENAVIDES VALENZUELA

SANTIAGO DE CHILE
DICIEMBRE, 2006

RESUMEN DE LA MEMORIA
PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL ELECTRICISTA
POR: JORGE ANTONIO POZO PEÑALOZA
FECHA: 28 DE DICIEMBRE DE 2006
PROF. GUÍA: Dr. NÉSTOR BECERRA Y.

"Evolución de las Redes de Transporte hacia la Integración de Servicios: Las Redes SDH"

Las empresas operadoras están enfrentando cambios radicales en el modelo de negocio. Sus clientes ya no contratan enlaces a redes porque ellos buscan servicios. Actualmente, los grandes sistemas de transporte digital, tanto urbanos como de larga distancia e internacionales, se basan en SDH (*Synchronous Digital Hierarchy*), las cuales son optimas para tráfico de voz pues están diseñadas para conmutar circuitos. Sin embargo, la conmutación de paquetes es la que ha experimentado un crecimiento exponencial y las empresas deben hacer frente a este proceso. El protocolo IP ha sido sin dudas el gran gestor de sistemas de valor agregado, mostrándose en franca consolidación y expansión. En respuesta a lo anterior, las plataformas actuales, compuestas por tecnologías variadas y muchas veces propietarias, deben evolucionar hacia estructuras más flexibles, dinámicas y, sobre todo, integradas y optimizadas para manejo robusto de tráfico paquetizado.

El objetivo principal de este trabajo es proponer una tecnología de transporte digital que permita llevar a efecto la evolución de las tecnologías de transporte rentabilizando los recursos, migrando los servicios de manera transparente, y permitiendo la escalabilidad para soportar las nuevas demandas de ancho de banda y prestaciones. Otro de los objetivos es mejorar la operación, simplificando las tareas de gestión, habilitación, provisión y mantenimiento. Las etapas para lograr lo planteado son cuatro: estudio teórico de la recomendación G.ASON (*Automatic Switched Optical Network*) de la ITU (*International Telecommunication Union*) y del estándar GMPLS (*Generalized Multiprotocol Label Switching*) de IETF (*Internet Engineering Task Force*); análisis técnico de las redes y protocolos en operación para voz, datos y otros servicios; especificación y propuesta de prototipo a escala de la solución; y, ejecución práctica e implementación de la maqueta de prueba para validar su funcionamiento.

Este trabajo demuestra la aplicabilidad de ASON/GMPLS como nuevo estándar de transporte digital porque resuelve la problemática presente y capacidad para abordar los retos futuros: aumento drástico y escalable del ancho de banda; soporte de los servicios de manera transparente ya que es compatible con elementos multiservicios; fuerte crecimiento de los indicadores de disponibilidad de la red; simplificación de la provisión, habilitación, gestión y mantenimiento pues muchas de estas tareas son facilitadas por el plano de control distribuido de la tecnología ASON; y, explotación de la capacidad ociosa de enlaces, sin afectar la calidad de servicio comprometida. Además, este proyecto de título entrega un modelo conceptual, teórico y práctico para la implementación de ASON, aporta al conocimiento operativo de los dispositivos tecnológicos, contribuye a la creación de un plan de migración de las redes existentes y define requerimientos a exigir de los proveedores de equipos.

La tendencia futura apunta hacia aplicaciones IP. En el núcleo de red de transporte, ASON basado en SDH mantendrá la supremacía. Esta tecnología será fortalecida con sistemas de gestión altamente inteligentes que permitirán inventario, provisión y reorganización de circuitos de manera totalmente automatizada.

… a Tania, porque con su fuerza y amor, todo es alcanzable.

¡Gracias por luchar a mi lado, tu apoyo y desvelos juntos, son la base de nuestros logros!
Te amo.

TABLA DE CONTENIDO

TABLA DE CONTENIDO

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

1. INTRODUCCIÓN

1.1. AVANCES TECNOLÓGICOS, EL NEGOCIO Y LOS SERVICIOS

En la actualidad, los avances tecnológicos han permitido el desarrollo de nuevos y novedosos servicios los cuales han cambiado el negocio de las telecomunicaciones. Los clientes ya no están interesados en que se les brinde conectividad, lo que buscan es una oferta de productos que le aporte ventajas competitivas.

Desde la perspectiva tecnológica, existen cuatro tendencias destacables que impactan en el ejercicio de un operador de telecomunicaciones integrado: los nuevos desarrollos propician la interoperabilidad de los servicios y el interfuncionamiento de redes; los equipos terminales se están convirtiendo en el elemento en donde reside la inteligencia de las prestaciones; la red evoluciona mas allá de la conectividad para ofrecer, además, almacenamiento y proceso; y, se les exige a los sistemas informáticos una gestión adecuada para incrementar la oferta. Estos aspectos hacen necesario que las empresas de telecomunicaciones pongan especial atención en la identificación y combinación de las tecnologías que le permitan entregar una oferta coordinada de soluciones al cliente. Por lo tanto, la nueva estructura de la red es el resultado de factores tecnológicos, de negocio, de operación y sin duda lo será también de la regulación local.

La Tabla 1, resume estos factores:

Tecnología	Negocio	Operación	Regulación
-Arquitectura multicapa: Red(Transporte y control) + Servicios -Evolución de las tecnologías de acceso. -Evolución a "all IP" -Movilidad. -Los clientes desean conectividad, almacenamiento y proceso.	-Decrecen los servicios PSTN *(public switched telephone network)*. -Prestaciones combinadas (Voz + Datos + TV + …). -El acceso está íntimamente asociado a los servicios.	-Mayor facilidad en la operación. -Unificación de procedimientos para las distintas redes. -Rapidez en la implantación de servicios.	-Regulación en el acceso. -Regulación a nuevos servicios de carácter masivo.

Tabla 1.: Factores que intervienen en la estructura de las nuevas redes

Las tendencias en las transformaciones del modelo de red también influyen en las determinaciones de las empresas operadoras a la hora de optar por tecnologías. Es así como se he visto una evolución global tendiente a simplificar e integrar las redes, llevando drásticamente todo a IP y a una conmutación óptica automática basada en GMPLS.

En la Figura 1, se aprecia este perfeccionamiento.

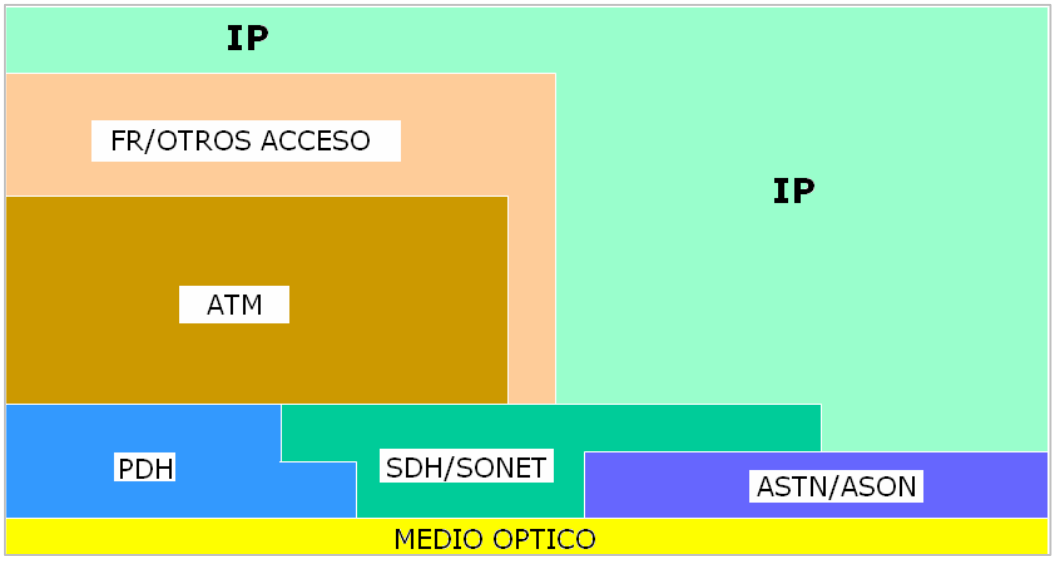


Figura 1.: Evolución hacia "todo IP", sobre una red ASON

1.2. LAS REDES Y SU ADAPTACIÓN A LOS NUEVOS SERVICIOS

La demanda por servicios de telecomunicaciones con valor agregado es creciente y se diversifica. Los volúmenes de tráfico de datos se incrementan. El mercado demanda la extensión de las Redes de Área Local. Los servicios de almacenamiento distribuido irrumpen con fuerza, sin embargo, hay que rentabilizar las cuantiosas inversiones realizadas en redes de fibra óptica y equipos de transporte, pues los precios de los servicios cada vez son más bajos. El gran problema es que las redes existentes no están orientadas a los nuevos productos. ¿Cómo evolucionarán estas estructuras para satisfacer la demanda con estos condicionantes?.., la solución inmediata es la adaptación de las redes actuales a las nuevas prestaciones con el fin de satisfacer: a) la demanda creciente de ancho de banda; y, b) El mercado emergente de servicios puramente ópticos. Por esto, se desarrollará la capa óptica para ofrecer transmisión y conmutación. En un plazo mayor, como resultado de la evolución de las redes de transporte, en especial su capa óptica y de los equipos de datos, se implementará la "Red óptica Inteligente", la que promete la flexibilidad y escalabilidad adecuadas para este nuevo escenario.

Los requerimientos para los cuales se diseñaron las redes actuales han cambiado como se muestra en la Tabla 2:

- **Ayer**	- **Hoy**
- Conmutación de circuitos - Transmisión de voz en canales de 64Kbps - Comportamiento de tráfico predecible	- Conmutación de paquetes - Datos en ráfagas de elevados anchos de banda - Comportamiento de tráfico impredecible

Tabla 2.: Comparación de requerimientos de la red

Actualmente existe una diversidad de redes dando servicios de manera independiente. Es posible encontrar estructuras de tecnología SDH, ofreciendo prestaciones de transporte a redes ATM, las que en definitiva llevan los servicios de un cliente final. Igual cosa pasa con equipos de ruteo IP, los cuales se conectan a equipos SDH como si se tratara de un camino de fibra. Estas implementaciones son ineficientes. Configuraciones como POS, Gigabit Ethernet y 10GEth, son ineficaces en la utilización de ancho de banda y no

garantizan los parámetros de calidad de servicio. Por lo tanto, se deben preparar las redes para la integración de las tecnologías y esto se debe realizar con miras a reutilizar las inversiones existentes.

Debido a que las grandes redes SDH actualmente soportan la mayor cantidad de tráfico telefónico y de datos (urbano, de larga distancia e internacional), cuentan con un alto grado de estandarización y garantizan calidad de servicio entre otras cualidades, deben, sin lugar a dudas, evolucionar para permitir esta demanda creciente de integración de Servicios, Operación y Gestión. Es por esto que se han definido los siguientes estándares, en cuya descripción, se utiliza terminología que es abordada con más detalle en el capítulo 2 de este trabajo:

-**GFP ("***Generic Framing Procedure"*): Adaptación de servicios de datos sobre la carga útil ("*payloads*") de SDH de forma flexible, robusta y con poco encabezamiento ("*overhead*"). Es capaz de preservar la información MAC ("*Media Access Control*"), por lo que soporta múltiples protocolos de nivel 2. Hay dos tipos de GFP: Transparente (GFP-T) y Basado en Tramas "*Framed-Based*" (GFP-F). GFP-T mapea toda la señal ("todos los bits, útiles o no") en tramas GFP de tamaño fijo, lo que hace que sea totalmente transparente, con tiempos muy bajos de latencia de transmisión de la señal y sencilla implantación pero con consumo de mayores anchos de banda. GFP-F sólo mapea los bytes de las tramas de la señal a transmitir, por lo que hace un mejor uso del ancho de banda. Sin embargo, sólo es capaz de soportar protocolos orientados a tramas, con adaptación particular para cada uno de los protocolos soportados.

-**VCAT** ("*Virtual Concatenation*"): Mecanismo para que las señales ocupen varios contenedores SDH virtuales no contiguos ajustados a su ancho de banda, en vez de un único contenedor de tamaño bastante superior. Estos contenedores pueden transportarse de forma independiente por la red y ser reensamblados en el destino, usando más eficientemente la red (trazado flexible de rutas, aprovechando toda la capacidad existente).

-LCAS. ("*Link Capacity Adjustment Scheme*"): Permite la reconfiguración dinámica de los contenedores virtuales que transportan los datos. Facilita, en tiempo real y de forma automatizada, añadir o eliminar ancho de banda adicional a un "circuito VCAT" sin afectar a los datos transmitidos. Opera de forma simétrica y asimétrica (diferentes velocidades en los dos sentidos de transmisión del circuito).

-**RPR** ("*Resilient Packet Ring*") Protocolo de nivel 2 para proporcionar un servicio de transmisión de paquetes no orientado a la conexión entre elementos de un anillo SDH. El objetivo de diseño es "Ethernet con calidad de servicio SDH". Sus principales características son: soporta múltiples servicios y aplicaciones (datos, voz, vídeo); topología de doble anillo (interior y exterior) ambos con tráfico útil; usa técnicas de nivel 2 para protección de tráfico y no reserva ancho de banda para este fin; descubrimiento automático de nodos y topología de red. Cada nodo de red almacena dos caminos (primario y secundario) al resto de nodos de la red. Conmutación automática a secundario en caso de fallo en menos de 50 mseg.; "Reutilización espacial". Los paquetes no circulan por todo el anillo, sino simplemente en el tramo comprendido entre emisor y receptor; todos los nodos comparten el ancho de banda disponible, sin necesidad de provisionar circuitos, negociando el acceso de forma equitativa; implanta de forma simple la funcionalidad de "*multicast*" y "*broadcast*", ya que los paquetes pueden circular por el anillo sin necesidad de replicarlos; implanta cuatro clases de servicio con diferentes prioridades en cuanto a garantías de ancho de banda, retardo y "*jitter*" (Reservado y clases A, B y C); arquitectura de "camino de paso o en tránsito" que permite a los paquetes cruzar rápidamente los nodos intermedios. Valores muy bajos de latencia y "*jitter*"; y, permite "sobre-suscripción" (multiplexación estadística), garantizando un valor comprometido, y a partir de ahí en función del estado de ocupación de la red.

1.3. CASO ILUSTRATIVO DE LOS CAMBIOS EN EL NEGOCIO

Como ejemplo de este planteamiento y de la necesidad de evolucionar las redes hacia la integración de servicios se presenta este caso: Hoy en día existen importantes clientes que son contrarios a la contratación de enlaces a nivel de capa 3 (según modelo de referencia OSI de la ISO) a empresas externas. Los bancos e instituciones financieras esgrimen razones de seguridad para limitar el acceso a sus redes corporativas. La solución que ellos están dispuestos a comprar son servicios de capa 2, es decir, se les vende un medio físico para que puedan conectar sus distintas dependencias. Las exigencias de estas corporaciones pueden ser muy variadas en cuanto a requerimientos de ancho de banda, área de cobertura y confiabilidad del enlace. Por lo tanto, cada servicio contratado tiene necesidades particulares que exigen una solución a la medida.

A continuación se describen los servicios que están soportados sobre redes de acceso ADSL y G.SHDSL. Generalmente estos servicios se ofrecen en forma asimétrica. En los puntos de acceso se instala un CPE (Equipo Local del Cliente) que establece una conexión ATM para transmitir la información. Cuando el cliente se conecta a Internet es mucho más el tráfico de bajada (desde la red al cliente) que el tráfico de subida. Considerando eso, en la red ATM todos los perfiles de usuario se configuran en forma asimétrica. Para el caso que se está analizando, la necesidad es distinta. El cliente no está comprando una conexión a Internet, sino que desea unir todas sus dependencias en una sola red. Un enlace asimétrico no le sirve. Esto supone varias dificultades, ya que algunos equipos no soportan servicios simétricos (la mayoría de los modelos de CPE disponibles sólo lo hacen a tasas de transmisión inferiores a 512 kbps). Por lo que es necesario cambiar los equipos instalados a otros de nueva generación (G.SHDSL).

Para el resto de los equipos fue necesario definir y probar nuevos perfiles de usuario. Un sólo enlace pasa por muchos equipos de distintos proveedores: concentradores (DSLAM),

routers y equipos de transmisión ATM y SDH ("*Synchronous Digital Hierarchy*" – Jerarquía Digital Sincrónica), cada uno con sus propios parámetros de configuración. La Figura 2, muestra un esquema de cómo sería un enlace para este tipo de servicios con todos sus elementos: CPE (que toma los paquetes IP y los convierte en celdas ATM), luego está el DSLAM (que concentra las celdas de muchos clientes), después están los equipos RTBA (equipos SDH que soportan señales ATM), le sigue la red ATM propiamente tal y finalmente se hace la conversión a IP en la casa matriz del cliente.

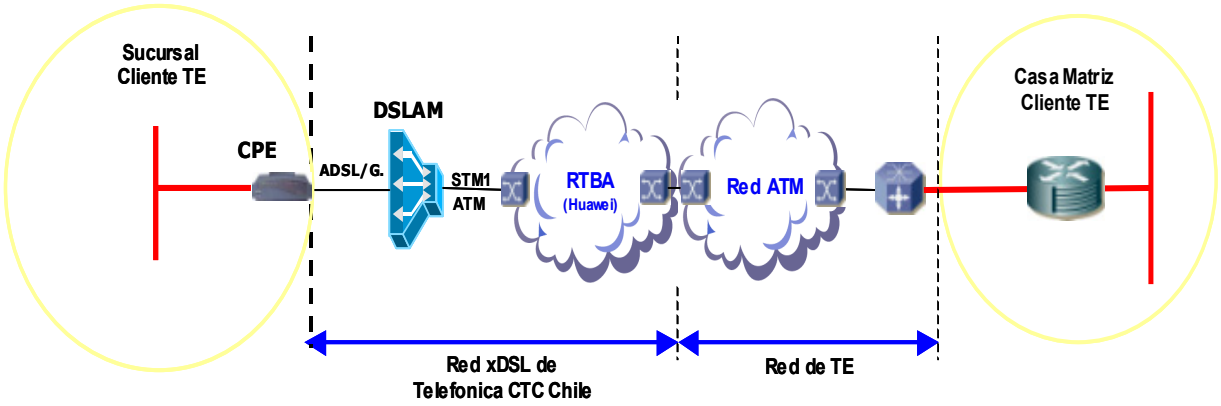


Figura 2.: Esquema de enlace simétrico para un cliente

Esta alternativa funciona para la mayoría de los clientes. Permite garantizar un determinado ancho de banda, pero sólo funciona a tasas bajas de transmisión. Este servicio utiliza la infraestructura ya instalada (la red de par de cobre telefónico), y por lo tanto, está limitado a 2 Mbps como máximo. Para aquellos clientes que necesitan más ancho de banda hay que invertir en toda una infraestructura nueva. La única alternativa factible es usar un enlace ethernet. Esta tecnología existe desde hace varias décadas, pero sólo en el último tiempo a despegado como la opción para aquellos clientes que requieren enlaces dedicados de gran capacidad.

Considerando sus costos bajos y gran versatilidad (es uno de los protocolos más extendidos) a experimentado un aumento explosivo en cuanto a número de clientes y área de cobertura. Durante una época se usaban los conversores LAN/E1 y V.35/E1 para llevar tráfico de datos a los clientes, pero usaban pares de cobre que los limitaban 2 Mbps. Con la aparición de los conversores electro/ópticos, que toman una señal eléctrica y la suben a una

fibra óptica, se rompió con esa limitación y, gracias a la fibra, se amplió dramáticamente el alcance de las redes. Ahora que se podía llegar a cualquier parte es necesario replantear la topología de la red. Tradicionalmente se tenía un *switch* al que llegaban muchos clientes vía fibra óptica. Eso significaba un gran gasto en fibra y en puertos ethernet, por lo que ambos comenzaron a escasear. Se hacía necesario acercar a los clientes los puntos de concentración de la fibra, de esa forma, una vez entroncados los servicios, bastaba un par de fibra y un puerto ethernet para completar el enlace. La Figura 3 ilustra ese escenario. Primeramente los clientes se conectaban directamente a la red IP o vía fibra óptica. Ahora se conectan a la nueva red RTBA(Red de Transporte de Banda Ancha) para llegar a la red IP. Igual se usa fibra, pero en tramos mucho más cortos.

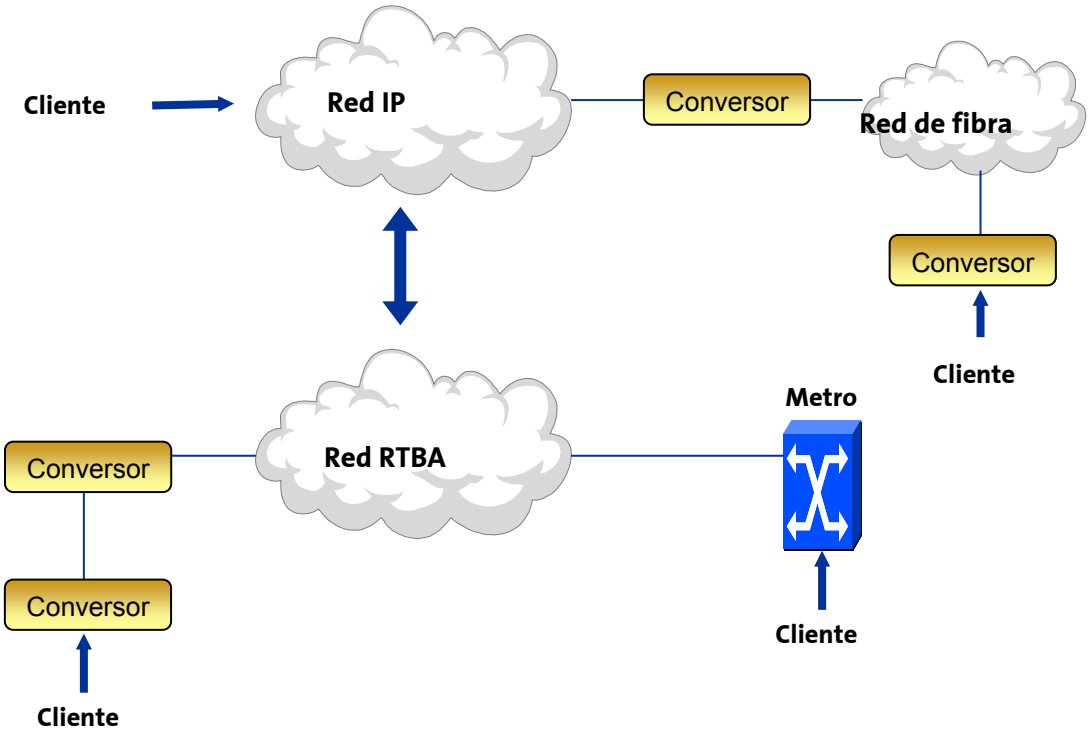


Figura 3.: Servicio ethernet a clientes

La alternativa de concentrar clientes usando los equipos de la Red RTBA es atractiva por dos razones: primero por su bajo costo; y segundo, porque son equipos SDH. En efecto, al ser equipos SDH (que soportan señales ethernet) pueden usar la infraestructura ya existente. La tecnología SDH nació para transportar el tráfico telefónico. De hecho, donde

hay una central telefónica, hay un equipo SDH. Se puede afirmar que la tecnología SDH es, después de la red de voz conmutada, la red de más amplia cobertura en Chile. Esta red SDH contaba con ancho de banda no utilizado, y ya no era atractiva para los clientes que habían descartado la utilización de los conversores LAN/E1. Con estos equipos Metro era posible utilizar este ancho de banda. Ahora se podían entregar enlaces ethernet de gran capacidad sin invertir en fibra. Para ser una tecnología aplicable estos equipos Metro debían tener todas las prestaciones de los *switch* convencionales: manejo de VLAN y configuración de las interfaces (10 mbps, 100 mbps, *full-duplex, half-duplex*). Pero al ser SDH se sumaba una ventaja que la tecnología ethernet pura no podía entregar. Ahora era posible garantizar un determinado ancho de banda para cada servicio. Una LAN es una red que funciona al mejor esfuerzo, no puede garantizar una calidad de servicio en caso de congestión o saturación de tráfico. Los equipos Metro en cambio, mapean las señales ethernet dentro de una trama SDH, reservando dentro de ésta, canales de datos para cada servicio. Se abre entonces una nueva forma de vender servicios de capa 2, de gran capacidad y gran confiabilidad.

1.4. ETAPAS PARA LA MIGRACIÓN

Sin duda los nuevos elementos de NGN ("*Next Generation Network*"), han ayudado a integrar soluciones finales para clientes. El desafío es ahora, llevar la red al plano óptico con el objetivo de incorporar en el corazón de esta, un plano de control eficiente, escalable y seguro.

Para realizar lo anterior es necesario definir las arquitecturas y soluciones de red, sus directivas de evolución y requisitos para troncales que permitan ofrecer los servicios "extremo a extremo" actuales y futuros. Evidentemente, se aplicarán los procedimientos probados por los proveedores de equipos, ajustando lo esencial para cubrir las necesidades y objetivos del trabajo. La metodología se dividirá en tres etapas: identificación de las tecnologías actuales, con un proceso de caracterización de los servicios y las plataformas que le dan soporte; estudio de los protocolos y elementos de ASON/GMPLS, que dará el marco teórico necesario para consolidar servicios; y, migración de las redes en la maqueta

de prueba, que va desde la actual situación de redes separadas, a servicios sobre NGN con un núcleo óptico inteligente.

2. EL PRESENTE DE LAS REDES FIJAS Y SU EVOLUCIÓN HACIA LA INTEGRACIÓN DE SERVICIOS

2.1. DESCRIPCIÓN DEL CAPÍTULO

En esta parte, se hará una descripción de las actuales tecnologías de transmisión y los servicios que estas soportan, en particular, el estándar **SDH** ("*Synchronous Digital Hierarchy"*) para comprender las funcionalidades de las actuales redes y los cambios que debe sufrir en su evolución. Se revisan los nuevos conceptos de sistemas de la **ITU-T**("*International Telecommunication Union – Telecommunication Standardization Sector"*) para redes ópticas contemplados en su recomendación **G.8080/Y.1304** para **ASON** ("*Automatic Switched Optical Network"*), y el protocolo **GMPLS ("***Generalized Multi-Protocol Label Switching"*) impulsado por la **IETF**("*Internet Engineering Task Force"*) en su **RFC-3473**, y finalmente, se da una revisión conceptual de los impactos de la implementación en transporte digital urbano.

2.2. VISIÓN DE LAS REDES Y LOS NUEVOS PARADIGMAS QUE ENFRENTAN

2.2.1. LAS ACTUALES REDES DE TRANSMISIÓN: SDH

2.2.1.1. GENERALIDADES

La mayor parte de la infraestructura para transmisión masiva de datos esta basada en sistemas SDH. Es necesario integrar la gran cantidad de equipamiento disponible en los esquemas modernos de red, y, para esto, se debe conocer el funcionamiento general de dichos elementos.

SDH es un estándar internacional para sistemas ópticos de telecomunicaciones de altas prestaciones. Esta red, por su característica sincrónica, está optimizada para manejo de anchos de banda fijos, lo que la ha convertido en el medio natural para la transmisión de

telefonía tradicional. Este estándar culminó en 1989 en las recomendaciones de la ITU-T G.707, G.708, y G.709 que definen la Jerarquía Digital Síncrona. En Norte América, ANSI publicó su estándar **SONET. (Red óptica síncrona).** Las recomendaciones de la **UIT-T** definen un número de tasas básicas de transmisión que se pueden emplear en **SDH**. La primera de estas tasas es 155.52 Mbps, normalmente referidas como un **STM-1** ("*Synchronous Transport Module – Level 1*"). Mayores tasas de transmisión como el **STM-4**, el **STM-16**, **STM-64** y STM-256 (622.08 Mbps, 2488.32 Mbps, 9953.28 Mbps y 39813.12 Mbps respectivamente) están también definidas. El protocolo además permite manejar señales de mas baja jerarquía como las provenientes del estándar PDH ("*Plesiochronous Digital Hierarchy*") por medio de puertos tributarios adecuados La formación de la señal sincrónica es la que se muestra en la figura 4.

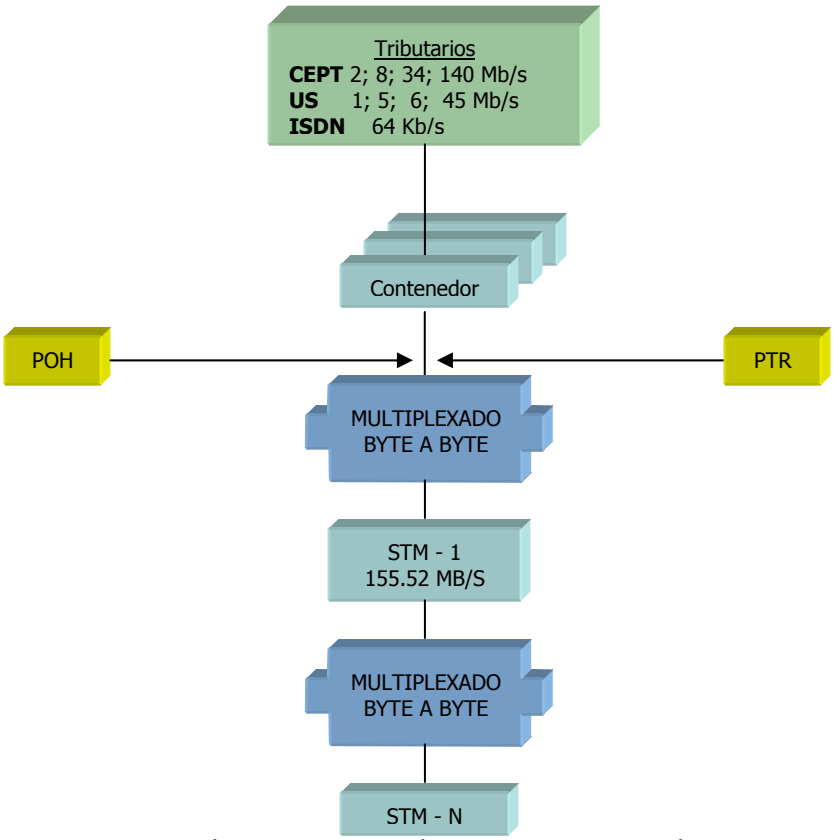


Figura 4.: Formación de la señal sincrónica a partir de jerarquías menores

Los tributarios (sincrónicos o plesiócronos) se acomodan en un contenedor C (Container) especifico. A cada contenedor se le agrega un encabezado o sobrecapacidad de

reserva llamada POH ("*Path Overhead*") para operación, administración y mantenimiento, y un puntero, PTR para identificación, formándose lo que se conoce como unidad tributaria TU ("*Tributary Unit*"). Finalmente las TU son multiplexadas byte a byte (cada uno equivale a 64kb/s) y con el agregado de información adicional de administración de la red, se forma el módulo STM-1. Las jerarquías superiores STM-N, se volviendo a multiplexar byte a byte N módulos STM-1.

2.2.1.2. SINCRONIZACIÓN

SDH nace de la necesidad de extender a velocidades superiores, la trama sincronía de 2 Mbps de los sistemas PDH. La trama de 2Mb/s es síncrona. Lo que esto significa es que los intervalos de tiempo son sincrónicos al encabezamiento de la trama: una vez sincronizado a la trama, un receptor puede extraer la información contenida en la trama sencillamente contando bytes hasta llegar a la posición deseada y copiando los bytes allí contenidos en memoria. Para insertar información en un intervalo de tiempo, el procedimiento sería igualmente sencillo: una vez alineado a la trama, el transmisor puede transferir los datos de memoria al intervalo de tiempo adecuado, el cual encuentra contando los bytes desde los bits de alineación de trama. La trama de 2Mb/s es sincrónica con sus tributarios de 64kb/s (cosa que no sucede con las tramas de 8, 34, 140 o 565 Mb/s). En la práctica ocurre que estos tributarios no siempre son sincrónicos y las centrales de conmutación y los *cross-connects* tienen que periódicamente introducir deslizamientos o *slips* cada vez que haya un defasaje grande entre carga que ingresa a la memoria elástica a la entrada del MUX y la señal multiplexada de 2Mb/s.

La velocidad con que llegan y se escriben en las memorias elásticas los datos de cada canal es determinada por la velocidad de línea de la trama recibida. La velocidad con que se leen los datos se encuentra condicionada por el reloj interno de la central o *cross-connect*, con el cual generan las tramas que transmiten. Si la información a la entrada llega más rápidamente de lo que puede ser leída, la memoria elástica se llena hasta desbordar. Para

evitar el desborde, el nodo de la red, descarta uno o varios octetos de información, vaciando la memoria elástica y permitiendo que nuevamente se comience a llenar. Esta acción corta un trozo de la secuencia de bytes transmitidos, constituyendo un **slip negativo**.

Puede darse el caso contrario. Si el reloj de escritura es más lento que el de lectura, la tendencia de la memoria elástica es a vaciarse. Cuando esto ocurre el nodo de la red deja de leer información reciente, transmitiendo uno o varios octetos viejos sin borrar el contenido de la memoria elástica, que de esta forma se vuelve a llenar. Estas repeticiones se llaman **slips positivos**. Los deslizamientos normalmente no son perjudiciales para las señales de voz, sin embargo pueden traer problemas en la transmisión de datos. Para manejar esta situación heredada de los sistemas PDH, la carga se acomoda en contenedores. Cuando esta carga es plesiócrona, es necesario adaptar el reloj de la carga al reloj de los contenedores. El procedimiento es similar al utilizado en los MUX PDH. La capacidad de carga es ligeramente superior a la necesaria. Estos contenedores disponen de bits adicionales que pueden o no contener información, así como bits que indican si en esas posiciones va o no información, es decir se utiliza justificación por bits (relleno adaptable). Una vez creado el contenedor en los **multiplexores de frontera**, la red ya no tiene que mirar dentro del mismo hasta el punto en el cual el contenido es devuelto a un elemento de la red. Como ya se dijo, el ajuste de velocidades de los contenedores entre nodos se hace a través de los punteros.

Cada uno de los contenedores creado recibe un encabezamiento, llamado **tara de trayecto** (TTY o POH). El POH contiene información para uso en los extremos del trayecto (canales de servicio, información para verificación de errores, alarmas, etc.). Los punteros apuntan al primer byte del encabezamiento de trayecto. Los contenedores a los cuales se ha agregado su POH se llaman **contenedores virtuales** VC ("*Virtual Container*"). Cada uno de los VC es transportado en un espacio al cual está asignado un puntero, que indica el primer byte del VC respectivo. Las señales tributarias (como puede ser una de 140 Mb/s) se

disponen en el VC para su transmisión extremo a extremo a través de la red SDH. El VC se ensambla y desensambla una sola vez, aunque puede atravesar muchos nodos mientras circula por la red. Los punteros correspondientes a cada contenedor se encuentran en posiciones fijas respecto al elemento de multiplexación en el cual los contenedores son mapeados. Los VC bajos (de jerarquías bajas) son mapeados en relación a contenedores más altos. Los VC altos son mapeados en relación a la trama STM-N. Por lo tanto los contenedores altos contienen también un área de punteros para los VC bajos (llamados unidades tributarias). Está claro que si en lugar de tributarios bajos los VC reciben señales digitales SDH, ellos no contienen ningún área de punteros, porque no hay unidades tributarias a localizar dentro de los mismos, sino que su área de carga está ocupada por una gran señal sincrónica. Los VC altos que son mapeados en relación a la trama STM-N son llamados **unidades administrativas** (AU). Por lo tanto, la trama STM-N siempre contendrá un área de punteros para las unidades administrativas.

El contenedor define la capacidad de transmisión sincrónica del tributario. La frecuencia de éste se incrementa mediante justificación positiva para acomodarla y sincronizarla con STM-1. Al agregar la información adicional POH se forma lo que se denomina contenedor virtual VC (Virtual Container). Posteriormente se agrega el puntero PTR, que es el direccionamiento de cada VC dentro de la estructura, obteniéndose la unidad tributaria TU. El proceso puede observarse en la figura 5.

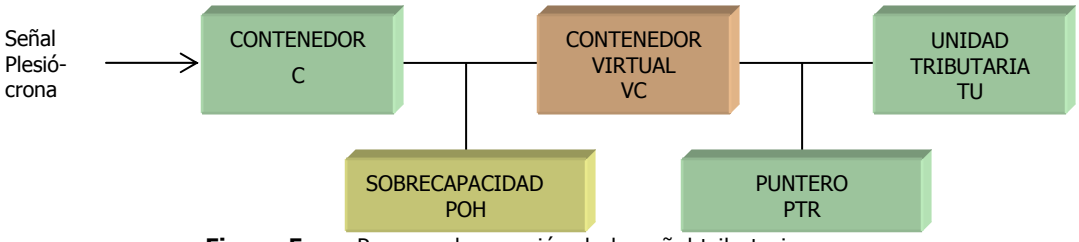


Figura 5.: Proceso de creación de la señal tributaria

Este conjunto constituye una unidad interna de la estructura. En caso que pueda ser transferida entre distintos STM-1, se denomina unidad administrativa AU ("*Administrative Unit*"). Varias TU idénticas, forman un grupo de unidades TUG ("*Tributary Unit Group*").

Varios TUG idénticos forman nuevamente una AU, la que con el agregado de un encabezado de sección SOH ("*Section Overhead*") con la información de operación, administración de la red, completa el STM-1. En la figura 6 se grafican las distintas alternativas para obtener un módulo STM-1 a partir de múltiples señales tributarias.

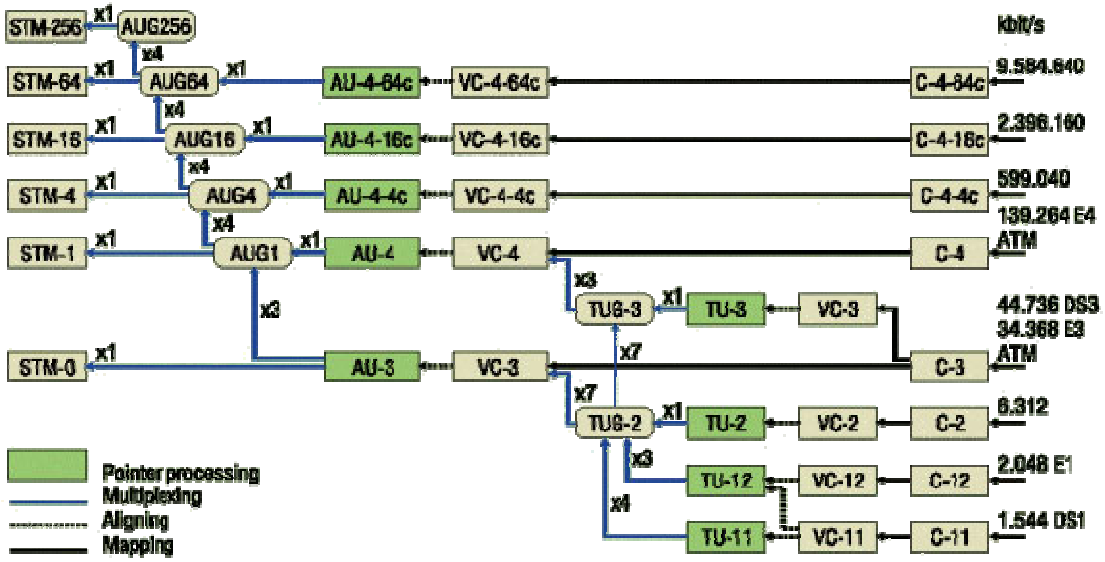
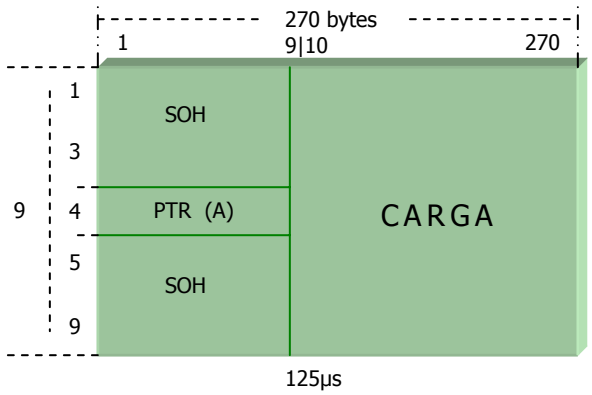


Figura 6.: Alternativas para la obtención de señales SDH

2.2.1.3. SDH: ESTRUCTURA DE LA TRAMA SINCRÓNICA

Una trama de flujo de señales serie puede representarse matricialmente, con N filas y M columnas. Cada celda representa un byte de 8 bits de la señal sincrónica. La estructura de la trama del módulo de transporte sincrónico STM-1 es la que puede observarse en la figura 7:



En general, la carga transportada no es síncrona con la trama. Para corregir esto, existe un puntero que entrega la ubicación de la data útil dentro del contenedor virtual
El espacio de carga síncrono, se denomina TU ó AU.
(Se denomina AU cuando la zona de carga es síncrona con la trama)

Figura 7.: Estructura de la trama STM-1

Un ejemplo sería una señal PDH de 140Mb/s transportada en un VC-4 que alineado usando punteros en la AU-4. Se dice TU cuando el espacio de carga es síncrono a un VC de orden superior (VC-3 ó VC 4). Por ejemplo, 63 señales de 2Mb/s mapeadas en contenedores VC-12 alineadas en TU-12 (los que a su vez se agruparán en un VC-4). La trama la forman 9 líneas (o secuencias) de 270 bytes cada una. La secuencia de transmisión se inicia en el byte 1 de la línea 1 hasta el byte 270 de la misma línea, luego el byte 1 de la línea 2 y así sucesivamente hasta el byte 270 de la línea 9. La duración total (período de la trama) es de 125µs (o sea una velocidad de 155.52Mb/s). Este período es equivalente al de la trama de una canal PCM de 8 bits. O sea que un byte se STM-1 podría ser una canal PCM (64kb/s). Como para componer la jerarquía sincrónica se realiza intercalación de bytes, siempre es posible extraer en cualquier nivel el byte completo (por ejemplo un canal PCM).

2.2.1.4. SECCIONES DE LA RED SDH

La trama SDH transporta dos tipos de datos: las señales tributarias y las señales auxiliares de la red, denominados encabezado global. El encabezado global aportan las funciones que precisa la red para transportar eficazmente las señales tributarias a través de la red SDH.

Se dividen en tres categorías: encabezado trayecto; encabezado de sección multiplexora; y, encabezado de sección regeneradora. La razón de estos encabezados se relaciona con los distintos segmentos de una red SDH como se puede observar en la Figura 8.

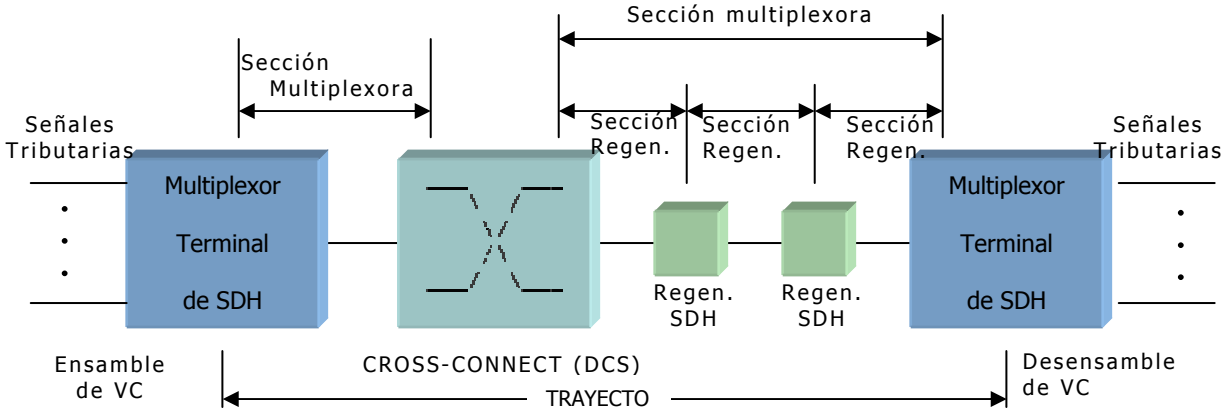


Figura 8.: Secciones de una red SDH

La ruta de transmisión consta de tres segmentos: el trayecto, la sección multiplexor y la sección regeneradora. Cada segmento aporta su propio encabezado que incluye las señales de soporte y mantenimiento asociadas a la transmisión a través de dicho segmento.

El trayecto de una red SDH es la conexión lógica entre el punto en el que se ensambla en su contenedor virtual y el punto en el que se desensambla desde el contenedor virtual.

2.2.1.5. ESQUEMAS DE PROTECCIÓN

La gran capacidad de los enlaces SDH hace que una simple falla tenga un impacto altamente 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.

2.2.1.5.1. Terminología Básica

-Subred: Una única red puede ser vista como la interconexión de múltiples subredes. Un anillo es un simple ejemplo de subred. Estas subredes pueden estar organizadas en diferentes áreas geográficas o a través de diferentes operadores.

-Supervivencia: Una red puede ser descrita como superviviente si no hay un punto singular de fallo entre dos nodos. La provisión de una ruta principal y otra alternativa entre dos nodos finales de la red significa que la red es superviviente en presencia de un punto de fallo único.

-Disponibilidad: Es la medida de la proporción de tiempo que la red está disponible para proporcionar servicios al cliente final. Indica con que frecuencia o consistencia la red puede proporcionar funciones de transporte en los cuales el servicio requerido es perfectamente empleable por el cliente final. Como esto es importante para el cliente, este factor contribuirá a la definición de nivel de servicio garantizado (SLA – "*Service Level*

Agreement"). El SLA es típicamente medido como un porcentaje de tiempo de una conexión en funcionamiento. Esto da cuenta de la supervivencia de una red, de la tasa de fallos de sus componentes y de los tiempos de reparación. Este término refleja la calidad de servicio promedio que un cliente final puede esperar de un operador.

Para conseguir esta disponibilidad podemos tomar alguno de los siguientes caminos:

- 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, sistemas de reloj, o unidades tributarias pueden ser duplicadas. Una tarjeta en fallo será reemplazada por su protección automáticamente donde este esquema de protección esté presente.

- **Resistencia de red**: Para incrementar la supervivencia de la red y por tanto la disponibilidad, los enlaces de red pueden ser protegidos. Procedimientos son aplicados para asegurar que el fallo de un enlace de transporte sea reemplazado por otro enlace en producción y que hay un camino alternativo ante la existencia de un fallo total de un nodo.

Hay dos tipos de mecanismos utilizados para asegurar que el servicio pueda ser recuperado de esta manera:

- **Restauración**: Esto es un proceso lento automático o manual la 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**: En contraste, 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 preasignada entre nodos y es preferible a la restauración porque la capacidad de reserva siempre estará disponible pudiendo ser accesible mucho más rápido.

2.2.1.5.2. Causas de Fallo

Las fuentes físicas de fallo en redes de transmisiones SDH pueden ser clasificadas en las siguientes categorías:

- Fibras y cables: La principal causa de fallo de fibras y cables es el daño causado por agentes externos como los trabajos de ingeniería civil y los efectos del entorno como rayos o terremotos.

- Equipamiento: puede fallar debido a efectos del envejecimiento, forzado de componentes o la aparición de humedad. Rigurosas pruebas son, de todos modos, realizadas normalmente para eliminar anomalías en el estado del equipamiento.

- Fallos de alimentación apagan el nodo cuando aparecen y que están fuera del control del operador. Los sistemas principales son provistos de reservas mediante sistemas de alimentación secundarios, pero los efectos transitorios en la señal pueden ocurrir mientras se conmuta al sistema de back-up.

- Mantenimientos: Mantenimientos no programados y errores realizados durante el mantenimiento pueden afectar a la disponibilidad del servicio.

- Desastres causados por la acción del entorno o humana, generalmente de gran alcance y con severos efectos, tales como la destrucción de componentes principales de la red.

2.2.1.5.3. Protección de Equipamiento

Los objetivos de calidad son establecidos para los elementos en una red SDH y esto afecta a la medida de disponibilidad de esta. Para alcanzar los requerimientos de disponibilidad es necesario en ocasiones duplicar módulos en los elementos. Cada componente de los elementos de red tiene asociado una tasa de fallo con él. Esto es usado junto con la información contemplada de interacción de componentes para calcular la tasa de fallos para tarjetas de circuitos. De manera similar las tasas de fallos de las tarjetas y la información de interacción son usadas para calcular la tasa de fallo de los elementos de red. Tomando en cuenta los tiempos de reparación y los fallos de software, se calcula una medida general de disponibilidad para los elementos de red. La disponibilidad puede ser mejorada

aprovisionando un componente en espera ("*stand-by*") empleable en caso de fallo. Esta protección local es comúnmente aplicada en algunas unidades como son las de alimentación, generación de reloj, matriz de cross-conexión y tarjetas tributarias. Así, una tarjeta tributaria puede ser provisionada en stand-by en un elemento de red. Ante un evento de fallo de la tarjeta tributaria que se encuentra trabajando, el tráfico es automáticamente conmutado a la tarjeta de reserva de modo que no haya una interrupción de servicio para el usuario final.

Fallos de tarjetas no son la única razón para protección de tributarios. Las tarjetas de reserva también pueden ser usadas durante rutinas de mantenimiento. El tráfico puede ser manualmente conmutado a la tarjeta de backup mientras la tarjeta primaria sigue funcionando. Esto también posibilita que la tarjeta en servicio sea actualizada mientras el elemento de red está en servicio sin interrupción de servicio al usuario final. Hay diferentes esquemas estándar para protecciones de equipamiento. Por ejemplo, si una tarjeta en stand-by se incluye por cada tarjeta en funcionamiento, estas tarjetas tienen protecciones 1+1. Es también común provisionar una tarjeta de protección para diversas tarjetas operativas. Ante un evento de fallo en alguna de las tarjetas en producción, el tráfico es normalmente conmutado hacia la tarjeta de protección. A este sistema se le denomina protección **1:n**.

Por ejemplo, en un multiplexor STM-16, la protección 1:16 podría ser implementada en tarjetas tributarias STM-1. Dieciséis tarjetas STM-1 eléctricas podrían ser instaladas en el armario para soportar a los dieciséis tributarios STM-1. Una decimoséptima tarjeta podría ser instalada como tarjeta en *stand-by*. Ante un evento de fallo en una de las tarjetas STM-1, el tráfico puede ser conmutado a la tarjeta en *stand-by* de protección. La protección de equipamiento incrementa la disponibilidad de los elementos de red individuales pero no protege el sistema contra pérdidas de elementos de red enteros. Para asegurarse que el tráfico puede ser reenrutado si un elemento de red es perdido, los esquemas de protección

han de implementarse para incrementar la supervivencia de la red. La resistencia de la red frente a la protección local de equipamiento es requerida para proteger contra fallos de un nodo o pérdida de un enlace.

2.2.1.5.4. Restauración

La restauración concierne a la disponibilidad de rutas de servicio extremo a extremo. Trabaja a través de la red entera y reenruta tráfico para mantener el servicio. Un porcentaje de la capacidad de la red es asignado para la restauración. Después de la detección de una pérdida de señal, el tráfico es reenrutado a través de la capacidad de repuesto. Los algoritmos de reenrutamiento son programados en el software de los elementos de red. El camino alternativo puede ser buscado descartando tráfico de menor prioridad o usando capacidad extra entre nodos. En contraste con los procedimientos de protección de equipos, la capacidad usada para restaurar necesita ser preasignada. En algunos esquemas de protección, un enlace es dedicado como enlace de protección para los enlaces en producción. Éste no es el caso de la restauración, donde la capacidad libre puede ser compartida. Así, esta estrategia ofrece gran flexibilidad, presentándose un considerable número de opciones de reenrutamiento, por lo que los algoritmos son relativamente complejos. El tiempo de procesamiento necesario para encontrar una ruta de tráfico alternativo se presenta como una dificultad para la rápida restauración del tráfico afectado. También se ha de tener en cuenta que la restauración es iniciada únicamente tras la detección de pérdida de señal por parte del sistema de gestión de red, no cuando el fallo ocurre. Esto lleva a que los tiempos de restauración sean relativamente lentos, del orden de segundos o minutos hasta horas. Este proceso se relata a continuación:

-Se detectan alarmas de la red por medio del sistema de gestión.

-Se analizan las alarmas para determinar su causa.

-Conexión de la subred alternativa para restaurar el camino

-Camino implementado por cambio de conexiones.

-Camino validado.

En una red protegida, los elementos detectan un fallo tan pronto como ocurre y toma acciones correctivas de acuerdo con los procedimientos predefinidos, sin instrucciones del sistema de gestión de red. Restauración es un proceso lento y hace que la disrupción de servicio experimentada por el cliente final sea grande. Por el contrario, en un esquema de protección automática como es la Protección de la Sección de multiplexación (MSP) o MS-SPRing, el tráfico es reenrutado en menos de 50ms, así que el cliente final no detecta deterioro de servicios.

2.2.1.5.5. Protección de Red

Los procedimientos de protección de red son empleados para auto-recuperarse de fallos 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 muchos mecanismos de protección definidos por los organismos de estandarización. Estos esquemas 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.

2.2.1.5.6. 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 porta 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 hecha por el nodo de salida de la mejor de las dos conexiones. El mecanismo puede ser aplicado a anillos y también circuitos punto a punto a través de redes malladas o mixtas mediante muchos elementos de red y subredes intermedias.

2.2.1.5.7. Protección de Conexión de Subred (SNCP)

SNCP es similar a caso anterior, pero en el cual, el camino de protección dedicado involucra conmutación en ambos extremos, 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 respaldo 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 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 porque permite a la red sobreponerse a dos fallos simultáneos cosa que el camino de protección no tolera. En principio, el camino de protección extremo a extremo parece tener mucho atractivo; una amplia protección en redes de este tipo es posible y las rutas individuales pueden ser selectivamente protegidas. Aun así, es requerido un complejo control que asegure realmente diversas rutas. La Figura 9 muestra la forma en que opera:

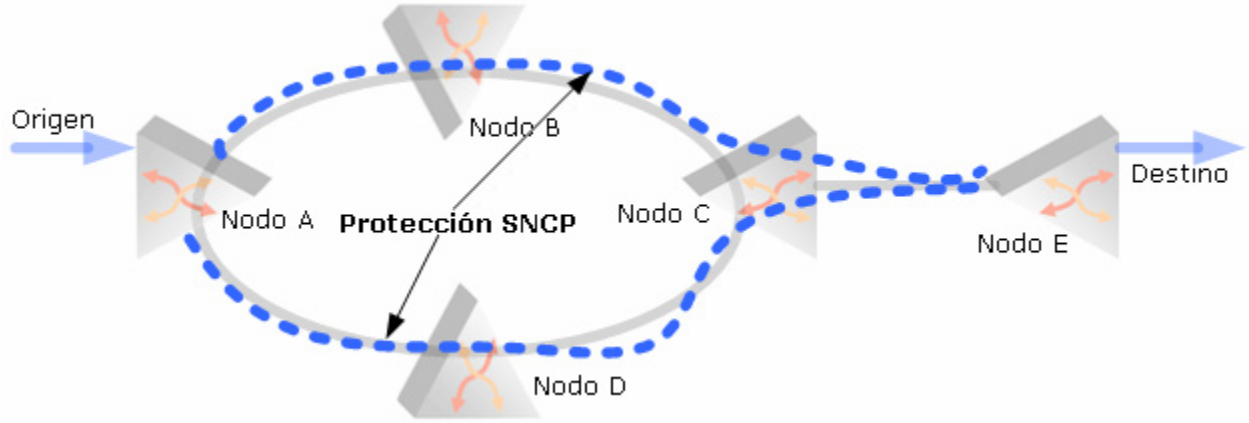


Figura 9.: Protección SNCP de trayecto

Una gran cantidad de capacidad de tráfico es usada y es muy difícil de coordinar actividades de mantenimientos programados a lo largo de la red. **SNCP** trabaja especialmente bien sobre anillos, porque se aseguran diversas rutas de fibra. 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 contratada, 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.

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**).

2.2.1.5.8. Protección de Línea de la Sección de Multiplexación

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 varios tipos 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.

- 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.

- 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 *stand-by* no puede ser utilizada para otro tráfico presentando unos altos requerimientos de capacidad de fibra.

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. En la Figura 10, se ilustra esta situación:

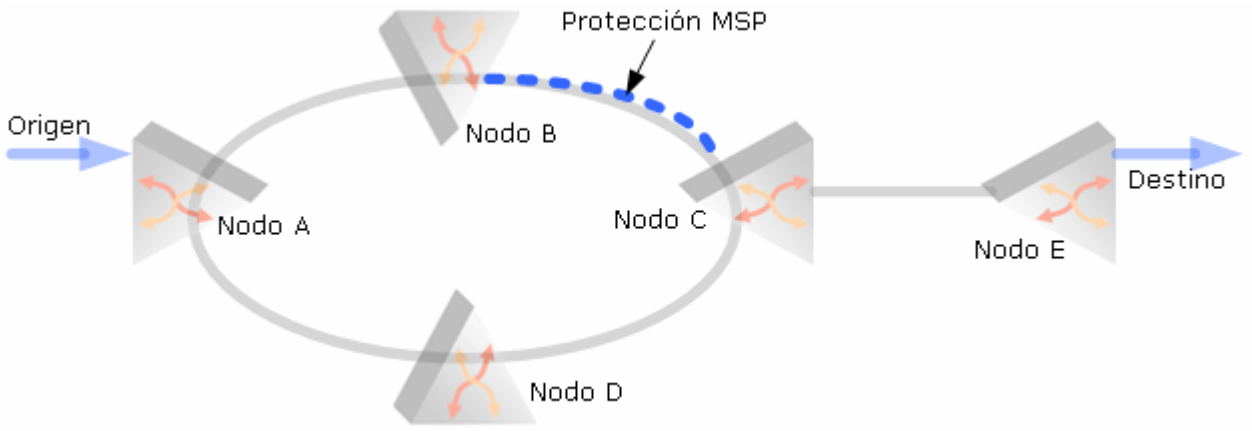


Figura 10.: Protección MSP de sección

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.

2.2.1.5.9. 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. Estos 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 unidireccionales y

bidireccionales. Dos tipos de mecanismos de anillos auto-recuperables serán considerados, puesto que son los más comúnmente desplegados en el mercado ETSI:

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

- Anillos bidireccionales de protección compartida (SPRings).

2.2.1.5.9.1. Anillos de protección dedicada

Son un tipo de protección de ruta dedicada, 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 ruta de trabajo "W" y la otra dirección el camino de protección "P". El nodo receptor seleccionara la señal de mayor calidad. Por ejemplo se asume que la mejor calidad es la de la señal "W"; ante un evento de rotura de fibra óptica entre A y B en "W", el Nodo B seleccionará el tráfico de la ruta "P". La Figura 11 muestra la operación de esta protección:

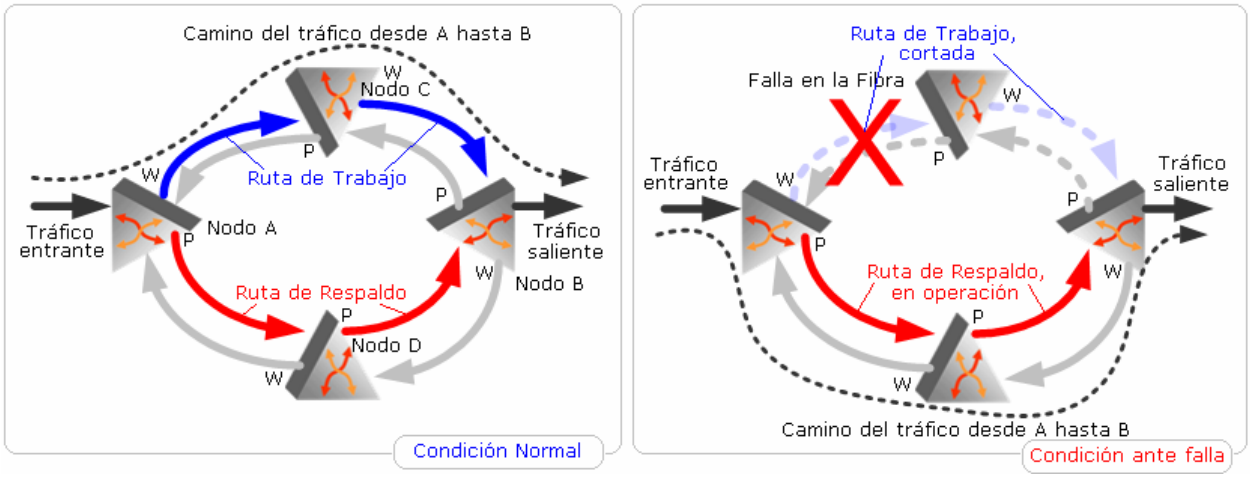


Figura 11.: Anillo de protección dedicada

2.2.1.5.9.2. 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 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. Considerando un patrón de tráfico uniforme en el cual el tráfico entrante sale del anillo en el nodo adyacente. La Figura 12 representa tal configuración:

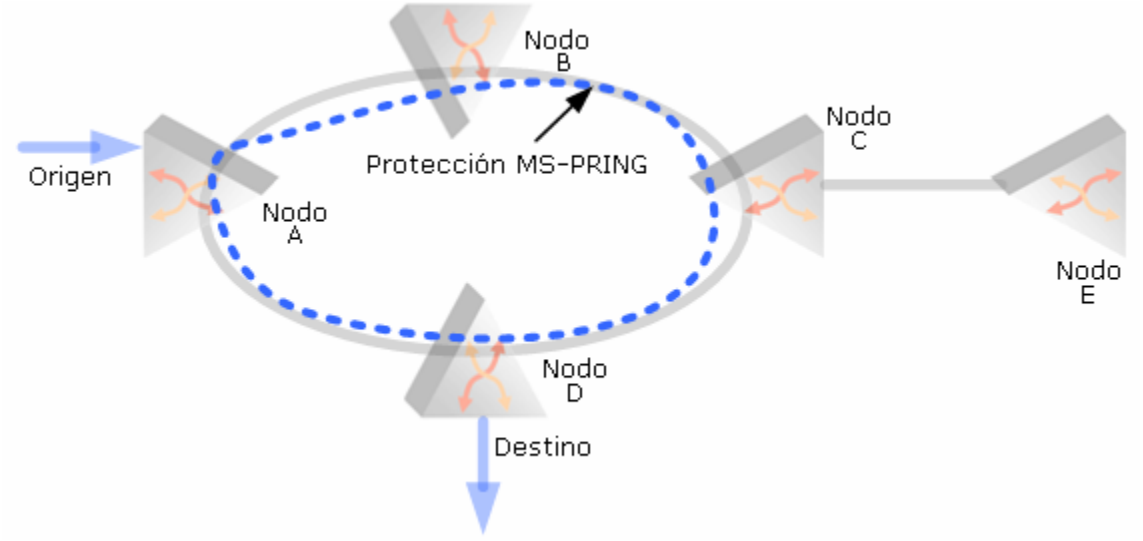


Figura 12.: Protección MS-PRING, en la configuración de anillo

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-1s son usados para tráfico activo girando en torno a todo el anillo y en cada sección otros ocho STM-1 estarán aun 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 dieciséis 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 precio donde el costo 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.

2.2.1.5.10. Comparación entre Esquemas de Protección

Como se puede apreciar en la Tabla 3, 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	SI	Anillo	<50ms
1+1 MSP	Todo el tráfico de la sección	Nodos Adyacentes	NO	SI	Lineal/ Mayada	<50ms
Ruta Dedicada	VC individual	Nodo del extremo final del anillo	SI	SI	Mixta	<50ms
SNCP	VC individual	Nodo final o intermedio de la ruta	SI	SI	Mixta	<5ms
Restauración	VC individual	No hay conmutación de protección.	SI	NO	Mayada	>1min

Tabla 3.: Cuadro comparativo entre esquemas de protección SDH

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. Ésta 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 interconexión con los adyacentes.

Un despliegue efectivo de subredes es interconectando subredes protegidas con 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.

2.2.1.6. INTERFASES DE LÍNEA DE SDH

Se definen para SDH interfases físicas tanto ópticas como eléctricas.

2.2.1.6.1. Interfases ópticas

Hay tres grados de aplicación distintos:

a) **Local** (indicados con I-n, donde n=nivel jerárquico STM). Abarca aplicaciones que requieren una transmisión a una distancia máxima de 2 km, con estimaciones de pérdidas entre 0 y 7 dB con fibra monomodo. Los transmisores ópticos I-n pueden ser LEDs o transmisores láser de modo multilongitudinal (MLM) de baja potencia con longitud de onda de 1310 nm.

b) **Corto alcance** (indicados con S-n.1 ó S-n.2, donde n=nivel jerárquico STM, 1=longitud de onda de 1310nm sobre fibra G.652; 2=longitud de onda de 1550nm sobre fibra G.652). Abarca aplicaciones a una distancia de hasta 15km, con pérdidas entre 0 y 12 dB., con fibra monomodo. Se utilizan transmisores láser de modo monolongitudinal (SLM) o de modo multilongitudinal (MLM) de baja potencia (50W ó -13dBm) con longitudes de onda de 1310 ó 1550nm.

c) **Largo alcance** (indicados con L-n.1 ó L-n.2 ó L-n.3, donde n=nivel jerárquico STM, 1=longitud de onda de 1310nm sobre fibra G-652; 2=longitud de onda de 1550nm sobre fibra G-652 ó G-654; 3=longitud de onda de 1550nm sobre fibra G-653). Abarca aplicaciones a distancias de hasta 40km, con pérdidas entre 10 y 28dB, con fibra monomodo. Se utilizan transmisores láser SLM ó MLM de alta potencia (500W ó -3dBm) con longitudes de onda de 1310 ó 1550nm.

2.2.1.6.2. Interfases eléctricas

Utilizadas básicamente para aplicaciones internas y de comunicación a muy corta distancia. Respecto de las STM-1, son CMI, 75 ohms coaxial NRZ según la norma G.707. También están las interfaces eléctricas para puertos tributarios multiservicios de baja velocidad tales como ATM, ETH, E1.

2.2.2. CONMUTACIÓN ÓPTICA E INTELIGENCIA EN LA RED

2.2.2.1. CONMUTACIÓN ÓPTICA

Se plantea la necesidad de incrementar el ancho de banda en la red para cursar la demanda creciente. Por otra parte, hay servicios (λ gestionadas,...) que no se pueden cursar por SDH. Las redes SDH se construyen con dos tipos de elementos: 1.- **ADMs**, con dos agregados (y múltiples tributarios), diseñados para formar anillos. Disponen de una buena capacidad de conmutación y regeneran la señal (Opt-Elec-Opt); y 2.- **DXC**s. (Cross conectores Digitales). Estos conectores unen cualquier puerto de entrada con otro de salida, permitiendo topologías malladas de red. Tienen grandísimas capacidades de conmutación y regeneran la señal. El punto negativo a destacar lo constituye su coste económico que es muy elevado.

Para incrementar el tamaño y tráfico de la red, se debe ampliar el equipamiento SDH, aumentándose asimismo las capacidades de transmisión y conmutación de la red. Sin embargo, el tráfico raramente va desde un nodo a otro adyacente, sino que normalmente cruza varios nodos, ineficientemente en SDH. Utilizando los recursos de la capa WDM, y perdiendo flexibilidad en la extracción de cargas útiles, se minimiza este número de saltos. Los ADMs ópticos (OADMs) extraen unas pocas LAMBDAS dejando el resto en paso tras amplificar su potencia. Por otra parte, a pesar de que hoy los servicios STM-16 son relativamente infrecuentes, su proporción está creciendo rápidamente y los equipos SDH son bastante ineficientes en su tratamiento. Adicionalmente la demanda cada vez mayor de gestionadas, no tratables en la capa SDH, favorece el desarrollo de la capa WDM. En este

sentido ha aparecido un nuevo elemento que va a ser estratégico en un futuro cercano: el Cross-Conector óptico, capaz de conmutar (como en el digital "*any to any*") entre puertos ópticos sin realizar regeneración eléctrica, posibilitando la creación de redes puramente ópticas malladas. El coste por puerto es del orden de la quinta parte de uno digital. Con estos elementos, además de cursar de forma eficiente las λ gestionadas, se liberará gran capacidad de conmutación de las redes SDH existentes, a costa de perder flexibilidad en la extracción/inserción de circuitos.

2.2.2.2. RED ÓPTICA INTELIGENTE

El desarrollo de la capa óptica es ya una realidad. Se han añadido funciones básicas de conmutación y la mayor parte de los esfuerzos de desarrollo hoy en día se centran en esta capa a fin de añadir inteligencia a la misma, dotándola de funcionalidades de capas superiores. Actualmente se está trabajando en la definición de una serie de estándares que permitan la interconexión de los elementos de datos (*routers*, etc.) directamente a la "red óptica inteligente".

Las principales características diferenciales de este modelo de red son: interconexión de los elementos de las redes de servicios a los elementos de capa óptica; facilidad para su gestión y operación automatizada. Todos los nodos mantienen activamente un mapa de red. Cada nodo descubre a sus vecinos, caracterizando los enlaces que los unen. Posteriormente, la topología, inventario e información de recursos de la red se distribuye a todos los nodos; provisión dinámica y automática. El elemento de datos del usuario de la red solicita al elemento de red una conexión a otro elemento de datos con unas determinadas características (calidad, latencia, ancho de banda, etc.). El elemento de red, basándose en la información de red que dispone calcula el camino óptimo. Finalmente, el circuito se establece tramo a tramo ("*hop-by- hop*") y notifica que la conexión está disponible; y Restauración automática. Actualmente hay dos mecanismos para la recuperación de fallos de red: protección, que implica reservar recursos de la red para casos de fallo, y restauración, que implica reconfigurar la red proveyendo nuevos recursos a fin de trazar una

ruta diferente para los servicios afectados. La protección está automatizada en los nodos de red, y entra rápidamente en funcionamiento (ms). La restauración hoy en día se hace de forma manual desde los sistemas de gestión, y tarda bastante más en reponer los servicios afectados. La restauración emplea de un 20 a un 50% menos de ancho de banda que lo hace la protección. Automatizarla mejora los tiempos de respuesta a la vez que optimiza el ancho de banda y dota a la red de una gran fiabilidad y robustez al ser capaz de recuperar se automáticamente ante fallos severos (evita puntos de fallo).

Son los protocolos de señalización y enrutado los que soportan la mayor parte de las nuevas funcionalidades. A continuación se expone una breve evolución de los mismos:

-1998 MPLS Provisiona circuitos ópticos WDM como MPLS paquetes: uso de etiquetas. Se concluye que se debe implantar las funcionalidades de provisión y restauración, extenderse a la capa WDM, y a SDH/TDM, conocer la capa de fibra subyacente.

-2000 GMPLS. Extiende MPS con: mapeo generalizado de etiquetas que alcanza a los *slots* TDM, transmisión bidireccional, mejora de las funcionalidades de señalización (conexiones permanentes, semipermanentes o *soft*), nuevas funcionalidades de enrutado (descubrimiento de la topología de la red y de servicios). GMPLS está todavía en fase de desarrollo. No es desplegable comercialmente. Los protocolos de conexión y señalización están completados, los protocolos de enrutado todavía en curso y la restauración no definida aún.

-2001 ASON (Iniciativa ASTN). Ha definido requisitos de arquitectura para la "Red óptica inteligente". Se está trabajando en los protocolos de conexión. Parte de GMPLS y otras experiencias particulares (OSRP). No habrá productos en el medio plazo.

-Actualmente se impone la optimización de las redes existentes. SDH tiene una larga vida por delante al dotarle de nuevas funcionalidades que permiten cubrir los nuevos servicios rentabilizando las inversiones realizadas y el "*know-how*" adquirido.

-Las operadoras van a cubrir una gran demanda de servicios muy diversos, tanto emergentes como ya habituales. Esto va a complicar considerablemente la topología y diseño de las redes, favoreciendo el desarrollo de las redes ópticas.

-La futura "Red óptica inteligente" supondrá una "nueva generación" para las tecnologías que soportan las redes troncales de las operadoras, pero tardará en llegar debido al incipiente estado de desarrollo de los estándares, de la falta de inversión y del esfuerzo fructífero para soportar la demanda de servicios sobre redes existentes.

2.3. ASON (*AUTOMATICALLY SWITCHED OPTICAL NETWORKS*)

2.3.1. DESCRIPCIÓN GENERAL DE LA RECOMENDACIÓN G.ASON

Grupos de trabajo de la UIT-T, definieron dos conceptos para las redes de transporte: ASTN y ASON. Estos esfuerzos de la UIT, contaron con el soporte del OIF ("*Optical Internetworking Forum"*) y del IETF ("*Internet Enginnering Task Force"*) entre otros. Su uso esta conceptualizado en la búsqueda de mejoras en las prestaciones de servicios basadas en redes ópticas de transporte que hacen uso de un plano de control óptico. Con esto se persigue simplificar y reducir las estructuras de capas de los servicios actuales mediante un plano de control inteligente sobre la capa física. Es así como la UIT, con su enfoque tradicional, considera los requerimientos para una ASTN, y a partir de ahí, se centra en la especificación de los detalles tecnológicos y de protocolos para definir la arquitectura y funciones de la red, dando lugar a las RFC G.8070 para ASTN y G.8080 para ASON[1][2][3].

Las principales características de ASON son: capacidad para soportar nuevos servicios ópticos como servicios de ancho de banda bajo demanda (BODS) y redes privadas virtuales ópticas (OVPN); enrutamiento dinámico con auto detección de "vecinos", de enlaces, de topologías (a través de OSPF-OE "*Open Shortest Path First with Optical Extensions*"); aumento de estabilidad y escalabilidad en los sistemas de gestión debido a que el plano de control se encuentra distribuido sobre los elementos de red; y, restauración mas eficiente de servicios pues ASON provee mecanismos de recuperación descentralizados y prácticamente en tiempo real.

2.3.2. ESTANDARES

La recomendación UIT-T G.807, es la primera de "Redes de Transporte con Conmutación Automática" ASTN y fue aprobada en el año 2001. Aborda la arquitectura de la red y los requisitos del plano de control, independiente a las tecnologías de transporte a aplicarse.

Luego de ello, se elaboraron para ASON: la recomendación UIT-T G.8080/Y.1304 que trata sobre la arquitectura y requisitos de las redes ópticas con conmutación automática, aplicable a las redes SDH (G.803), y a otras redes definidas en la RFC G.807; La RFC G.7713/Y.1704 que incluye conceptos para la Gestión de Conexión Distribuida y requerimientos para las interfaces de red de usuario UNI y Nodo de Red NNI y señalización; la G.7714/Y.1705 que cita sobre descubrimiento automático generalizado; la G.7712/Y.1703 que trata sobre la arquitectura de la Red de Comunicación de Datos DCN, aplicable a ASON; y, la G.8080/Y.1304 que describe las normas básicas del plano de control de las ASON.

2.3.3. PLANOS DE ASON

Las redes de conmutación automática, como son establecidas en los estándares ASTN/ASON, están constituidas por tres planos: El de Transporte, el de Control y el de Gestión. En la Figura 13 se muestra la interacción entre estos planos.

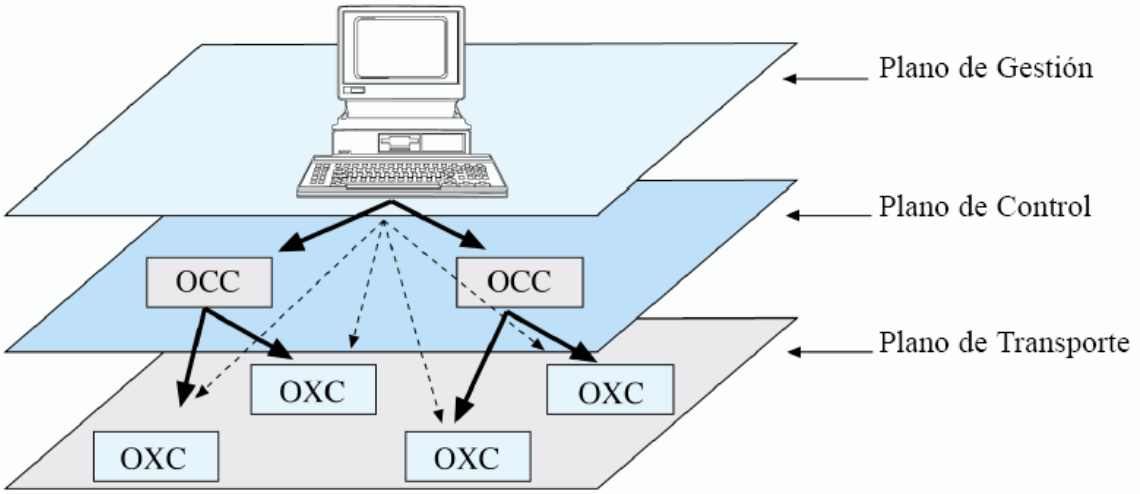


Figura 13.: Interacción entre los planos de Gestión, Control y Transporte ASON

Se busca proveer a la red de un plano de control inteligente que cuente con aprovisionamiento dinámico y funciones de supervisión, protección y restauración de conexiones. El plano de control es el que deberá establecer, supervisar, mantener y liberar las conexiones. El plano de gestión se encargara de la supervisión, configuración, seguridad y facturación de enlaces. Finalmente, el plano de transporte, se encargará de la transferencia de información de un lugar a otro de la red.

2.3.3.1. INTERRELACIÓN ENTRE LOS PLANOS

ASTN/ASON se diseñaron en su concepción, para soportar múltiples clientes y variadas tecnologías. Esto crea los diferentes dominios de cada plano. La conexión Intra-Dominios e Inter-Dominios dentro de la capa de control, se realiza a través de las interfaces I-NNI ("*Internal Network to Network Interface*") y E-NNI ("*External Notwork to Network Interface*") respectivamente. Además existe la interfaz que enlaza los dominios de los usuarios con la red de los proveedores de servicio que se conoce como UNI ("*User to Network Interface*") La Figura 14 detalla como interactúan los diversos dominios de la red y los enlaces entre planos.

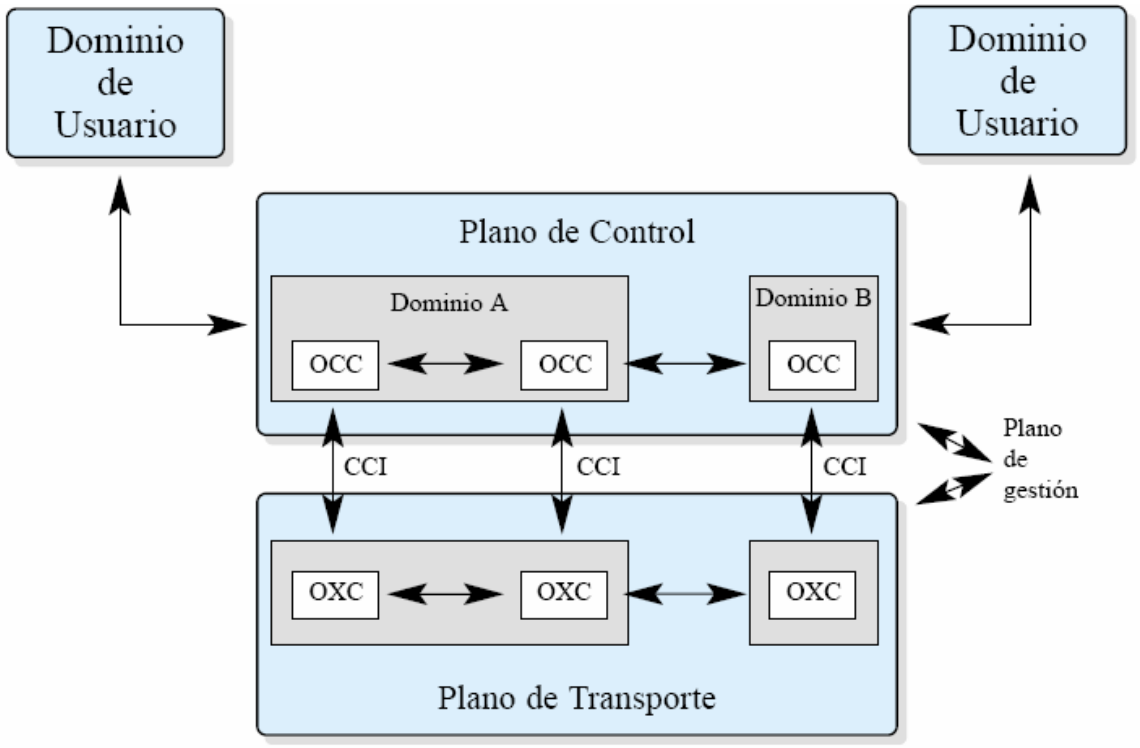


Figura 14.: Interacción entre los dominios de red y enlaces entre planos

Se puede apreciar que planos de control y de transporte se encuentran bien diferenciados, y sus interrelaciones vienen dadas, como se ilustra en la figura 14, por la interfaz de control de conexión CCI ("*Connection Controller Interface*"). A través de ella se

pasa la información del control de la conexión para establecer las respectivas conexiones entre los diferentes puertos de los centros de Conmutación ópticos.

El protocolo en que se basa esta comunicación debe soportar dos aspectos fundamentales: establecimiento y liberación de conexiones; y, búsquedas del estado de los puertos.

Entre los protocolos que cumplen con los requerimientos para la CCI se encuentra GSMP *("General Switch Management Protocol"),* el cual es un protocolo de propósito general que permite el cumplimiento de las funciones básicas y se soporta en arquitecturas de redes tales como ATM, FR y GMPLS. El plano de control ejecuta funciones para manipular efectivamente la capa de transporte. La primera función que ejecuta es el control del auto descubrimiento de los dispositivos y recursos de esta capa de transporte. Cada OXC comienza a detectar los recursos y capacidades disponibles en su adyacencia, así como las conexiones entre los otros dispositivos adyacentes, mediante el intercambio de señalización. Cuando cada OXC reúne la información acerca de los recursos y la topología involucrada, la envía a los OCC (Controladores de Conexión Óptica) pertinentes utilizando las interfaces CCI (interfaz controladora de OCXs). Luego estos OCC comienzan a descubrirse entre sí, y con ello la topología de toda la red, además de los recursos de ancho de banda disponible, utilizando para esto la NNI (interfaz de nodo a nodo) con el soporte de una versión mejorada del protocolo OSPF (Primero la vía más corta – "*Open Shortest Path First"*). Con toda esta información recopilada, se crea una base de datos de la topología de la red, que luego es utilizada por los OCC para calcular los caminos requeridos a través de esta red. Para la señalización de estos caminos, los OCC utilizan el protocolo de señalización GMPLS[5], esto permite activar, establecer, modificar o desactivar los enlaces en forma dinámica, procurando rutas óptimas y eficientes para los Caminos ópticos ("*Lightpath")*. El enrutamiento distribuido le da a las redes, escalabilidad, robustez, mayor velocidad de conmutación y mejor rendimiento de la señalización, permitiendo la creación de enrutamientos jerárquicos

y varios dominios de administración. Aquí el controlador de conexiones óptico – OCC ("*Optical Connection Controller*") es el ente fundamental del plano de control. Aparte de las interfaces del plano de control UNI, I-NNI, ENNI, ya mencionadas, se tiene también la interfaz de gestión de la red – NMI ("*Network Management Interface*"), necesaria para llevar a cabo las operaciones y mantenimiento del sistema.

2.3.4. PLANO DE TRANSPORTE

El plano de transporte contiene todos los elementos de transporte de red (*switches* y enlaces) que hacen posible la conexión. Las conexiones extremo a extremo son establecidas dentro del plano de transporte bajo el control del plano de control de ASON, siendo este elemento la principal característica de interrelación entre estos planos. Los elementos básicos que conforman el plano de transporte son:

-Conmutadores Ópticos

-OXC Conmutadores ópticos/ eléctrico/ópticos

-PXC Conmutadores ópticos/ Ópticos

-Topología de red tipo malla, de fibra óptica

-LMP Protocolo de Capa de Enlace, "*Link Management Protocol*"

Como ya se ha comentado, el Plano de Transporte contiene elementos de la red de transporte (nodos y enlaces) que llevan una «entidad conmutada», como por ejemplo, las conexiones ópticas. Las conexiones punto a punto son establecidas dentro del plano de transporte, bajo el control del Plano de Control. El Plano de Transporte proporciona un flujo unidireccional o bidireccional para el intercambio de información a ser usado entre dos entidades. Este plano es equivalente al descrito en la Recomendación G.805 de la UIT-T, (Arquitectura Funcional Genérica de las Redes de Transporte).

A continuación se citan los Componentes, Entidades y Funciones de estas Redes de Transporte, los cuales como todo elemento genérico utilizado en normas UIT, tienen definiciones un tanto abstractas:

-Componentes Topológicos: proporcionan la descripción más abstracta en términos de relaciones topológicas, entre conjuntos de puntos de referencia similares.

-Red de Capa ("*Layer Network*"): definida por el conjunto completo de grupos de acceso del mismo tipo que pueden estar asociados, a efectos de transferencia de información.

-Subred: define el conjunto de puertos disponibles para la transferencia de información característica.

-Enlace: consta de un subconjunto de puertos situados en el borde de una subred, o grupo de acceso asociado con un subconjunto correspondiente de puertos situados en el borde de otra subred, o grupo de acceso a los efectos de transferencia de información característica.

-Grupo de acceso: grupo de funciones de terminación de camino situada en la misma ubicación y conectada a la misma subred o al mismo enlace.

-Entidades de Transporte: proporcionan la transferencia de información transparente entre puntos de referencia de una «red de capa» en particular. En estas entidades se distinguen:

-Conexión de Enlace: es capaz de transferir información de forma transparente a través de un enlace. Está delimitada por puertos y representa la relación fija entre los extremos de ese enlace.

-Conexión de Subred: es capaz de transferir información de forma transparente a través de una subred. Está delimitada por puertos de conexión en la frontera de la subred y representa la asociación entre esos puntos de conexión.

-Conexión de Red: es capaz de transferir información de forma transparente a través de una «red de capa». Está delimitada por Puntos de Conexión de Terminación (TCP). Se constituye a partir de una concatenación de conexiones de subred y/o conexiones de enlace.

-Camino: representa el soporte para la transferencia de información característica adaptada y supervisada de la red de capa de cliente entre puntos de acceso.

-Funciones de Tratamiento de Transporte

-Función de Adaptación: Tiene tres ámbitos como, fuente de adaptación, sumidero de adaptación, y adaptación como tal. Como ejemplos de procesos que pueden ocurrir de forma aislada o en combinación en una función de adaptación, pueden citarse la codificación, modificación de la velocidad, alineación, justificación y multiplexación.

-Función de Terminación de Camino: Abarca las funciones de fuente de terminación de camino, sumidero de terminación de camino, y terminación de camino bidireccional.

–Puntos de Referencia: Se forman mediante la vinculación entre las entradas y salidas de las «funciones de tratamiento de transporte» y/o «entidades de transporte»

2.3.5. PLANO DE CONTROL

ASON define una arquitectura para el Plano de Control que permite el establecimiento y desconexión de las sesiones como resultado de requerimientos de los usuarios. Para lograr una cobertura global y el soporte de múltiples tipos de clientes, es que se describe esta arquitectura en términos de componentes y de un conjunto de reglas y puntos de referencia que se deben aplicar en los puntos de interfaz entre los clientes y la red, y entre las propias redes en sí. Una arquitectura del plano de control bien diseñada debe dar a los proveedores de servicio, un mejor control de su red proveyendo al menos las siguientes características: Ser aplicable a las diferentes tecnologías de red de transporte (SONET, SDH, OTN, PXC, etc.,). Para alcanzar esta meta es esencial que la arquitectura aísle los aspectos dependientes de la tecnología, de aquellos que no lo son; Ser lo suficientemente flexible para permitir un rango de diferentes escenarios en la red. Para ello se divide el plano de control en diferentes componentes; Permitir conexiones permanentes, semipermanentes y conmutadas, las cuales pueden ser unidireccionales y bidireccionales.

El plano de control lleva a cabo una serie de tareas que son definidas en los siguientes módulos funcionales: el Controlador de Conexión Óptico *("Optical Connection Controler"*), el cual provee enrutamiento, señalización, control de conexión, etc., el

Controlador de Enrutamiento ("*Routing Controler*"), el Gestor de los Recursos de Enlace ("*Link Resorce Manager*") y el Componente Regulador de Tráfico ("*Traffic Policing Component*"). La interacción entre los diversos componentes se muestra en la Figura 15.

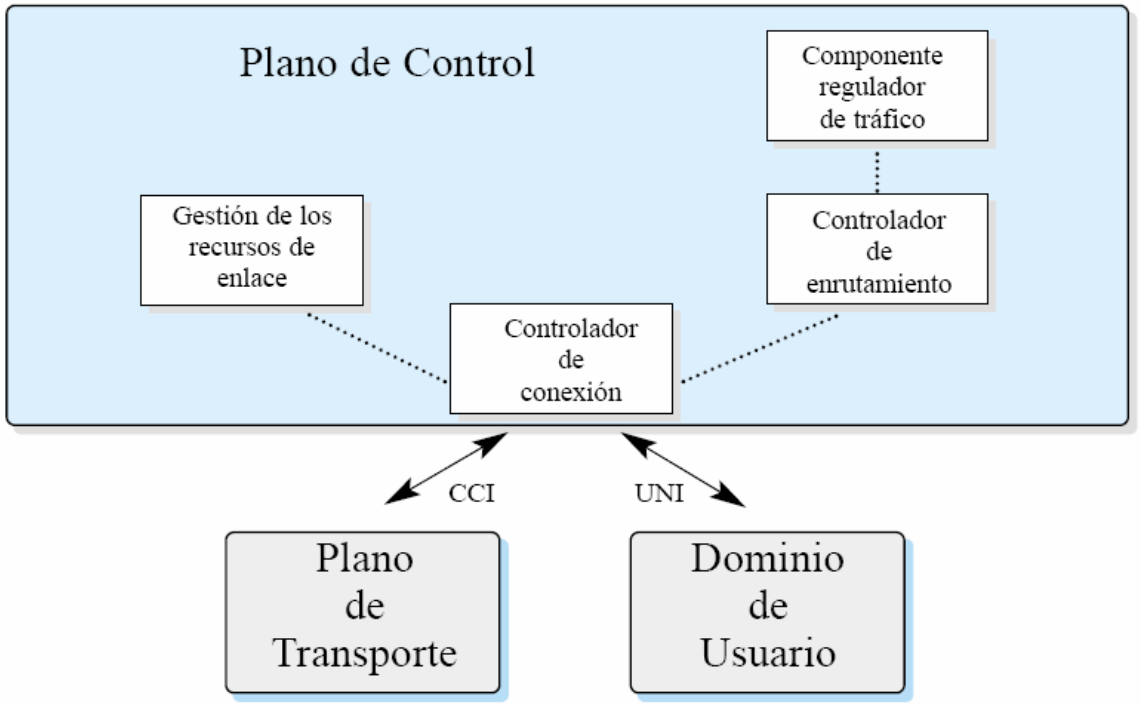


Figura 15.: Interacción de componentes entre planos ASON

-Controlador de Conexión Óptico: es el responsable de coordinar tanto al Gestor de Recursos de Enlaces, como al Controlador de Enrutamiento, con la finalidad de manejar y supervisar el establecimiento y la liberación de las llamadas, además de la modificación de los parámetros de conexión para aquellas ya establecidas. Adicionalmente, el Controlador de Conexión también provee la interfaz hacia las varias subredes ubicadas en el plano de transporte, y la interfaz respectiva hacia los dominios de usuarios.

-Controlador de Enrutamiento: se encarga de proveer la información del camino o ruta cuando el Controlador de Conexión la requiere para el establecimiento de una conexión. El controlador en cuestión logra su función primordial a través de unas tablas de enrutamiento que se actualizan dinámicamente y donde se reflejan todos los destinos que se pueden alcanzar a través de las subredes vecinas.

-Gestor de los Recursos de Enlaces: realiza un seguimiento de la manera en que los recursos de enlace son asignados para la conexión, para de esta manera controlar la capacidad de los recursos. El comportamiento del Gestor va a depender del tipo de conexión involucrada y de los conjuntos de prioridades establecidas.

-El Componente Regulador de Tráfico: la misión de este ente es verificar que las conexiones entrantes manejan el tráfico acordado según los parámetros de cada usuario.

También existen otros componentes como los Controladores de Llamadas y los Controladores de Protocolos.

2.3.5.1. ARQUITECTURA DEL PLANO DE CONTROL (RECOMENDACIÓN G.8080/Y.1304 UIT-T)

Esta arquitectura debe ser lo suficientemente flexible que facilite a los clientes de los Operadores un mejor soporte para su negocio, practicas administrativas eficientes, así como mejoras en lo referente a facturación de servicios. La arquitectura del plano de control debe tener las siguientes características: soportar varias infraestructuras de transporte, tales como la red de transporte SONET/SDH, y la red de transporte Óptico (OTN); ser aplicable independientemente del protocolo elegido; ser aplicable independientemente de cómo el plano de control haya sido subdividido en dominios y áreas de enrutamiento, y cómo los recursos de transporte hayan sido particionados en subredes; y, ser aplicable independientemente de la implementación del control de conexión, es decir, que pueda abarcar desde una arquitectura de control completamente distribuida a una arquitectura de control centralizada.

Esta arquitectura describe: todos los componentes funcionales del plano de control, incluyendo interfaces abstractas y primitivas, protocolos, etc.; las interacciones entre componentes controladores de llamadas; y, las interacciones entre otros componentes durante el establecimiento de la conexión.

2.3.5.2. NOTACIÓN

En esta sección consideraremos la notación de arquitectura de Componentes basada en ciertas reglas del vocabulario de la UML ("*Unified Modeling Language*").

-Interfaz: Una interfaz soporta un conjunto de operaciones que especifica un servicio de un Componente, y es específico independientemente del componente que use para suministrar el servicio

Cada interfaz tiene un nombre que identifica el Rol. La Interfaz de entrada representa el servicio suministrado por el Componente. Los parámetros básicos de entrada son solicitados por el rol específico. La Interfaz de salida representa el servicio utilizado por el Componente, el parámetro básico de salida define la información suministrada. La Interfaz de notificación representa acciones no solicitadas por el componente.

-Rol: Un rol representa el comportamiento de una Entidad cuando está participando en un contexto particular. El rol permite la posibilidad que entidades diferentes participen en tiempos distintos, y se designan anotando una relación con el nombre de una interfaz.

-Componente: Los componentes se utilizan para representar entidades abstractas, más que instancias de implementación de códigos. Se utilizan para construir escenarios que expliquen la operación de la arquitectura. Los componentes se representan como un rectángulo con una etiqueta. Esto se muestra en la Figura 16.

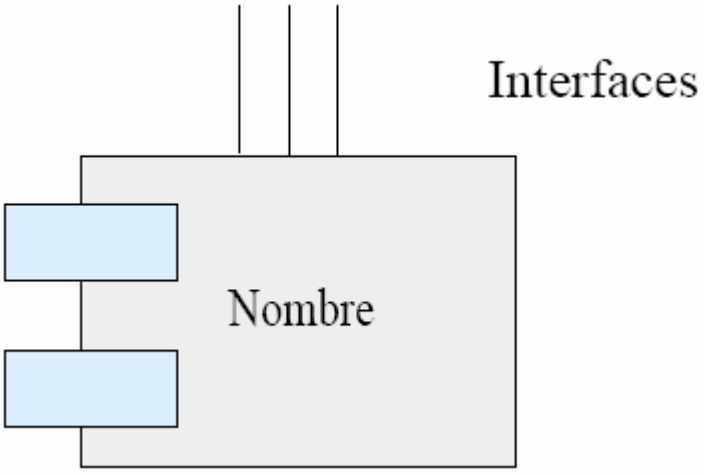


Figura 16.: Representación de componentes

Genéricamente, cada Componente tiene un conjunto de interfaces especiales que permiten monitorear sus operaciones, configurar políticas dinámicamente, y afectar su

comportamiento interno. Estas interfaces no son obligatorias, y son proporcionadas en componentes específicos sólo donde sean necesarias. Donde es necesario, el uso del interfaz monitor, se describe como un componente individual. No se asume que los componentes serán distribuidos estáticamente.

Todos los componentes tienen la propiedad de soportar múltiples llamadas y múltiples suministros de servicio. Como los componentes se utilizan en una forma abstracta, esta especificación se extiende hacia las técnicas de subclasificación y composición de componentes.

2.3.5.3. TIPOS DE CONEXIÓN

Existen básicamente tres tipos:

-**Conexión Permanente** (PC): La petición para el establecimiento de la conexión, se produce a través de la red de gestión, la cual está enmarcada dentro del plano de gestión. Allí se crea la ruta o el camino, y seguidamente se notifica a los respectivos conmutadores ópticos involucrados en la ruta, para que realicen las respectivas conexiones cruzadas.

En el ejemplo de la Figura 17, el dominio de usuario A desea conectarse al dominio de usuario B, por lo que envía la petición de conexión al plano de gestión. Éste establece la ruta, y ordena a los OXC de los dominios A, B y C pertenecientes al plano de transporte, que se interconecten entre sí, para de esta manera enlazar el dominio del usuario A con el B.

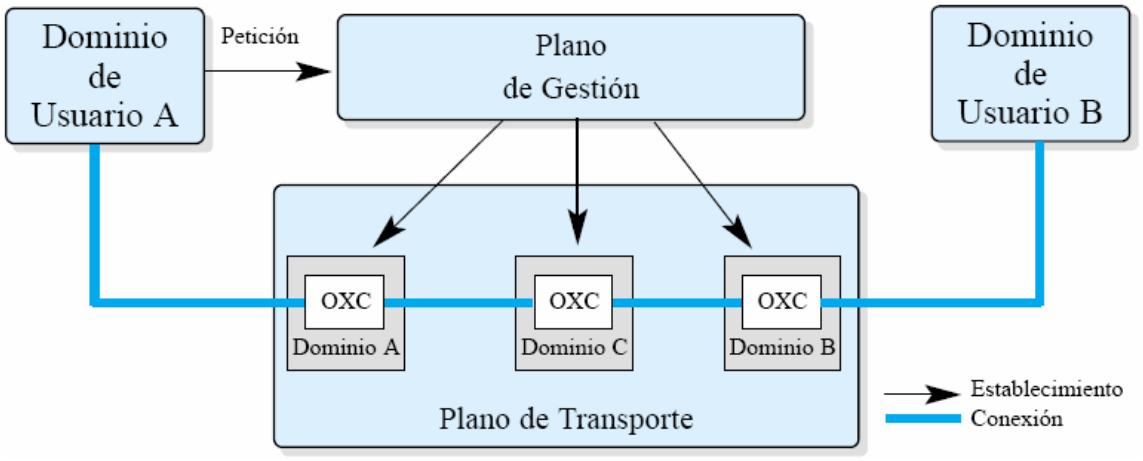


Figura 17.: Proceso de establecimiento de conexión entre dominios

-**Conexión Lógica Permanente** (Suave) (SPC): En este tipo de conexiones, el enrutamiento como tal ya no lo realiza la capa de gestión, a pesar de que las peticiones para la conexión se siguen realizando a través de este ente. Ahora la parte de la definición del camino está a cargo del plano de control.

En el ejemplo de la Figura 18, se observa cómo el dominio del usuario A realiza la petición de conexión al plano de gestión. El dominio B del plano de control recibe la petición de llamada, y en conjunto con los otros dominios establece la ruta de A hacia B.

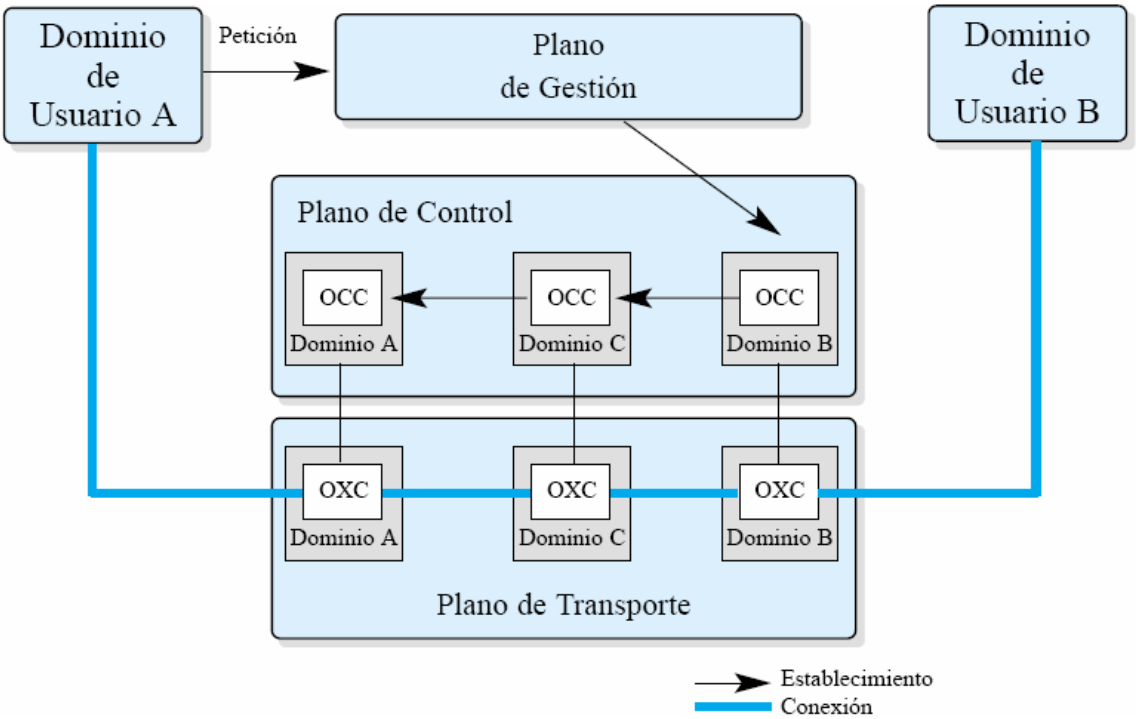


Figura 18.: Proceso de petición de conexión al plano de gestión

[Definición UIT: La SPC es una conexión usuario a usuario, en la que la porción usuario a red, de la conexión extremo a extremo, la establece el sistema de gestión de red como una conexión tipo PC. La porción de red, de la conexión extremo a extremo, se establece como conexión conmutada mediante el Plano de Control. En la porción de red, de las conexiones, las peticiones de establecimiento de la conexión las inicia el Plano de Control].

-**Conexión Conmutada** (SC): Para el caso de la conexión conmutada, la solicitud proveniente del dominio de usuario se realizará directamente en el plano de control, a través de la interfaz UNI. El plano de control de nuevo se encargará de todo lo que es el establecimiento de la conexión y el enrutamiento, y algunas otras tareas como la supervisión y control de admisión de las llamadas y de la cobranza entre otras.

En el ejemplo de la Figura 19, se observa cómo la petición de llamada llega al dominio A del plano de control, y cómo éste se encarga completamente de establecer la ruta hacia el usuario B.

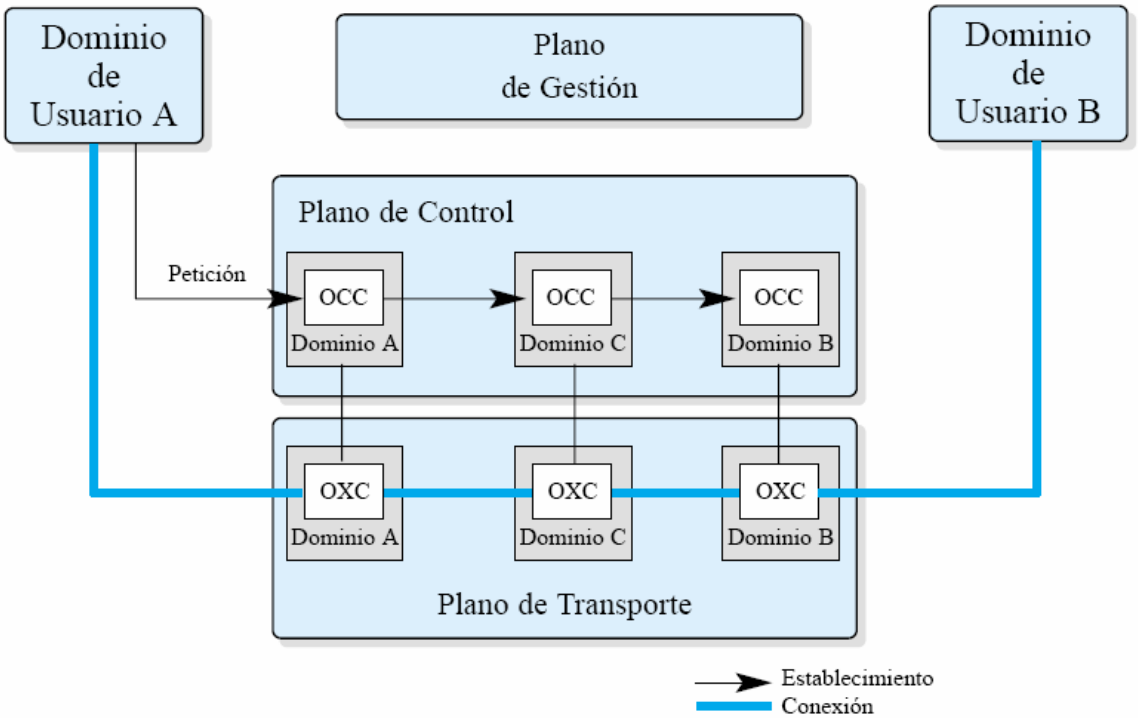


Figura 19.: Proceso de establecimiento de ruta

[Definición UIT: Una Conexión Conmutada es cualquier conexión que se establece, como resultado de una petición del usuario, entre puntos extremos de conexión, mediante un plano de señalización y control, y con un intercambio dinámico de información de señalización entre los elementos de señalización de los planos de control].

La interconexión entre dominios, áreas de enrutamiento y en donde sea requerido, se hace en términos de Puntos de Referencia, los cuales describen el conjunto de componentes de control necesarios para el intercambio de información. La interconexión física es provista por una o más de estas interfaces. Una interfaz física se provee relacionando una interfaz abstracta hacia un protocolo determinado.

2.3.6. INTERFACES DEL PLANO DE CONTROL (PUNTOS DE REFERENCIA, PDER)

Tal y como se ha apreciado en las figuras anteriores, el plano de control define interfaces con los clientes (UNI), entre nodos de la misma red (I-NNI)[2], entre nodos de diferentes redes (E-NNI), y entre los elementos del plano de control y los del plano de transporte (CCI). Es de hacer notar que hay publicaciones en donde estas Interfaces son también llamadas «Puntos de Referencia». A continuación se da una breve explicación de cada una de ellas:

2.3.6.1. INTERFAZ UNI

Representa el PdeR que separa el dominio del Operador, del de sus usuarios. Los protocolos de señalización en la interfaz UNI[4], deben permitir al usuario ASON llevar a cabo las siguientes funciones:

-Creación de una conexión: Esta función consiste en señalizar a la red para crear una nueva conexión, la cual tendrá unos ciertos atributos como, ancho de banda, protección, restauración y diversidad.

-Eliminación de una conexión: el usuario ASON indica a la red, la necesidad de finalizar una conexión existente.

-Modificación de la conexión: permite al cliente en un momento dado modificar los atributos característicos de la conexión.

-Solicitud de Status de la conexión: el usuario puede verificar la situación de una conexión a través de una consulta de status.

Las cuatro funciones anteriores son las de mayor importancia, y están relacionadas con las conexiones como tal. Sin embargo, existe otro grupo de ellas, que son igualmente, responsabilidad del protocolo de señalización. Estas son: registro de usuarios, asignación de direcciones, descubrimiento de redes y servicios vecinos, etc.

Todas las funciones de señalización presentes en la interfaz UNI son controladas del lado del plano de control, por el Controlador de Conexiones. Este constituye el ente señalizador, pero también se apoya en otras entidades como el Controlador de Enrutamiento y el Gestor de Recursos de Enlaces, para realizar completamente sus labores respectivas.

Los protocolos de señalización deben ser capaces de soportar las funciones descritas anteriormente. En este sentido se han realizado extensiones a los protocolos LDP y RSVP-TE para que puedan ser empleados en esta interfaz. Los esfuerzos de la ITU en cuanto a señalización se han enfocado en definir los requerimientos y las funcionalidades necesarias en la interfaz UNI. El registro de clientes/usuarios y aspectos de sus direcciones están muy relacionados.

2.3.6.2. INTERFAZ O-UNI

La O-UNI separa el dominio IP, tanto de tipo de medio, como en modo de enrutamiento. Mientras que una red IP, requiere un análisis del paquete, para determinar la ruta más adecuada a seguir, en el dominio ASTN se utiliza el protocolo MPLS, el cual coloca las etiquetas LSP en los paquetes para el enrutamiento respectivo usando la capa 2, dándole así una mayor velocidad al enrutamiento de los paquetes

Mientras que en el dominio IP cuando un paquete llega a un router, éste analiza la dirección IP (en la capa 3) para determinar, de acuerdo a sus tablas la dirección que debe seguir y esto lo hace con todos aquellos paquetes, teniendo un tiempo de procesamiento considerable, y en ASTN en cambio, cuando este paquete llega al O-UNI, éste consulta las tablas de la red ASON (capa de control) y determina cuál es la mejor ruta a seguir por este paquete, luego le coloca una etiqueta LSP, la cual contiene la información de enrutamiento dentro de la red ASON. De esta manera, cuando el paquete llega a un OXC, éste sólo ve la etiqueta LSP en la capa 2 y la dirige hacia el próximo OXC indicado en la etiqueta, reduciendo de esta forma el tiempo de procesamiento.

2.3.6.2.1. Acciones de la O-UNI

-Creación de la ruta. Se realizan las conexiones adecuadas, para establecer la ruta óptica, con atributos específicos.

-Eliminación de la conexión óptica. Elimina las conexiones de la ruta óptica ya existente.

-Modificación de la conexión óptica. Modifica uno u más atributos de la ruta óptica ya existente.

-Indagación del estado de la conexión óptica. Averigua acerca del estado de la ruta óptica existente Cada acción realizada por el O-UNI, es mediante un set de mensajes.

2.3.6.3. INTERFAZ I-NNI

I-NNI define la interfaz entre Controladores de Conexión adyacentes dentro de la misma red. Existen dos aspectos de importancia a considerar en esta interfaz: la señalización y el enrutamiento.

La selección y establecimiento del camino a través de la red óptica requiere un protocolo de señalización. Las redes de transporte típicamente emplean enrutamiento explícito, en el sentido que la ruta se selecciona, o por el Operador o por herramientas de software en el sistema de gestión. En ASON, las conexiones extremo a extremo se deben realizar tomando en cuenta ciertas restricciones. Por ello la selección de la ruta se basa en algoritmos de enrutamiento que toman en cuenta diversos objetivos tales como: el balanceo de la carga de tráfico de la red, para obtener la mejor utilización de los recursos; y, políticas de enrutamiento para seguir los caminos preferidos o más rápidos.

Para facilitar la automatización del establecimiento de la conexión, y tomando en cuenta las limitaciones mencionadas en el párrafo anterior, los nodos en la red óptica deben poseer la actualización de sus puntos adyacentes, así como también los niveles de utilización que presentan dichos nodos. Esta información debe ser repartida por toda la red a través de los protocolos de señalización dentro del plano de control.

También es importante señalar que, de igual manera los protocolos de la interfaz I-NNI deben soportar las funcionalidades presentes en la interfaz UNI, es decir, deben permitir crear, modificar y eliminar conexiones, así como proveer status de la misma.

La interfaz I-NNI podría ser implementada a través de dos protocolos claves, IP y MPLS. Inclusive el protocolo GMPLS posee unas ampliaciones a nivel de enrutamiento, que permitiría una más fácil adaptación en la interfaz en estudio.

2.3.6.4. INTERFAZ E-NNI

El PdeR entre dominios diferentes está representado por la E-NNI. Estos dominios pueden pertenecer a una misma administración, o a diferentes administraciones. El protocolo BGP pudiera ser recomendado para usarse entre diferentes dominios ASON, de forma similar a su uso en dominios diferentes IP. ENNI es similar a la UNI, pero con ciertas funciones de enrutamiento que permiten el intercambio de información entre las redes involucradas.

La diferencia entre I-NNI y ENNI es significativa. I-NNI se aplica sobre un área con esquemas de enrutamiento únicos, y en donde todos los equipos soportan el mismo protocolo de enrutamiento, y el intercambio de información de ruteo entre los nodos es posible. Por otro lado, E-NNI sí soporta diferentes esquemas de enrutamientos y de protección que pudieran usar los diferentes dominios.

2.3.6.5. INTERFAZ CCI

Esta interfaz define la interrelación entre los elementos de los planos de control y de transporte.

2.3.7. ENRUTAMIENTO Y SEÑALIZACIÓN

2.3.7.1. SEPARACIÓN DE LLAMADAS Y CONTROL DE CONEXIÓN

La arquitectura de ASON trata separadamente las llamadas y su control de conexión. Esto permite la introducción de servicios mejorados, en donde una simple llamada puede estar compuesta de más de una aplicación. Esta característica brinda beneficios a las áreas de mantenimiento y restauración.

2.3.7.2. FEDERACIÓN

El control de la conexión a través de múltiples dominios requiere la cooperación entre los controladores de estos diferentes dominios. Una Federación se define como la comunidad de dominios que cooperan para una mejor gestión de sus conexiones. Dos tipos de Federaciones están definidas: el modelo de federación conjunta, en donde un controlador de conexión tiene autoridad sobre otros controladores de dominios diferentes. El segundo modelo es un modelo totalmente cooperativo, en donde no existe la figura de un líder.

2.3.7.3. ESTRUCTURAS FÍSICAS DE CONTROL ENTRE UNI'S

-Interfaz Directa: Involucra el uso de un canal de control IP (IPCC) dentro o fuera de banda que se puede implementar entre el cliente y cada cross-conector óptico (OXC).

-Interfaz Indirecta: Involucra el uso de un canal de control IP fuera de banda que se puede implementar entre el cliente y un dispositivo de control dentro de la red óptica, para así proporcionar servicios de señalización.

Es esencial que tanto las interfaces directas como las indirectas sean soportadas por un protocolo cualquiera de señalización en la UNI. La entidad que realiza esta señalización del lado del cliente se conoce como UNI-C, y aquella que lo hace del lado de la red se llama UNI-N.

2.3.7.4. ENRUTAMIENTO EN REDES ÓPTICAS

Las redes ópticas son capaces de entregar conexiones de banda muy ancha a través de los *lightpaths* (equivalentes a los LSP). Un *lightpath* se establece entre dos puntos terminales en la red óptica, a la cual los clientes están conectados. Las propiedades de estos *lightpaths* se definen mediante los atributos especificados durante el establecimiento de la conexión, o mediante algunas solicitudes de modificación soportables.

La noción de grupos de trabajo se considera como una parte integral del establecimiento del *lightpath*. Un Grupo de Trabajo se define como un conjunto de dispositivos de clientes que restringen la conectividad con otros dispositivos fuera de este Grupo.

Las acciones soportadas por los servicios *lightpath* son las siguientes:

-Creación de *Lightpath*: Esta acción permite la creación de una ruta entre dos terminales. A cada ruta se le asigna un identificador único dentro de la red óptica llamado *ligthpath* ID.

-Eliminación de *Lightpath*.

-Modificación de *Lightpath*: Esta acción permite modificar algunos parámetros de la ruta, dependiendo de las políticas de la red, y en ningún caso puede ser destructiva.

-Solicitud de estado del *Lightpath*: Esta acción permite acceder a ciertos valores del estado de la ruta, especificándola por su identificador.

Adicionalmente, se pueden realizar los siguientes procedimientos de direccionamiento dentro de la UNI:

-Registro de cliente: Este permite que un cliente registre su(s) dilección(es) y su(s) identificador(es) de Grupo dentro de la red óptica. Este registro puede ser de distintos tipos (IP, ATM, etc.). La red óptica asocia la dirección y el identificador de grupo con una "dirección administrada por la red óptica" ("*Optical-Network- Administered Address"*).

-Eliminación del registro de cliente

-Solicitud: Permite al cliente suministrar a otros clientes, una dirección y un identificador de Grupo para crear una «dirección administrada por la red », que pueda ser usada para los mensajes de creación de ruta.

Como sabemos, cada OXC en una red óptica, posee una o más direcciones IP asociadas a ella, la cual se asume única dentro del dominio de servicio de la UNI. Estas direcciones son del tipo "administradas por la red". Cada punto de conexión de los clientes tiene asignado una de estas direcciones, por lo que es posible que varios puntos de conexión tengan asociados la misma dirección. Los mensajes de creación de *lightpaths* deben identificar la fuente y el destino de la ruta, y si éstos no pueden ser asociados a una dirección única, se puede utilizar una componente opcional de direccionamiento llamada Identificación Lógica del Puerto ("*Logical Port ID"*).

2.3.7.5. SEÑALIZACIÓN EN REDES ÓPTICAS

Como es sabido, las UNI son capaces de soportar distintos protocolos de señalización. Pero es importante destacar que éstos deben cumplir con un cierto número de mecanismos para su correcto funcionamiento, los cuales se mencionan a continuación:

-Canal de control IP: Se requiere un IPCC entre la UNI-C y las correspondientes UNI-N, por lo que para implementarlo es necesario que estas entidades conozcan sus respectivas direcciones IP. Es necesario que para el establecimiento de conexiones en la unidad de control UNI, se cumplan los siguientes requerimientos:

-El enlace debe ser capaz de transportar paquetes IP desde UNI-C hasta UNI-N.

-La tasa de transferencia del enlace debe ser adecuada para soportar esta función.

-El enlace debe ser seguro, ambas unidades deben implementar procedimientos para evitar accesos sin autorización.

-Ambas unidades deben ser capaces de detectar rápidamente fallas en la conexión.

-Mensajes de Señalización UNI: Debido a que como se mencionó anteriormente, se pueden utilizar distintos protocolos de señalización, la lista de mensajes que se presenta a continuación es lo mas genérica posible:

-Solicitud de creación del *Lightpath*: Enviado desde la UNI-C fuente hacia la UNI-N fuente.

-Respuesta a la solicitud de creación del *Lightpath*: Enviado desde la UNI-C destino hacia la UNI-N destino aceptando la solicitud de creación de la ruta, o desde la UNI-N fuente hacia la UNI-C fuente indicando, la exitosa, o no exitosa solicitud de creación de ruta.

-Solicitud de eliminación del *Lightpath*: Enviada por la UNIC fuente, o por la UNI-N fuente, indicando que la red eliminó la ruta.

-Respuesta a la solicitud de eliminación del *Lightpath*.

-Solicitud de modificación del *Lightpath*.

-Respuesta a la solicitud de modificación del *Lightpath*.

-Solicitud de estado del *Lightpath*.

-Respuesta a la solicitud de estado del *Lightpath*.

-Notificación: Este mensaje se envía de modo autónomo desde una UNI-C o una UNIN, indicando un cambio de estado en la ruta.

-Solicitud de Dirección de un cliente remoto.

-Parámetros de los mensajes UNI: Los siguientes parámetros deben ser codificados por los mensajes de señalización UNI. Es de esperarse que el formato de los mismos sea muy similar a los desarrollados por la señalización GMPLS:

-Identificación: Identificación del *Lightpath*: Un identificador único (64 bits) dentro de la red. Identificación de contrato: Un identificador de longitud variable asignado por el proveedor de servicios, que especifica la calidad de servicio. Punto de conexión fuente/ destino del cliente. Identificador del grupo de usuario. Identificador del UNI-C

-Relacionado con servicio: Direccionalidad: Bandera que indica si la ruta es uni o bidireccional. Tipo de trama: Especifica el formato de la señal a transportar (ej. SONET, SDH, etc.) Ancho de banda. Retardo de propagación. Nivel de servicio.

-Relacionado con enrutamiento: Diversidad.

-Misceláneos: Código de resultado: Un código que indica el éxito o falla de una operación. Estado.

-Relacionado con seguridad.

-Relacionado con políticas, cuentas y autorización.

2.3.8. PLANO DE GESTIÓN

Este plano se encarga de las funciones de gestión del Plano de Transporte, Plano de Control y del Sistema como un todo. También provee coordinación entre todos los Planos.

El Plano de Gestión presenta las siguientes funciones, identificadas en M.3010 y otras recomendaciones de la serie M (UIT): Gestión de desempeño; Gestión de falla; Gestión contable; Y Gestión de seguridad.

Para permitir un enrutamiento inteligente en el plano de transporte, son requeridos parámetros adicionales tales como: enlace, costo, retardo, calidad, los cuales pueden ser provistos por este Plano de Gestión.

Este plano además tiene otras áreas generales funcionales: gestión de funcionamiento; gestión de configuración; y, gestión de estadística. Otras de las tareas de las cuales se encarga el Plano de Gestión, son: localizar recursos del Plano de Transporte en particiones del Plano de Control; activar y desactivar los procesos de descubrimiento; particionar los recursos usados por el Plano de Control; asignar identificadores únicos a los puntos de acceso de las diferentes capas de red; invocar o invalidar la protección o restauración de una conexión, a través de un comando; y, realizar funciones de administración del Plano de Transporte, del Plano de Control y del sistema en su totalidad, así como proporcionar la coordinación entre todos los planos.

2.4. GMPLS ("*GENERALIZAD MULTIPROTOCOL LABEL SWITCHING*")

2.4.1. EVOLUCIÓN DEL MODELO ÓPTICO

En la actualidad, las redes ópticas se conforman de muchas capas. Cada una está preparada para manejar un determinado tipo de tráfico y proporcionar servicios específicos. Se observa también que han surgido equipos independientes y especializados en una capa y en un tipo de tráfico (*Routers, Switchs Eth.,Switchs* ATM dispositivos SONET/SDH o conmutadores DWDM). Si bien esta práctica permite simplificar el diseño de los dispositivos, tiene el inconveniente de conformar redes complejas y difíciles de gestionar. Por ello, últimamente se está tendiendo a reducir el número de dispositivos distintos que podemos encontrar en la red, consolidando determinadas capas, eliminando redundancias y mejorando sus funcionalidades. Se tiende a un esquema de red con tan sólo dos capas. En este escenario se desarrolla un plano de control común para todas las capas con una única serie de protocolos como GMPLS. Para el correcto funcionamiento de esta red basada en GMPLS, se requieren además elementos de conmutación ópticos capaces de encaminar o conmutar el tráfico de cualquier tipo: TDM, de paquetes o de longitudes de onda (Lambdas). En la figura 16 se puede ver la evolución que está sufriendo el modelo de capas de las redes ópticas.

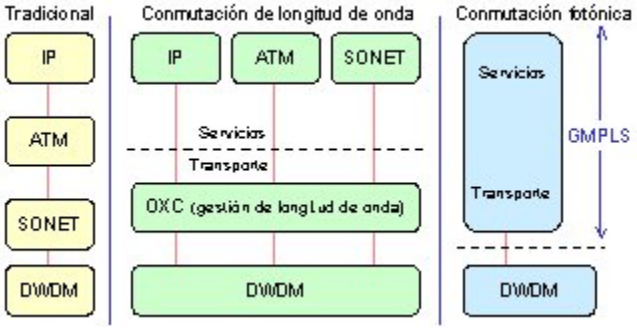


Figura 20.: Evolución del modelo de capas.

2.4.2. EVOLUCIÓN DE IP/MPLS HACIA ASON/GMPLS

La tecnología MPLS se erige como la base para las nuevas redes de banda ancha. En la actualidad, la banda ancha está basada principalmente en ATM, con velocidades que típicamente van de los 155,52 Mbit/s hasta varios Gbit/s. ATM viene usándose desde mediados de la década pasada, y su renovación parece cercana. El principal candidato es MPLS, y su despliegue ya es de hecho una realidad en muchos grandes operadores. ATM

seguirá todavía, pero por el momento su convivencia con MPLS será necesaria. MPLS ofrece grandes ventajas a la hora de definir y establecer VPNs. Además, MPLS ya tiene otras soluciones tecnológicas avanzadas, como son MPλS y GMPLS, orientadas al dominio óptico, que permiten a las redes alcanzar caudales del orden del Tbit/s por una sola fibra. Aunque parezcan capacidades enormes, podemos dar por supuesto que tarde o temprano serán caudales que acabarán siendo llenados por los servicios que los usuarios comienzan a demandar, en especial los relacionados con video e Internet (video bajo demanda, videoconferencia, videotelefonía, vigilancia remota, etc.)

2.4.2.1. FUNDAMENTOS DE MPLS

Bajo MPLS ("*Multiprotocol Label Switching*") [11][12] o Conmutación de Etiquetas multiprotocolo, se encuentra una tecnología de conmutación de circuitos que ofrece capacidades de multiprotocolo, porque sus técnicas son aplicables a cualquier protocolo de nivel de red. MPLS es un mecanismo de enrutamiento flexible basado en la asignación de flujos a rutas extremo-extremo dentro de un Dominio Autónomo. La flexibilidad ofrece la libertad de escoger el criterio por el cual los flujos de tráfico serán reconocidos y tratados de forma distintiva. En particular, tal libertad permite que un tráfico entre un par origen-destino pueda separarse en rutas paralelas para evitar congestionar los enlaces en la red. La ingeniería de tráfico en Internet es una de las aplicaciones primarias previstas para MPLS y sus principales ventajas son: permite especificar mecanismos para la administración de flujos de tráfico de diferentes tipos (Ej.: flujos entre diferente hardware, diferentes máquinas, etc.); independiza los protocolos de la capa de enlace y la capa de red; disponer de medios para traducir las direcciones IP en etiquetas simples de longitud fija utilizadas en diferentes tecnologías de envío y conmutación de paquetes; ofrecer interfaces para diferentes protocolos de encaminamiento y señalización; soporta los protocolos de la capa de enlace usados tradicionalmente para IP. Además opera perfectamente sobre ATM y *Frame Relay*, dado el parecido en el mecanismo de transporte y conmutación.

Una red MPLS esta compuesta por *Routers* MPLS: LSR ("*Label Switched Router*") que representan el núcleo de la red (*backbone*) y los LER ("*Label Edge Router*"), que son los encargados de realizar la interfaz con otras redes.

Los LSR son *Router* de gran velocidad en el núcleo de la red MPLS. Sus principales funciones son: participar en el establecimiento de los circuitos extremo-extremo de la red o LSPs ("*Label Switched Path*") usando un protocolo de señalización apropiado y conmutar rápidamente el tráfico de datos entre los caminos establecidos. Los LER son los *routers* situados en la frontera de la red. Son responsables de enviar el tráfico entrante a la red MPLS utilizando un protocolo de señalización de etiquetas y distribuir el tráfico saliente hacia las distintas redes destino. Los LERs se clasifican en nodos de entrada ("*ingress node*") y nodos de salida ("*egress node*").

Cuando un paquete entra a una red MPLS, se le asigna un determinado FEC ("*Forwarding Equivalency Class*"). Un FEC es un conjunto de paquetes que comparten las mismas características para su transporte, así todos recibirán el mismo tratamiento en su camino hacia el destino. Cada FEC puede representar requerimientos de servicio para un conjunto de paquetes o para una dirección fija. La clase FEC a la cual se asigna el paquete se codifica como un valor corto de longitud fija conocido como etiqueta. Esta etiqueta es usada por los conmutadores de la red para encaminar el paquete hacia su siguiente nodo. Cuando un paquete se envía a su siguiente *router*, la etiqueta es enviada con él. La etiqueta se usa como un índice en la tabla que especifica el próximo salto y una nueva etiqueta. La etiqueta vieja es sustituida por la nueva, y el paquete es enviado al salto siguiente [13]

2.4.2.1.1. Establecimiento de un LSP

Dentro de un dominio MPLS, un camino es establecido para que un paquete dado viaje con un determinado FEC. Existen dos mecanismos para establecer un LSP: encaminamiento salto a salto: cada LSR selecciona independientemente el próximo salto para un FEC

determinado. El LSR utiliza cualquier protocolo de encaminamiento disponible como OSPF, ATM PNNI ("*ATM Private Network-Node Interface*"),etc.; encaminamiento explícito: El LER de entrada determina la secuencia de saltos explícito desde la entrada hasta la salida. Puede que la ruta no esté completamente especificada, es decir, puede haber un conjunto de nodos que es representado como un único salto en la ruta. También puede contener un identificador de Sistema Autónomo que permita que el LSP sea encaminado a través de un área de la red que está fuera del control administrativo de quien inició el LSP. Dentro de estos dos casos se hará un encaminamiento salto a salto.

En la Figura 21, se pueden ver los componentes de una red MPLS y el establecimiento de un LSP.

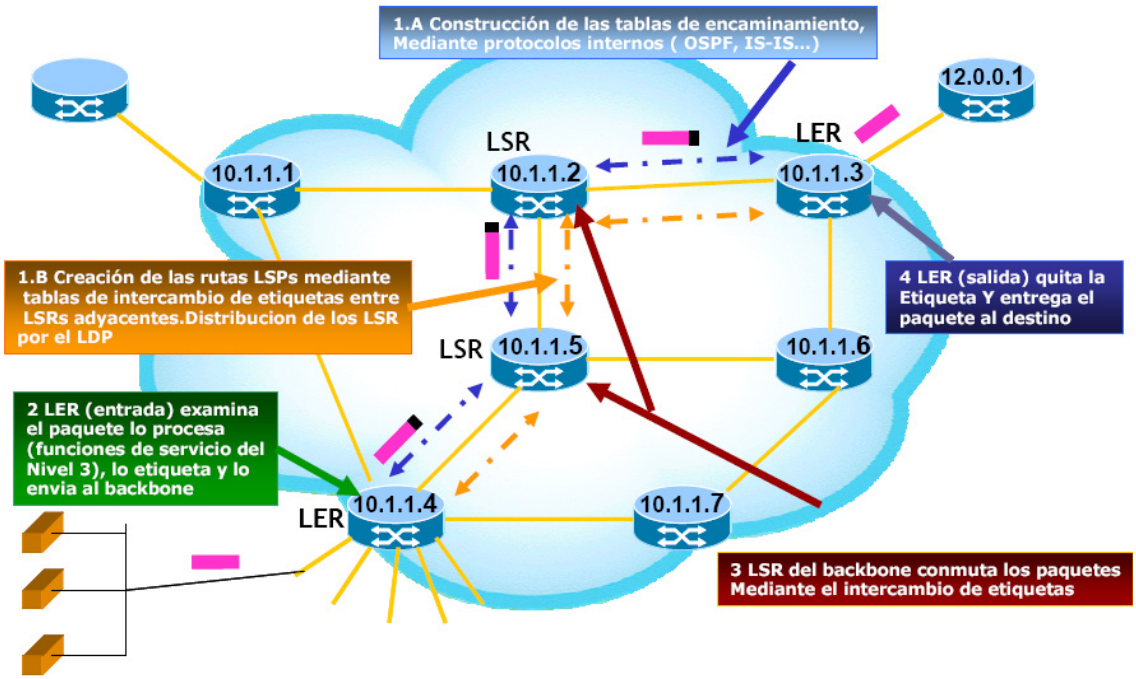


Figura 21.: Componentes de una red MPLS y establecimiento de un LSP

MPLS permite establecer LSP primarios y además establecer LSP de respaldo (backup) asociados a los de trabajo. El establecimiento de todos estos LSP se realiza usando algoritmos de encaminamiento con calidad de servicio que buscan la ruta óptima, tanto desde el punto de vista de la calidad de servicio requerida como desde el punto de vista del uso de los recursos de la red. A partir de este punto la gestión de recursos básicamente se

encarga de ajustar los LSP establecidos en la red adaptándolos al uso real que se esté haciendo de ellos.

Para conseguir esta adaptación al tráfico real de la red, los mecanismos de ingeniería del tráfico deben realizar tareas de monitorización. Por lo tanto, se puede afirmar que los mecanismos de gestión de recursos están constantemente pendientes del estado real de la red y fuertemente relacionados con el establecimiento de LSP de trabajo y de respaldo con algoritmos de encaminamiento con calidad de servicio. Por este motivo, la gestión de recursos también cubre la detección de las alarmas en el momento en que se produce un fallo en la red y la activación de los LSP de respaldo, así como la monitorización del estado real de la red y procede a su adaptación (cambiando los LSP existentes) al tráfico real y a los posibles fallos que puedan surgir (activando los LSP de respaldo necesario). Una vez establecidos los LSP, éstos tendrán una cierta vida, corta o larga, durante la cual pueden sufrir una serie de problemas. Se puede establecer un LSP con un cierto ancho de banda asignado para una cierta cantidad de tráfico con una determinada calidad de servicio [15].

Sobre este LSP puede suceder que, al cabo de un cierto tiempo, la demanda de tráfico supere la reserva inicial y se produzca un rechazo de tráfico de entrada. Este rechazo o bloqueo se produce debido a algún tipo mecanismo de control de admisión, necesario para garantizar la calidad de servicio de las distintas conexiones existentes, y puede cuantificarse calculando la probabilidad de bloqueo para cada LSP. Otro fenómeno que puede suceder es que, una vez reservada una cierta cantidad de ancho de banda para un cierto LSP, después de cierto tiempo este LSP esté poco utilizado y se estén desperdiciando los recursos de la red, cuando posiblemente otros LSP puedan estar congestionados y rechazando tráfico.

La técnica habitual para adaptar el ancho de banda de los LSP al tráfico real es la reasignación de banda de los mismos, incrementándola o decrementándola según sea el caso. Para poder incrementar la banda de un LSP es necesario que a lo largo del camino que

sigue este LSP (los diferentes enlaces físicos que atraviesa) existan los suficientes recursos libres. Si esto no sucede, existen dos posibles acciones a tener en cuenta. La primera es buscar en qué enlaces físicos no se cumple la condición de que no exista suficiente banda disponible, y posteriormente, en estos enlaces comprobar si existe algún otro LSP infrautilizado y del que se pueda tomar la banda necesaria. En otras palabras, consiste en traspasar banda de LSP´s pocos usados a un LSP congestionado y que necesita incrementar su banda. La segunda posibilidad, en el caso de que la primera no sea posible, es reencaminar el LSP que necesita mayor ancho de banda a través de otro camino que pueda satisfacer sus necesidades. También en este caso, si no es posible reencaminar al LSP congestionado, existe la posibilidad de reencaminar uno o varios de los demás LSP con los que comparten los mismos enlaces físicos, con lo cual se liberan recursos y permite incrementar su banda. En los casos en los que hay que reencaminar LSP se puede hacer uso de los algoritmos de encaminamiento dinámicos y con calidad de servicio.

De ahí que estos mecanismos de gestión de recursos estén estrechamente relacionados con los mecanismos de establecimiento de LSP de trabajo y de respaldo con calidad de servicio, creando un entorno global de ingeniería del tráfico. Otro aspecto a tener en cuenta es qué mecanismos toman la decisión de adaptar la banda de los LSP y realizar las operaciones anteriormente descritas. Existen diferentes ejemplos en la literatura, y dependiendo de dónde se tome la decisión, se puede hablar de mecanismos centralizados o distribuidos. Estos mecanismos, por las tareas que realizan, se situarían dentro del plano de gestión. Tradicionalmente la gestión, en este caso de recursos y de fallos, se ha realizado de forma centralizada, lanzando algoritmos de optimización que, disponiendo de los datos de monitorización de toda la red, calculan la distribución óptima de los LSP. En redes troncales relativamente grandes, por las que circula gran cantidad de LSP, es muy difícil disponer de todos los datos de monitorización de forma centralizada y calcular la distribución óptima a tiempo antes de que el estado de la red ya haya cambiado. Una de las opciones que aparecen en la literatura reciente es tratar de mantener la distribución de LSP lo más

cercana posible a la óptima haciendo pequeños ajustes usando algoritmos distribuidos. La ventaja principal de los algoritmos distribuidos es que disponen de la información de forma local y permanentemente actualizada. Por el contrario, la desventaja está en que no se dispone de una visión global de la red. Por esta razón algunos algoritmos de este tipo se basan en distintas técnicas de inteligencia artificial y/o en distintas heurísticas para intentar realizar las mejores adaptaciones, aunque no se disponga de una completa información [16], [17] y [18].

2.4.2.1.2. Protocolo de Distribución de Etiquetas

Un protocolo de distribución de etiquetas es un conjunto de procedimientos por los cuales un *router* LSR informa a otro de la relación etiqueta/FEC que ha hecho. Dos *routers* LSR, que usan un protocolo de distribución de etiquetas para intercambiar la información de la etiqueta/FEC se les conoce como "puertos de distribución de etiquetas" respecto a la información que intercambian. Si dos *routers* LSR son puertos de distribución de etiquetas, se habla de que hay una "distribución de etiquetas adyacente" entre ellos [19]. El protocolo de distribución de etiquetas también abarca las negociaciones en el que dos puertos de distribución de etiquetas necesitan comunicarse con el fin de aprender de las posibilidades MPLS del otro.

Dependiendo de como se establezcan los LSP se pueden presentar diversas opciones: si se utiliza la aproximación salto a salto (*hop by hop*) para el establecimiento de los LSP la IETF ha recomendado (no obligatorio) el uso del protocolo LDP ("*label Distribution Protocols*") para la asignación de etiquetas, en este caso también se pueden utilizar los protocolos RSVP y CR-LDP. Si la estrategia utilizada es la "*downstream unsolicited*" donde el LER de salida distribuye las etiquetas que deben ser utilizadas para alcanzar un determinado destino, la única opción disponible es LDP.

Cuando la estrategia es "*downstream on demand*" iniciada por el LER de entrada y no se desea seguir el camino calculado paso a paso, sino que se desea utilizar el que permita definir una ruta explicita, las opciones actualmente disponibles son CR-LDP y RSVP.

2.4.2.1.2.1. El protocolo LDP

Es la opción recomendada aunque no obligatoria del IETF [20]. Para el intercambio de mensajes entre LSR´s se realiza mediante el envío de PDU´s de LDP. Este envío se basa en la utilización se sesiones LDP que se establecen sobre conexiones TCP. Es importante destacar que cada LDP PDU puede transportar más de un mensaje LDP, sin que estos mensajes tengan que tener relación entre ellos. El protocolo LDP utiliza el esquema de codificación de mensajes conocido como TLV (Tipo, Longitud, Valor), cada mensaje LDP tiene la siguiente estructura:

-U campo de un bit que indica el comportamiento en caso de recibir un mensaje desconocido. U=0 hay que responder con un mensaje de notificación al LSR origen, U=1 se ignora el mensaje y se continua procesando el PDU

-F Campo de un bit. Este campo sólo se utiliza cuando el bit U esta en 1. Si se recibe un mensaje desconocido que debe propagarse y el bit F está en cero, este mensaje no progresa al siguiente LSR, en caso contrario si se hace.

-Tipo Campo de 14 bits que define el tipo de mensaje y, por lo tanto indica cómo debe ser interpretado el campo valor.

-Longitud: campo de 2 octetos que especifica la longitud del campo valor

-Valor: Campo de longitud variable que contienen la información del mensaje. La interpretación de la cadena de octetos de este campo depende del contenido del campo tipo.

2.4.2.1.2.2. RSVP ("*Resource reservation Protocol*")

Para poder utilizar este protocolo en el entorno MPLS se le han agregado nuevas capacidades, estas se refieren a los objetos formatos de los paquetes y procedimientos necesarios para establecer los túneles LSP. Para el establecimiento de los túneles LSP el

protocolo de señalización utiliza el modelo *downstream on demand*. Esto significa que la petición de asociación entre el FEC y una etiqueta para crear un túnel LSP es iniciada por el LSR de entrada, para lograr este objetivo hay que agregar un objeto (*LABEL_REQUEST*) al mensaje del *path* propio de RSVP antes mencionado.

Un requisito adicional para este protocolo RSVP es que el dominio MPLS debe soportar el encaminamiento explicito ("*explicit routing*") para facilitar la gestión de tráfico. Para lograr esto se añade el objeto (*EXPLICIT_ROUTE*) en los mensajes del *path*. Este nuevo objeto encapsula el conjunto de nodos ordenados que constituyen la ruta explícita que deben seguir los datos. Como la asignación de etiquetas se realiza desde el destino hacia el origen, en sentido contrario al flujo de datos, es necesario incrementar el mensaje *resv* con un objeto adicional (*LABEL*) capaz de transportar la nueva información requerida para este uso del protocolo. El funcionamiento de este protocolo para el establecimiento de túneles LSP se describe a continuación:

-Cuando un LER de entrada al dominio MPLS decide que necesita establecer un LSP hasta un determinado LER de salida, debe iniciar un procedimiento para establecerlo, mediante un mensaje *path*. La ruta que debe seguir el LSP puede ser una ruta explícita determinada por el gestor de la red (esta ruta no puede coincidir con la calculada por los algoritmos de encaminamiento de la capa red).

-Cuando los LSR intermedios reciben el mensaje de *path* lo procesan de acuerdo con las especificaciones del protocolo y una vez reconocido que no son el extremo del FEC, transmiten el mensaje hacia el siguiente nodo de la ruta.

-Cuando el mensaje de *path* finalmente alcanza el LSE destino, éste procede a reservar los recursos internos, selecciona la etiqueta a utilizar para este túnel LSP y procede a propagarla hacia el anterior LSR mediante un mensaje de reserva (*resv*).

-Cuando los LSR´s intermedios reciben la asignación de la etiqueta con el mensaje de *resv* proceden a reservar los recursos internos necesarios y determinar la etiqueta a utilizar para el flujo. Una vez calculada la propagan para el LSR anterior de nuevo con ayuda del mensaje

resv. Este proceso se repite hasta alcanzar el LSR origen donde también se realiza el proceso de reservar recursos internos, pero en este caso no es necesario asignar etiqueta y propagarla ya que se ha alcanzado el origen del FEC

2.4.2.1.2.3. CR-LDP ("*Constraint-Based Routing label Distribution Protocol*")

Es un encaminamiento basado en restricciones ("*Constraint-based routing*"). Esta extensión del LDP se basa en el calculo de trayectos que están sujetos a ciertas restricciones: ancho de banda, los requisitos de calidad de servicios QoS, demora ("*delay*"), variación de demora o *jitter*, o cualquier otro requisito asociado al trayecto que defina el operador de la red. Esta es una de las herramientas más útiles para controlar el dimensionado del tráfico y la QoS en la red que pueden ofrecer a sus clientes y/o usuarios.

Debido a ello, el capítulo MPLS de la IETF ha elaborado las extensiones necesarias para que el protocolo LDP pueda soportar este tipo de encaminamiento esta extensión es conocida como CR-LDP ("*Constraint-Based Routing label Distribution Protocol*") y se ha definido expresamente para soportar el establecimiento y mantenimiento de LSP encaminados en forma explícita y las modificaciones de los LSP, pero no incluyen los algoritmos necesarios para calcular trayectos según los criterios definidos por el operador de la red [19].

Las principales limitaciones son las siguientes: solo se soportan LSP´s punto a punto; solo se soportan LSP´s unidireccionales; y, sólo se soporta una única etiqueta por LSP.

2.4.2.2. MPLAMBDAS (MPλS)

De forma general MPλS se considera como una extensión de MPLS que opera en el núcleo óptico. Como lo indica su nombre, en MPλS la longitud de onda de la luz es utilizada como etiqueta. MPλS puede ser considerada como una versión simplificada de MPLS ya que no cuenta con las facilidades de *stacking* de etiquetas o reenvío por paquetes. Existen algunas semejanzas funcionales entre los LSR´s y los conmutadores de longitud de onda, y entre un

LSP y un camino de canal óptico. Acorde a dicha analogía en una red MPLS un LSR se encarga de la conmutación de etiquetas, en tanto en una red MPλS un conmutador óptico conmuta longitudes de onda desde los puertos de entrada a los puertos de salida. Similar a como ocurre en los LSR´s, los conmutadores fotónicos necesitan para el cálculo del camino óptico protocolos de encaminamiento tales como OSPF e IS-IS para intercambiar información sobre los estados del enlace de la topología y sobre la disponibilidad de recursos ópticos. Igualmente ambas tecnologías necesitan protocolos de señalización, tales como RSVP y LDP para automatizar el proceso de establecimiento del camino [21] [22].

MPλS es un avance en la tecnología del plano de control aplicado a la capa óptica a través del uso de cross conectores ópticos (*OXC: Optical Cross Connect*). Esto permite a la capa óptica controlar partes de la capa IP y de la capa de acceso a la red. El propósito de MPλS es proporcionar aprovisionamiento en tiempo real de redes ópticas, desplegar clases versátiles de nuevos OXC, y usar semánticas uniformes para la gestión de red y operaciones de control en redes híbridas que consistan de OXC´s y LSR´s. MPλS permite a la red de transporte óptico tener funciones limitadas de una red en malla, haciendo posible la integración de redes de datos y ópticas. La Tabla 4., permite apreciar las similitudes y diferencias entre MPLS y MPλS.

MPLS	**ASPECTOS COMUNES DE CONTROL**	**MPλS**
Eléctrico	Encaminamiento: OSPF, IS-IS Señalización: CR-LDP, RSVP	Óptico
Nivel de Enlace de datos y Red		Nivel Físico
Conmutación de Etiquetas		Conmutación de longitudes de onda
Conmutación de Paquetes		Conmutación de circuitos

Tabla 4.: Comparación entre MPLS y MPλS

2.4.2.3. GMPLS

2.4.2.3.1. Generalidades

Para ejercer control con el nivel óptico, GMPLS ("*Generalized MPLS*") extiende el concepto de plano de control para abarcar los dominios de MPLS tales como SONET/SDH, ATM y Gigabit Ethernet. GMPLS es un paradigma de plano de control multipropósito que soporta no solamente dispositivos que realicen conmutación de paquetes, sino también dispositivos que

realicen conmutación en el dominio del tiempo (TDM), longitud de onda (Lambda) y espacio (Fibra/Puerto).

2.4.2.3.2. Plano de control GMPLS

El plano de control GMPLS permite un control total de los dispositivos de red. Dicho plano proporciona las siguientes funciones [25]:

- Descubrimiento de vecinos ("*Neighbor Discovery*"): Con el fin de poder gestionar la red de manera integral, la red GMPLS debe conocer todos los dispositivos que la conforman. Para descubrir los dispositivos y negociar sus funciones, utiliza un nuevo protocolo conocido como LMP ("*Link Management Protocol*").

- Distribución del estado de los enlaces ("*Dissemination of Link Status*"): La información sobre el estado de la red (operación) se distribuye a través de protocolos de encaminamiento, tales como OSPF o IS-IS modificados.

- Gestión del estado de la tipología ("*Typology State Management*"): Los protocolos OSPF e IS-IS, pueden ser usados para controlar y gestionar la tipología del estado del enlace. – Gestión de trayecto ("*Path Management*"): Para establecer los trayectos extremo a extremo puede usar LDP, CR-LDP o RSVP.

- Gestión del Enlace ("*Link Management*"): En GMPLS se requiere tener capacidad para establecer y agregar canales ópticos. LMP extiende las funciones de MPLS en el plano óptico donde la construcción de los enlaces mejora la escalabilidad.

- Protección y Recuperación ("*Protection and Recovery*"): En GMPLS en lugar de tener un anillo de respaldo (*backup*) para el anillo primario como mecanismo de protección, la red crea una red en malla que permite tener diferentes caminos alternos

2.4.2.3.3. Capacidades de Conmutación en GMPLS

GMPLS generaliza a MPLS en el sentido que define etiquetas para conmutar diversos tipos de tráfico de capas 1, 2 o 3. Los nodos GMPLS pueden tener enlaces con una o más de las siguientes capacidades de conmutación:

-PSC: *Packet-Switched Capable*. Procesan tráfico de acuerdo a los límites de los paquetes, celdas, tramas. Pueden enviar datos basándose en el contenido de la cabecera de paquete. Los LSP´s son conmutados entre dos dispositivos basados en paquetes, tales como GSRs o conmutadores ATM.

-L2SC: *Layer-2 Switched Capable*. Estas capacidades reconocen los límites de tramas/celdas y pueden enviar datos basándose en el contenido de la cabecera de las tramas/celdas.

-TDM: *Time-Division Multiplex Switched Capable*. Procesan el tráfico basándose en la ranura temporal de los datos dentro de un ciclo de repetición. Los LSP´s son conmutados entre dos dispositivos TDM, tales como Multiplexores *Add/Drop* SONET/SDH.

-LSC: *Lambda-Switched Capable*. Procesan el tráfico basándose en la longitud de onda sobre la que se reciben los datos. Los LSP´s son conmutados entre dos dispositivos DWDM, tales como OXC´s que operan a nivel de longitudes de onda individuales.

-FSC: *Fiber-Switched Capable*. Procesan el tráfico basándose en la interfaz física en que se reciben los datos (Fibra Óptica/puerto). Los LSP´s son conmutados entre dos dispositivos basados en fibra, tales como OXC´s que operan a nivel de fibras individuales.

La figura 22 muestra las capacidades de conmutación GMPLS.

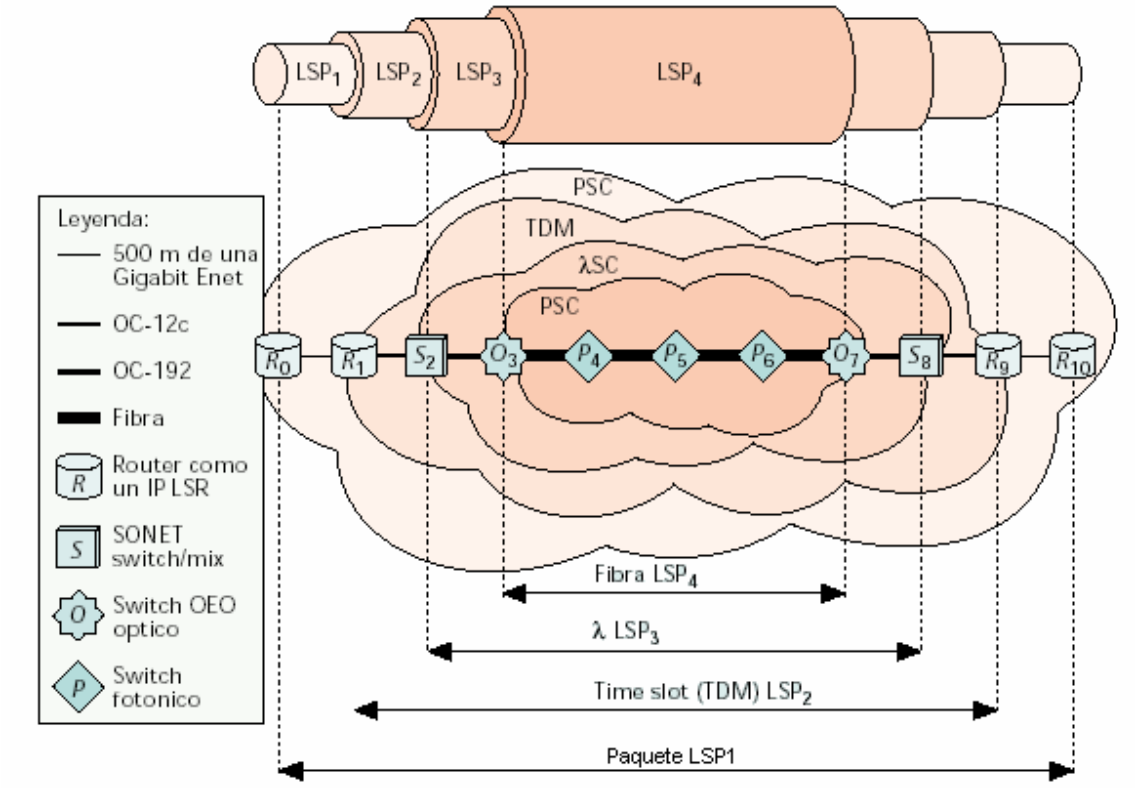


Figura 22.: Capacidades de conmutación GMPLS

Genéricamente todas las diversas clases de circuitos que se pueden establecer entre dos capacidades de conmutación del mismo tipo reciben el nombre de LSPs. Un LSP debe iniciar y terminar sobre enlaces con la misma capacidad de conmutación (interfaces del mismo tipo). Un LSP puede anidarse dentro de otro creándose una jerarquía de LSPs.

2.4.2.3.4. Señalización generalizada

La señalización GMPLS extiende ciertas funciones básicas de los protocolos de señalización RSVP-TE y CR-LDP y en algunos casos añade unas nuevas. Estos cambios afectan las propiedades básicas de los LSP´s respecto a cómo se solicitan y comunican las etiquetas, a la naturaleza unidireccional de los LSP´s, a cómo se propagan los errores y a la información proporcionada para sincronizar la entrada y la salida.

La especificación de la señalización GMPLS se compone de tres partes: una descripción de la funcionalidad de la señalización; extensiones RSVP-TE; y, extensiones CR_LDP.

La señalización GMPLS define sobre MPLS-TE los siguientes bloques constructivos: un nuevo formato genérico de solicitud de etiqueta; etiquetas para las interfaces TDM, LSC y FSC llamada Etiqueta Generalizada; soporte para la conmutación de una banda de longitudes de onda; sugerencia de etiqueta por el canal ascendente con propósitos de optimización; restricción de etiquetas por el canal ascendente para soportar restricciones ópticas; establecimiento de LSP´s bidireccionales con resolución de contiendas; extensiones para la rápida notificación de fallos; información de protección, centrándose realmente en la protección del enlace más indicación de LSP primario y secundario; enrutamiento explícito con control explícito de etiquetas para un grado de control fino; parámetros específicos de tráfico por tecnología; y, manejo del estado administrativo del enlace

2.4.2.3.5. Protección del enlace

La información de protección se transporta en un nuevo objeto/TLV ("*Time, Length, Value*") de la opcional ("*Protection Information*"). Este objeto indica la clase de protección deseada del enlace. Si se solicita un tipo particular de protección (1+1, 1:N, ...), sólo se procesa la petición de conexión si se puede garantizar dicha protección. GMPLS anuncia las posibilidades de protección de un enlace en los protocolos de enrutamiento. El algoritmo de cálculo del camino utiliza esta información para calcular los caminos y establecer un LSP. La información de protección también indica si el LSP es primario o secundario. Un LSP secundario es un backup para el LSP primario.

Actualmente hay definidos seis tipos de indicadores individuales de protección de enlace, los cuales también se pueden combinar, estos son: mejorado, dedicado 1+1, dedicado 1:1, compartido, no protegido, tráfico extra:

-Mejorado ("*enhanced*"): Indica que se debe utilizar un esquema de protección más fiable que el esquema dedicado 1+1.

-Dedicado 1+1: Indica que se debe utilizar un esquema de protección dedicado del nivel de enlace.

-Dedicado 1:1: Significa que se debe utilizar un esquema de protección del nivel de enlace dedicado 1:1, estos es protección 1:1, podría ser usada para soportar el LSP.

-Compartido ("*Shared*"): Indica que se debe utilizar un esquema de protección compartido del nivel de enlace, tal como protección 1:N, puede se utilizado para soportar el LSP.

-No protegido: Indica que el LSP no podría utilizar ningún esquema de protección del nivel de enlace.

-Tráfico Extra (*Extra Traffic*): Significa que el LSP podría utilizar enlaces que están destinados a proteger otro tráfico de alta prioridad. Dichos LSP´s pueden ser apropiados (*preemted*) cuando los enlaces que transportan tráfico de alta prioridad fallan.

2.4.2.3.6. Fases de implantación

No es necesario realizar toda la implantación de GMPLS en una determinada arquitectura de red. Para empezar, GMPLS puede desplegarse solamente en una capa del modelo tradicional de red "*overlay*", para posteriormente extenderse en sucesivas fases según se requiera, y mejorar, de este modo, la eficiencia de la red. El proceso de implantación de GMPLS se puede resumir en las siguientes fases:

Fase 0: supongamos que esta es la fase inicial en la que se encuentran la mayoría de las redes actuales basadas en un modelo "*overlay*". La red de servicios IP ejecuta protocolos IP/MPLS. Por otro lado, la red de transporte (SONET/SDH óptico) utiliza protocolos propietarios o de gestión de red para facilitar la configuración y el establecimiento de las conexiones entre los elementos de red. Las peticiones de establecimiento o de terminación de conexiones se realizan por vía telefónica o a través de un interfaz Web.

Fase 1: se diseña para aumentar la velocidad y la precisión de las peticiones de conexión, incrementando de este modo la eficiencia y flexibilidad de la red. Se automatizan las peticiones de la red de servicio a la red de transporte para el establecimiento y terminación

de conexiones. Para ello se utiliza un interfaz de señalización basado predominantemente en GMPLS.

Fase 2: consiste en la estandarización de los protocolos a través de las capas, acercando la red hacia un control integrado de las capas de servicio y transporte. En esta fase, los protocolos GMPLS sustituyen a los protocolos propietarios y de gestión de red en la red de transporte para facilitar el establecimiento de conexiones entre nodos.

Fase 3: esta es la fase final de la integración. Una vez que los operadores pueden aprovechar la eficiencia de una arquitectura de red con integración vertical, la integración del plano de control continúa. GMPLS es entonces el estándar para los protocolos de señalización y enrutamiento de todos los tipos de tráfico (longitudes de onda, TDM y paquetes) a través de la red de conmutadores. Todos los elementos de red tienen ahora conocimiento del resto de elementos de red que transporten cualquier tipo de tráfico. Finalmente, la eficiencia de los conmutadores se maximiza convenientemente mediante la instalación de una combinación óptima de tarjetas de línea para los diferentes tipos de servicios en función de la carga de tráfico.

3. IMPLEMENTACIÓN

3.1. DESCRIPCIÓN DEL CAPÍTULO

En este capítulo, se describen las etapas del trabajo realizado. Se comienza con una breve caracterización de los servicios de telecomunicaciones ofrecidos, las redes que les dan soporte, los requerimientos de tráfico y disponibilidad. Se continúa con la propuesta, una pequeña descripción del equipamiento a utilizar, diseño y construcción de las maquetas. Se desarrollan pruebas locales, de sistema y de servicios, obteniendo valores para el análisis.

3.2. TOPOLOGÍAS DE RED Y TRÁFICO

La diversidad de requerimientos de los clientes, tanto del segmento empresas como del segmento masivo, han presionado para que los operadores de servicios cuentes con redes que permitan ofrecer los enlaces requeridos. Esta necesidad ha producido en el tiempo, un sinnúmero de plataformas con tecnologías y funciones distintas. Entre las prestaciones más persistentes, podemos mencionar Telefonía (redes TDMs, E1s), Tráfico Internet (IP), TV (SDH), Datos Empresas (IP, ATM, Eth, SDH), las cuales están comenzando a integrarse con redes NGN pero que aún se soportan en gran medida con redes independientes.

Los servicios ofrecidos por la empresa son muy variados. Sin embargo, centraremos el análisis en los siguientes:

-Internet

-Servicios privados para Empresas

-Telefonía fija

-Internet: Básicamente, para enlazar al suscriptor a Internet, la línea de acceso del cliente se conecta a un DSLAM (*Digital Subscriber Line Access Multiplexer*). Los servicios telefónicos de banda estrecha sobre la línea continúan conectados al conmutador local. El DSLAM

agrega el tráfico de varios clientes y distribuye el flujo de tráfico a clientes individuales. El tráfico se canaliza en un SDH o línea ATM hacia el servidor remoto de acceso de banda ancha (BRAS), normalmente un ERX, que controla las sesiones, la calidad del servicio y los servicios que se prestan, así como información para la facturación. El BRAS provee acceso a la red IP del operador donde el RADIUS (*Remote Access Dial In User Server*) revisa la autenticación del cliente y asegura que tienen acceso a los servicios. Un *backbone* de *Routers*, (*GSR's Giga Switchs Routers*), trabajando bajo protocolo MPLS (conectados por enlaces dedicados o a través de la red de transporte SDH), da conectividad entre equipos de autenticación y agregación para permitir el acceso a Internet. La Figura 23 muestra el esquema de conexión.

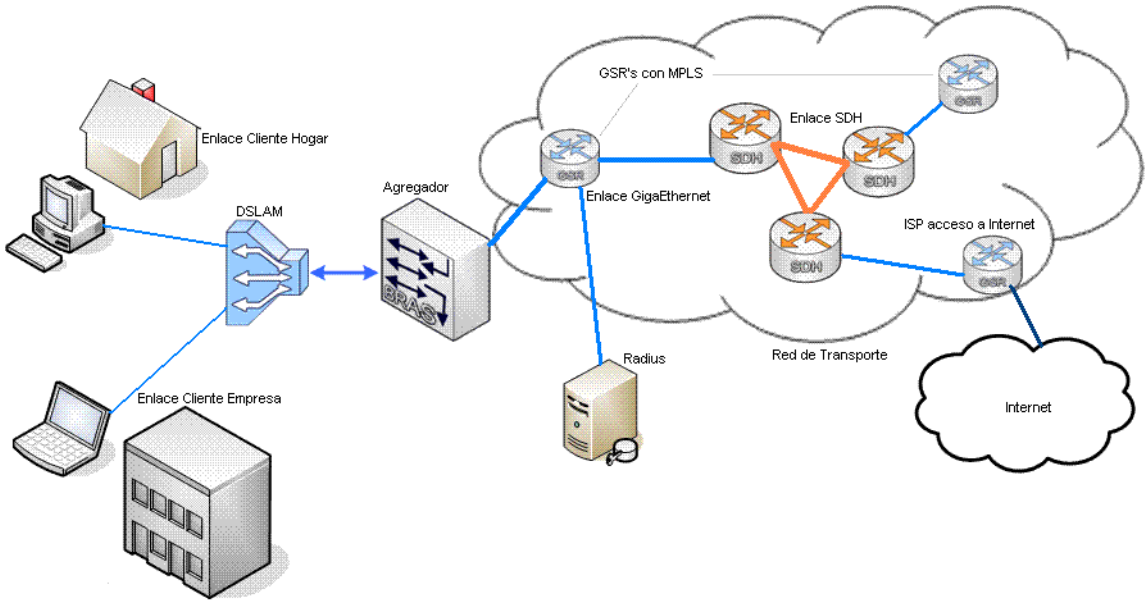


Figura 23.: Esquema de conexión a Internet

Esta es una red de muy gran envergadura, con equipos de muy altas prestaciones y que requieren enlaces respaldados y eficientes.

En la Figura 24 se muestra el frente de uno de los DSLAMs en servicio y en la Figura 25, se ve un ERX-1440, como los utilizados en la empresa

Figura 24.: DSLAM Alcatel en servicio

Figura 25.: BRAS Juniper (modelo ERX-1440)

Los equipos GSRs se interconectan regularmente con la red de transporte SDH por medio de interfaces POS (*packet over SONET*) o GigaEthernet. Los equipos SDH NGN, permiten ambas configuraciones. La transmisión se produce de manera transparente para los GSR's, los cuales utilizan los equipos sincrónicos como un medio físico mas. En la Figura 26 se muestra la interfaz POS de uno de los equipos GSR Cisco.

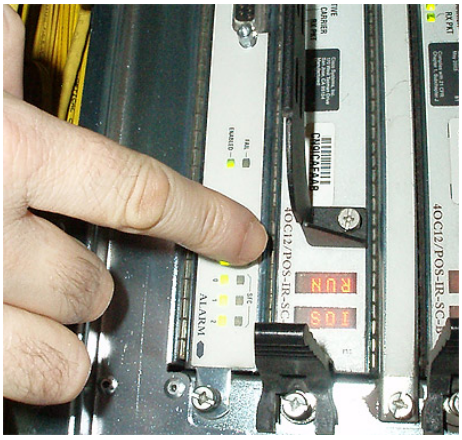


Figura 26.: Interfaz POS para conexión con SONET/SDH

-Los **Servicios privados para Empresas** corresponden a enlaces simétricos, VPN's y telefonía entregados a clientes. Dichos servicios son normalmente de capa 2, como Ethernet. En estos casos, el acceso desde el punto de entrada del cliente es por medio de conversores de medio y equipos Metro (como se vio con anterioridad en la introducción, Figura 2). Los dispositivos involucrados en esta configuración, son *Switchs Ethernet* y nuevamente SDH.

El esquema resumido de la red, se muestra en la Figura 27.

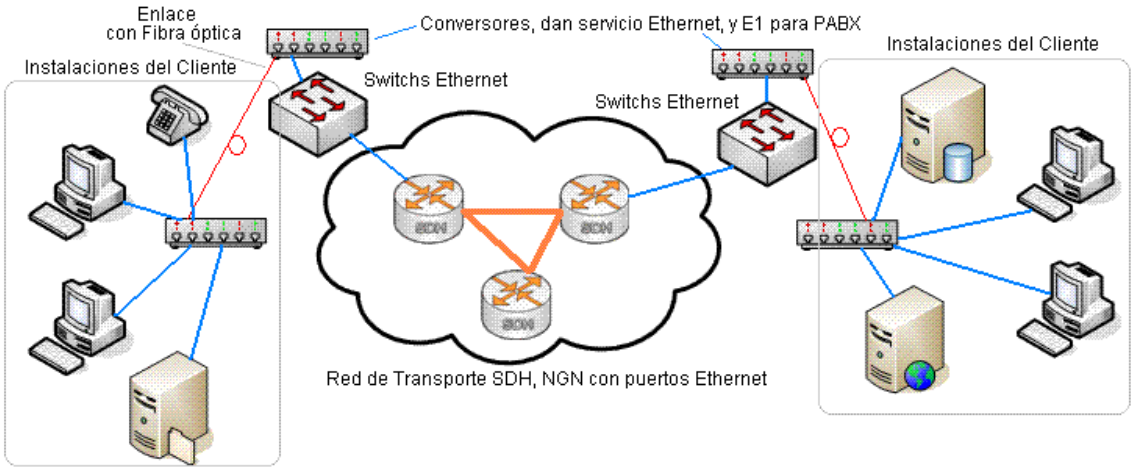
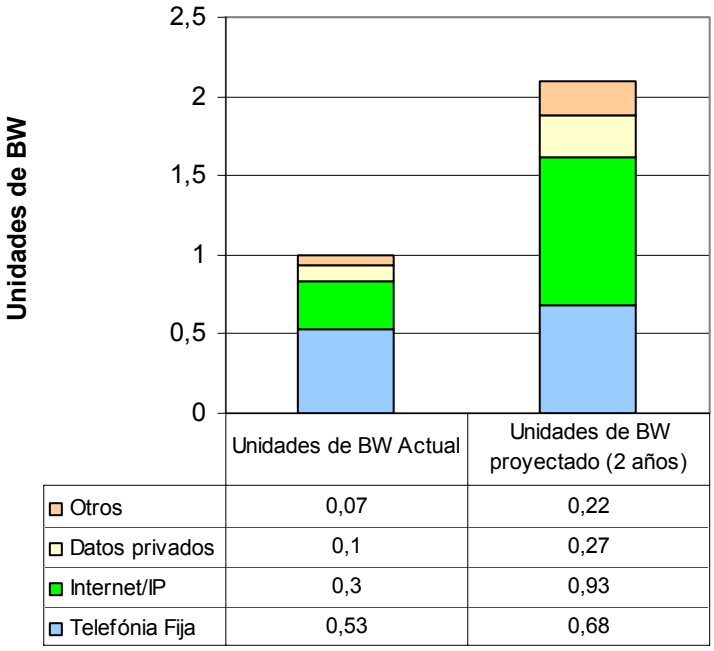


Figura 27.: Esquema de red con servicios a empresas

-La **Telefonía** fija utiliza centrales de conmutación que están entrelazadas en una compleja red de señalización y datos. La voz proveniente de las conversaciones telefónicas, es convertida en información digital. En este caso, la trama E1 consta en 31 divisiones (*time slots*) PCM ("*pulse code modulation*") de 64k cada una, lo cual hace un total de 30 líneas de teléfono normales mas 1 canal de señalización. Nuevamente, la red de transporte ejerce como medio físico para la comunicación de las centrales primarias de conmutación

Existen otros servicios (IPTV Televisión IP, Televisión Digital Satelital, Telefonía IP, Servicios dados por microondas y satélite) que son omitidos en este análisis, pues la criticidad y requerimientos de ellos, son equivalentes a los tratados.

En relación al tráfico involucrado, se analizó la información de los sistemas con los cuales se obtuvieron los resultados que muestra el gráfico de la Figura 28



	Unidades de BW Actual	Unidades de BW proyectado (2 años)
Otros	0,07	0,22
Datos privados	0,1	0,27
Internet/IP	0,3	0,93
Telefónia Fija	0,53	0,68

Figura 28.: Proyección de la cantidad y tipo de tráfico

Los datos fueron extrapolados con el crecimiento experimentado en los últimos años y las proyecciones de crecimiento e inversiones que se realizarán en los próximos dos años. Se toma como Unidad de BW, el actual nivel de tráfico (septiembre 2006).

A modo de ejemplo, se presenta el gráfico de tráfico de equipos GSR de borde, Figura 29.

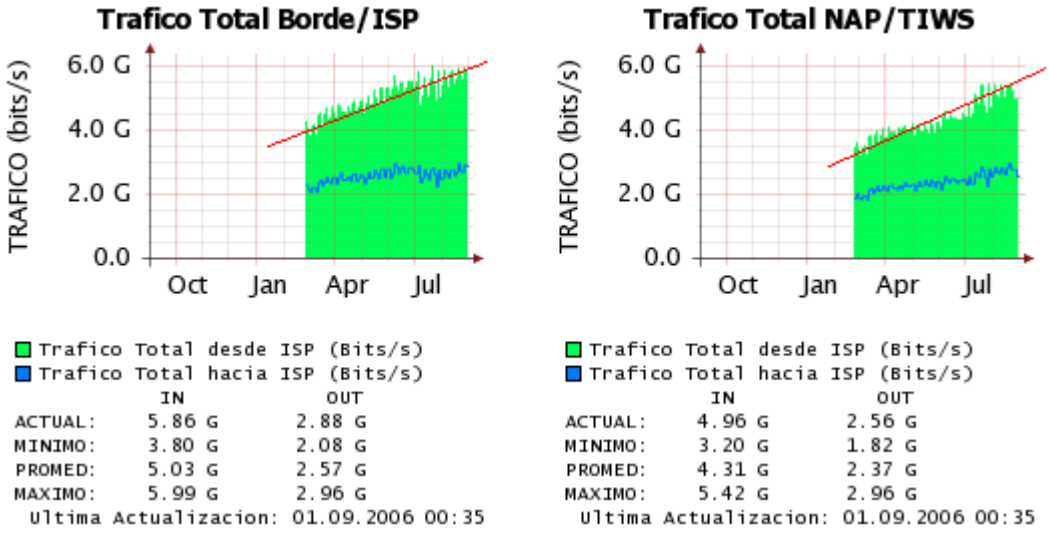


Figura 29.: Tráfico de equipos de borde

3.3. MAQUETAS

3.3.1. PROPUESTA DE TOPOLOGÍAS

El objetivo de este diseño, es probar la compatibilidad, robustez y escalabilidad de ASON frente al modelo actual (SDH con protección tradicional). También se aplica para ver los procedimientos y requisitos al momento de migrar hacia esta nueva red. Con esto en mente, se trabaja en tres configuraciones diferentes, las cuales involucran cuatro centrales en zona urbana de Santiago. La propuesta utiliza equipos de transporte Huawei OSN 3500 de los cuales se mencionan algunas características:

3.3.2. GENERALIDADES EQUIPOS HUAWEI OPTIX OSN 3500

El equipo OptiX OSN 3500 es un equipo de transmisión integrado que permite velocidades de 2.5G (STM-16) y 10G (STM-64) como interfaces de línea. Es una plataforma de transmisión multiservicios. Es compatible con las tradicionales redes SDH e integra además, muchas y variadas tecnologías, tales como PDH, Ethernet, WDW, ATM, y RPR entre otras tecnologías. Sus aplicaciones más comunes se orientan a los backbones de las redes de transmisión con la ventaja de que provee una completa solución para evolucionar desde las plataformas SDH existentes hacia redes ópticas de conmutación automática

3.3.2.1. CARACTERÍSTICAS

a) Plataforma económicamente eficiente:

-Las tarjetas para servicios y software de los equipos OptiX OSN de las series 7500/3500/2500/1500 son completamente compatibles, lo que permite unificar la plataforma. Esto reduce enormemente los costos de mantenimiento. Además, la plataforma, cuenta con la inteligencia para permitir la creación de redes mixtas con los existentes equipos Huawei los cuales podrían ser gestionados unificadamente.

b) Configuración flexible:

-Compatibilidad con STM-64/16

-Soporta actualización on-line de 2.5G a 10G

c) Alta capacidad en la planificación:

-Provee coss-connect de alto orden de 80G para VC-4, y cross-connect de bajo orden de 20G para VC-12, o equivalencias de VC3.

d) Provisión multiservicio

1) Interfaces

-STM-1 (O/E);

-STM-4/16/64 estandard o concatenados;

-E1/T1/E3/T3/E4;

-ATM

-IMA, SAN y otros

2) Provisto de protocolo GMPLS para servicios *end-to-end*

e) Alta integración

-Las dimensiones del subrack son 730mm (alto) x 496mm (Ancho) x 295mm (Fondo), soporta 15 posiciones para tarjetas de servicios y 16 posiciones para tarjetas de línea.

f) Robusto

-Soporta incorporación dinámica de nodos a la red enmallada y permite actualización y expansión en línea.

-Cada subrack puede habilitar anillos 1xSTM-64 de cuatro fibras o anillos 2xSTM-16 de cuatro fibras o anillos 4xSTM-16 de dos fibras

g) Tecnología WDM incorporada

-Provee dos canales ópticos para tarjetas ADM

h) Completos mecanismos de protección de red

-Recuperación de mallas

-Mecanismos distribuidos de recuperación de rutas de protección

-Incorpora cinco tipos de esquemas de servicios con SLA, *"diamond", "gold", "silver", "cooper" e "iron"*

-Protección SDH

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

-Protección de servicio de datos

-Soporta protección en anillo RPR y STP *spanning tree protection*;

-Soporta protección de anillo VP-RING para servicios ATM

i) Completos mecanismos de protección de equipo

-Control inteligente de unidades de protección 1+1 hot backup, tanto para elementos claves, incluida la cross-conectora, y reloj

-Protección de energía y térmico (TPS)

j) Características físicas

El equipo tiene las siguientes dimensiones: 730mm de alto, 496 mm de ancho y 295 mm de fondo. Pesa 18,6 Kgs y tiene un consumo máximo de 390 Watts. Ver Figura 30:

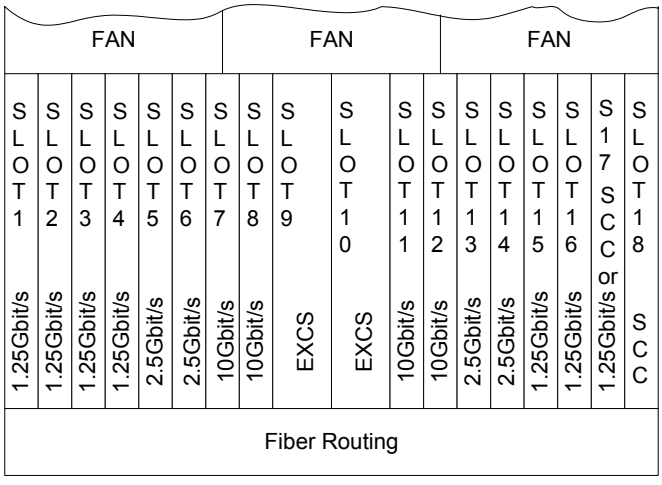


Figura 30.: Equipo OptiX OSN 3500 y un esquema de acceso en chasis inferior

3.3.2.2. NIVELES DE SERVICIO ASON EN EQUIPOS HUAWEI OSN 3500

Las redes ASON soportan la función de SLA y cuentan con varias alternativas de niveles de Calidad de Servicio. De acuerdo a los distintos tipos de prestaciones, el esquema de reconstrucción de enlaces puede operar en tres niveles de calidad: "*Diamond*", "*Gold*" y "*Silver*".

Un servicio de nivel "*Diamond*" provee "conexiones permanentes" (PC) 1+1. A nivel SDH, esta opera bajo protección SNCP Si se corta la fibra por donde está pasando el tráfico, el servicio conmutará el tráfico a la fibra de respaldo en menos de 50ms. Al mismo tiempo, el sistema buscará una nueva ruta de protección para el enlace. Este nivel es usado principalmente para tráfico de muy alta prioridad, Clientes estratégicos, gobierno, fuerzas armadas y todo enlace crítico para la empresa.

El nivel "*Gold*" utiliza "conexiones lógicas permanentes" 1:1. A nivel de SDH, la protección opera en anillos MSPRING. En este tipo de conexiones el servicio es configurado previamente por el operador. Los tiempos de conmutación son menores a 50ms. Se utiliza este tipo de calidad para prestaciones como ATM, POS, TDM y líneas privadas.

Nivel "*Silver*" provee protección de ruta conmutada, es decir, la restauración se produce en tiempo real. Los tiempos de conmutación fluctúan entre 60ms y 400ms. Es eficiente en servicios no críticos.

Existen dos clasificaciones más, "*Cooper*" e "*Iron*", las cuales no proveen protección pero permiten utilizar el ancho de banda disponible de la red.

La Tabla 5 hace una comparación de los niveles de servicios de ASON Huawei

	"Diamond"	*"Gold"*	*"Silver"*	*"Cooper"*	*"Iron"*
Nivel de Servicio	☆☆☆☆☆	☆☆☆☆	☆☆☆	☆☆	☆
Política de protección	SNCP y restauración	MSPRING y restauración	Restauración automática	Sin protección	Sin protección, capacidad ociosa
Tiempo de conmutación	< 5ms	Protección < 50ms, restauración < 2s	< 2s	-	-
Ocupación de Ancho de Banda	Alto	Media	Media/Baja	Bajo	Muy bajo
Uso	Tráfico Internet a ISP, Enlaces Críticos	Tráfico telefónico Grandes clientes	Datos clientes	Respaldos SDH tradicionales	Servicios temporales Despachos TV

Tabla 5.: Cuadro comparativo de los niveles de servicio ASON de Huawei

3.3.2.3. SELECCIÓN DE TRÁFICO Y NIVELES DE SERVICIOS

La selección del tráfico se hace en función del análisis de tráfico anterior. Teniendo en cuenta que los tráficos más críticos, son los estratégicos para la compañía, estos serán los que tendrán un tratamiento preferencial. Tráfico Internet a los ISP ("*Internet Service Provider*"), y enlaces internos críticos para la operación son priorizados y configurados en ASON como servicios "*Diamond*" y se representan en las maquetas como GigaEthernet que son configurados para ser trasladados por 8 tramas STM-1 (8xSTM-1).

Las prestaciones a grandes clientes, gobierno, instituciones militares y otros de mucha importancia, son configuradas con nivel "*Gold*". Ellos se representan como GigaEthernet compuesto por 4 tramas STM-1 (4xSTM-1). Los servicios de menor prioridad y que requieren de rutas respaldadas son transportados por tributarios de alta jerarquía STM-1 con nivel de servicio "*Silver*".

En la Figura 31 se representan los enlaces y sus niveles de servicio:

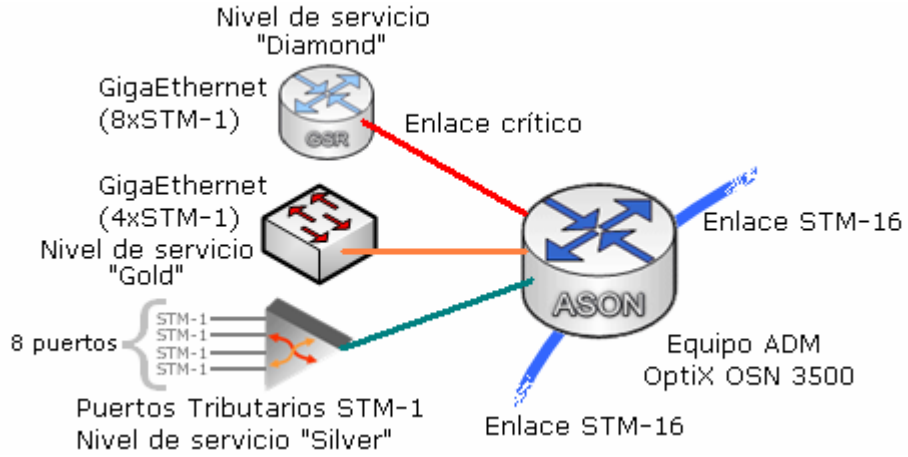


Figura 31.: Niveles de servicios ASON en las maquetas

3.3.3. CONFIGURACIÓN DE LAS MAQUETAS DE TRABAJO

1) Maqueta1 con equipos SDH Huawei 3500 NGN: En esta configuración, existen dos anillos adyacentes con protección MS-SPRing. Las tarjetas de línea son STM-16 y conectan centrales urbanas en Santiago. Las curvas entre los equipos, representan los enlaces de las tarjetas de línea y están numeradas del 1 al 6. La comunicación utiliza dos fibras, una para transmisión y otra pare recepción, por lo que las fibras se individualizan con la notación X.Y, en donde X representa el enlace (1 a 6) e Y representa la fibra (1=Transmisión, 2=Recepción). En esta primera configuración, cada uno de los servicios que conforman el tráfico, están respaldados y no existe uno con más prioridad que otro. La Figura 32 representa esta maqueta:

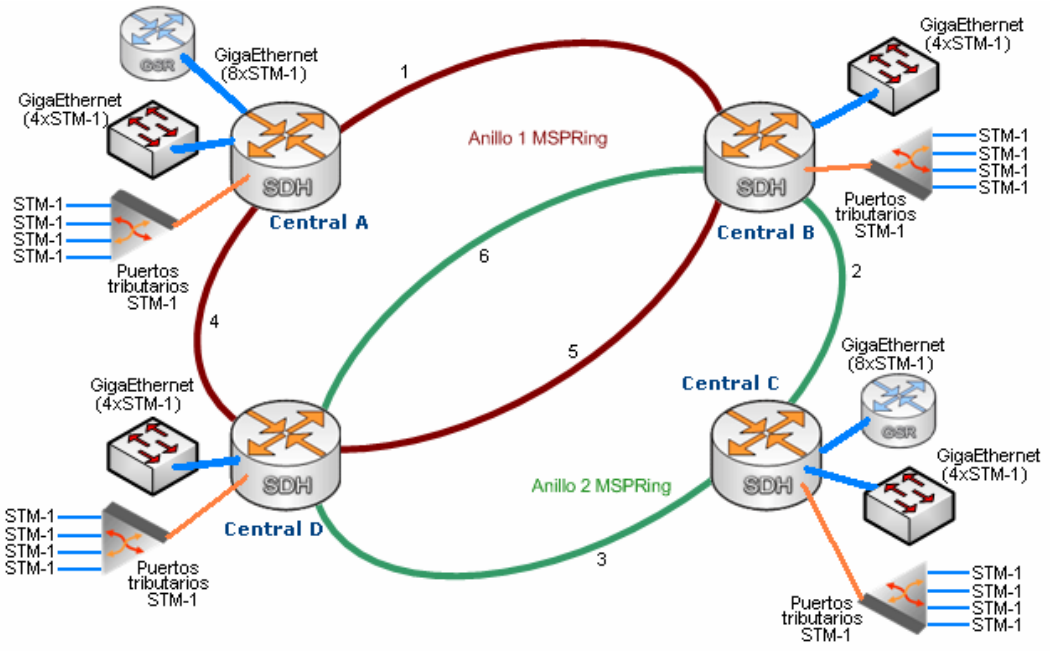


Figura 32.: Esquema de maqueta 1 (anillos adyacentes en sistema SDH)

2) Maqueta2 con Equipos ASON Huawei 3500 (cambio de controladora), configuración equivalente: Se les cambia la controladora a los equipos Huawei, esto permite que las máquinas funcionen como ASON, integrando en el sistema operativo el protocolo GMPLS para Ingeniería de Tráfico. La topología de la red no es alterada con respecto al caso 1. Los enlaces mantienen la misma numeración que en el caso anterior y los servicios están configurados con los niveles de servicio ASON mostrados en la Figura 31. La Figura 33 representa esta maqueta:

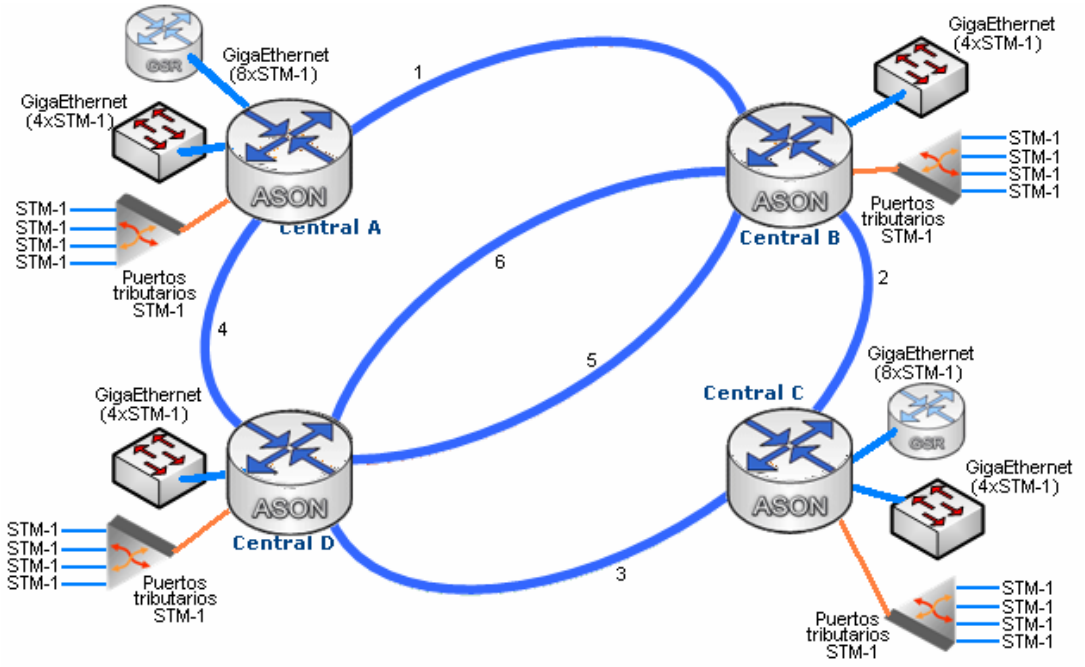


Figura 33.: Esquema de maqueta 2 (ASON con enmallado parcial)

3) Maqueta con Equipos ASON Huawei 3500 (cambio de controladora), configuración mejorada: con el Hardware actualizado de la configuración 2, se cambian de equipos, dos tarjetas de línea STM-16. Con ello se logra una red totalmente enmallada (*full mesh*). La numeración de los enlaces entre tarjetas de línea cambia ligeramente. En este caso el enlace 6 es desde el Nodo de la central A, al nodo de la Central C.

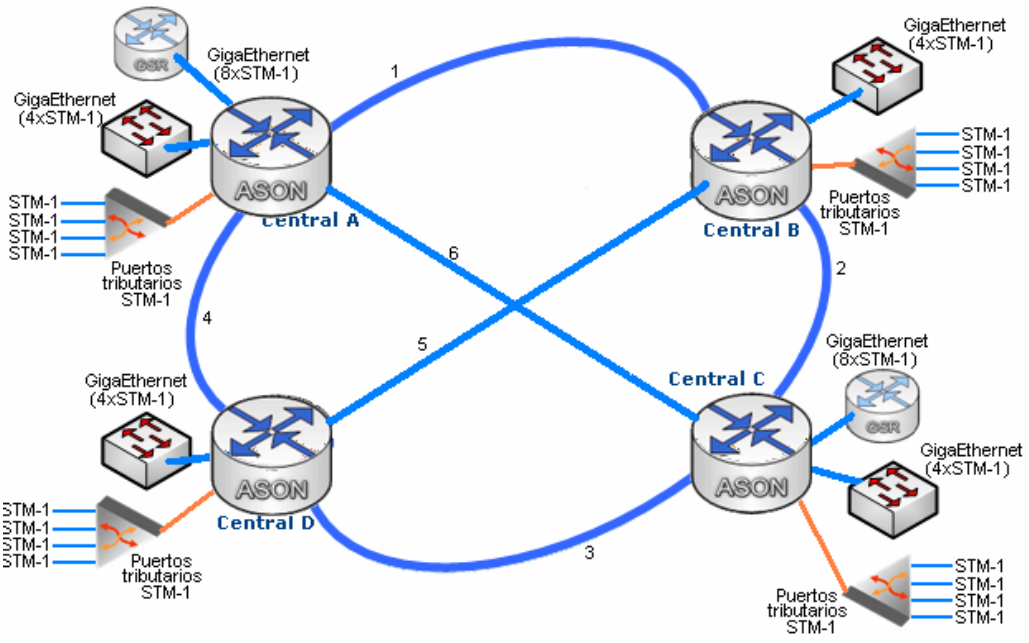


Figura 34.: Esquema de maqueta 3 (ASON *Full Mesh*)

3.3.4. ASPECTOS LOGÍSTICOS PARA LA CONSTRUCCIÓN

Para crear las configuraciones propuestas en la sección anterior, es necesario contar con condiciones técnicas adecuadas. Los aspectos más críticos en este caso son: la fibra óptica, la cual debe ser la adecuada para el tipo de señal a enviar (STM-16) y además requiere una atenuación máxima; la energía, pues se requiere contar con alimentación estable y segura en cada central; el espacio físico, ya que debe existir un lugar adecuado para instalar los chasis de equipos; y, la climatización, pues es necesario que estas máquinas funcionen en rangos de temperatura bien especificados. Existen muchos otros detalles importantes que contemplar, solo se comentan los mencionados:

-**Fibra óptica**: Si bien se cuenta con disponibilidad de fibra para crear los enlaces, esta debe ser verificada para comprobar que los niveles de atenuación, PMD y otros efectos indeseados, estén en los rangos aceptables. Para realizar las mediciones y selección de las fibras, se utilizó una herramienta de supervisión de fibra óptica (ISFO) y, además, un espectrómetro, para verificación.

La Figura 35 muestra una lectura de dicho sistema y la Figura 36 nos muestra un reflectómetro EXFO, similar al utilizado para verificar las fibras seleccionadas.

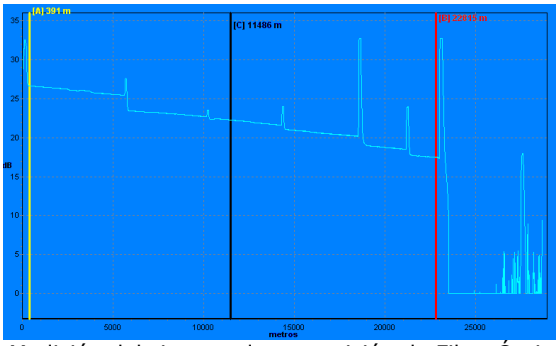


Figura 35.: Medición del sistema de supervisión de Fibra Óptica (ISFO)

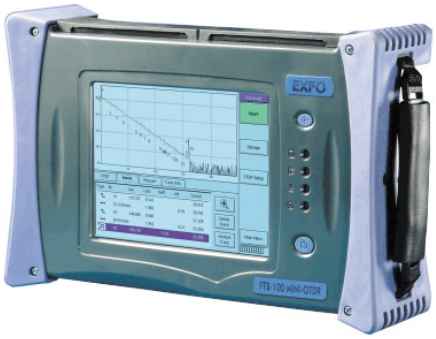


Figura 36.: Reflectómetro EXFO utilizado para verificar las fibras

Luego de escoger las fibras, se verificaron en lo que respecta a su atenuación y potencia de llegada.

Los resultados de las mediciones se muestran en la Tabla 6, en donde los orígenes y destinos, son las centrales definidas en los esquemas de las maquetas.

Fibras	Desde	Hasta	Maqueta	Atenuación (db)
1.1	A	B	1, 2 y 3	-10
1.2	A	B	1, 2 y 3	-9.5
2.1	B	C	1, 2 y 3	-8.7
2.2	B	C	1, 2 y 3	-9.3
3.1	C	D	1, 2 y 3	-11.2
3.2	C	D	1, 2 y 3	-11.0
4.1	D	A	1, 2 y 3	-6.5
4.2	D	A	1, 2 y 3	-6.7
5.1	B	D	1, 2 y 3	-10.2
5.2	B	D	1, 2 y 3	-11.3
6.1	B	D	1 y 2	-10.8
6.2	B	D	1 y 2	-10.3
6.1	A	C	3	-9.6
6.2	A	C	3	-8.8

Tabla 6.: Medidas de atenuación de fibras ínter centrales

-**Energía**: Los equipos modernos no consumen gran cantidad de energía, sin embargo, una sala de quipos puede tener cientos, y todos son importantes, por lo que, el tema de la alimentación es muy delicado.

Si bien la energía esta disponible, es necesario verificar su correcto funcionamiento y protección. Los equipos Huawei OSN 3500, funcionan con -48Vcc. Con fuentes redundantes, y tarjetas duplicadas.

La Figura 37, muestra el tablero de energía existente en la sala de equipos de la Central A.

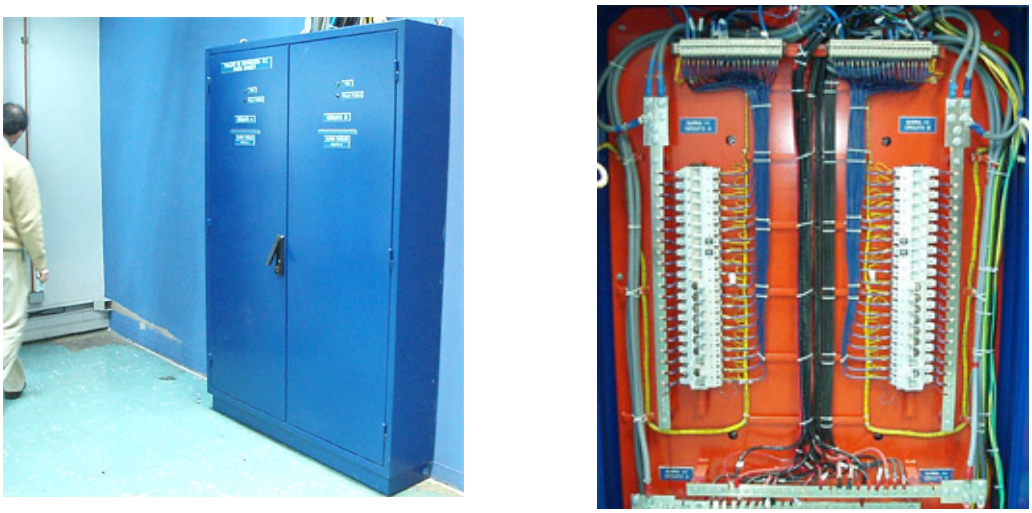


Figura 37.: Tablero de potencia (vista exterior e interior)

-**Espacio Físico**: El equipo necesita de la instalación de un bastidor en donde residen los chasis y los paneles de energía. En este caso, la ubicación ya estaba determinada pues los bastidores ya estaban instalados en las salas. La Figura 38 muestra el bastidor de equipos.

Figura 38.: Bastidor Huawei y vista de Panel de energía

-**Climatización**: Los equipos de climatización deben mantener una temperatura de trabajo adecuada para el equipamiento electrónico. Esta temperatura es normalmente de 19°C. En la Figura 39 se muestra el imponente sistema de climatización de la sala de equipos.

Figura 39.: Equipo de climatización y vista de Panel de control

3.3.5. MONTAJE Y PREPARATIVOS PREVIOS

Existiendo todo lo necesario en la sala de equipos de la central, ahora se debe verificar que los elementos propios del equipo también estén en orden. Es así como se verifica que las tarjetas de energía, las cuales deben estar duplicadas, funcionen correctamente. Otras tarjetas que deben estar respaldadas son: La de Cross-conexiones y la controladora. Esta última, será reemplazada por una tarjeta ASON para el mismo chasis.

En la Figura 40 se muestran algunas tarjetas del equipo.

Figura 40.: Tarjetas de equipo, energía y vista de controladoras

Además, es necesario realizar algunas pruebas de comunicación, configuración de la gestión del equipo y potencias de Transmisión. También se efectúan pruebas SDH, las que consideran Mediciones de potencia, tasas de error, sincronización, funcionamiento de canales de servicio y conmutación por fallas.

3.4. PRUEBAS DE SERVICIOS

Las pruebas de servicio nos entregan los resultados necesarios para hacer el análisis del comportamiento de la red con y sin ASON. Cada uno de los escenarios propuestos en la sección 3.3.1, será sometido a cortes controlados con el propósito de medir los tiempos de conmutación y la persistencia de los servicios.

-Se somete a prueba la **maqueta 1**, la que es un arreglo de anillos MS-PRING, que por su característica de protección, dispone solo de 8 STM-1 (de los 16) para tráfico regular por interfaz de línea. Los otros 8, están reservados para respaldo. En la Figura 41, se muestra nuevamente la primera configuración, en donde se destacan dos puntos con círculos **1** y **5**, que representan las secciones de fibra que serán abiertas para simular cortes.

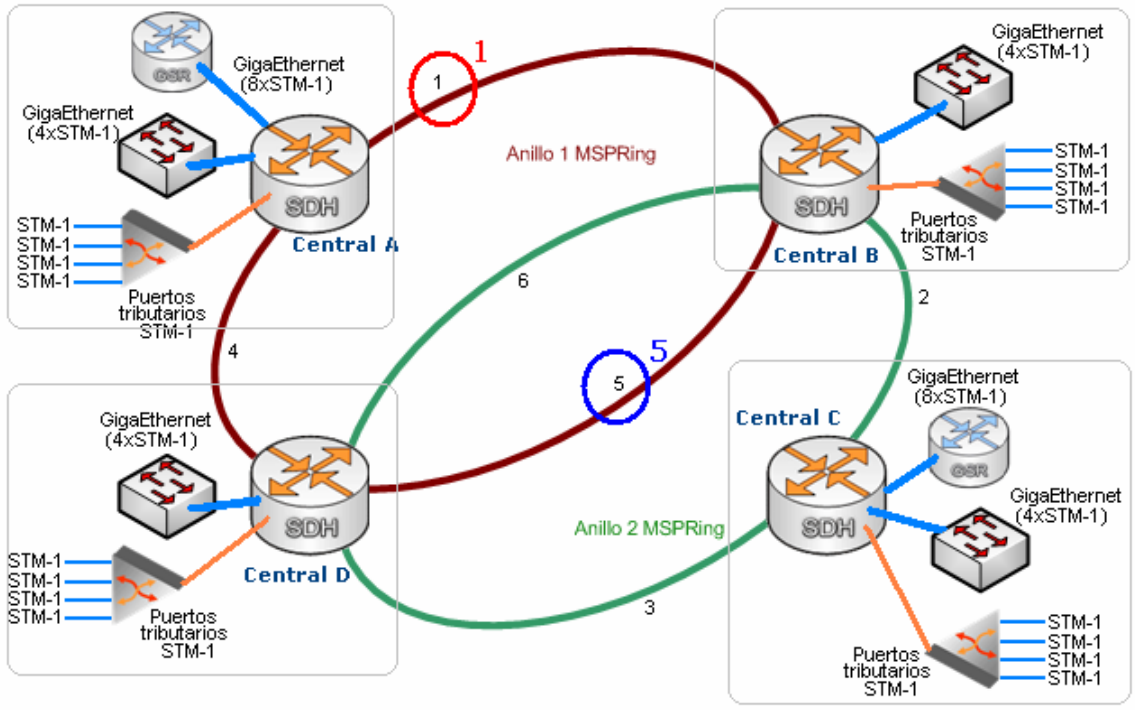


Figura 41.: Esquema general de maqueta 1 con puntos de intervención

Las pruebas de equipos y de sistema son realizadas en conjunto con el proveedor. En los Apéndices el lector podrá revisar algunos de los formularios utilizados para este efecto.

En la Tabla 7 se describen los servicios configurados en los equipos de la maqueta1

Central	Servicio	Trayecto
A	GigaEthernet (8xSTM-1)	A→B→C
A	GigaEthernet (4xSTM-1)	A→D→C
A	4 STM-1 con tráfico variado	A→D→B
B	4 STM-1	B→D→C
B	2 STM-1	B→D→C
B	GigaEthernet (4xSTM-1)	B→D

Tabla 7.: Descripción de servicios maqueta 1

La ocupación de la capacidad total de la estructura se muestra en la Tabla 8

Enlace	Capacidad utilizada	Capacidad Máxima
1	8	8
2	8	8
3	8	8
4	8	8
5	4	8
6	8	8

Tabla 8.: Tabla de ocupación de los enlaces

Al realizar los cortes en el sistema, hemos de realizar las mediciones para determinar los tiempos de conmutación y continuidad de servicio. Los resultados se muestran en la Tabla 9

Central	Servicio	Corte en 1		Cortes en 1 y 5	
		Estado	Tiempo de conmutación	Estado	Tiempo de conmutación
A	GigaEthernet (8xSTM-1)	OK, conmuta y toma ruta A→D→B	39ms	FALLO	-
A	GigaEthernet (4xSTM-1)	OK	-	OK	-
A	4 STM-1	OK	-	OK	-
B	4 STM-1	OK	-	FALLO	-
B	2 STM-1	OK	-	OK	-
B	GigaEthernet (4xSTM-1)	OK	-	OK	-

Tabla 9.: Tabla de resultados pruebas de corte en maqueta 1

-Se somete a prueba la **maqueta 2**, la cual es la misma topología de la anterior, solo se intervienen las tarjetas controladoras de los equipos OSN 3500 para dar soporte ASON. Se mantiene el mismo nivel de tráfico y los mismos servicios, pero se configuran con los niveles de protección ASON expuestos en la Tabla 10 En la Figura 42 se muestra la configuración,

en donde se destacan cuatro puntos **1, 2, 5 y 6** que representan las secciones de fibra que serán abiertas para simular cortes.

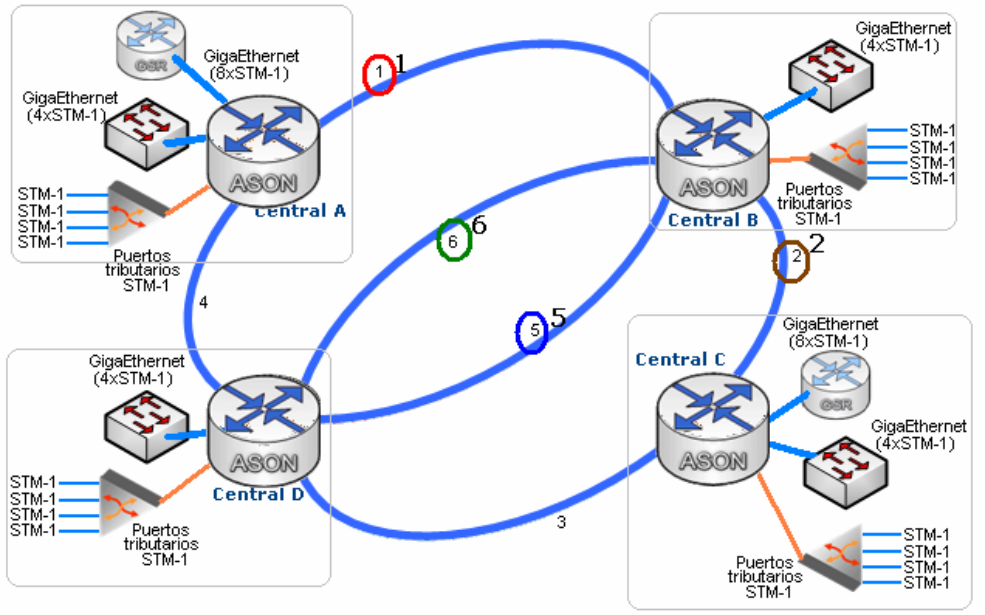


Figura 42.: Esquema general de maqueta 2 con puntos de intervención

En la Tabla 10 se describen los servicios configurados en los equipos de la maqueta2.

Central	Servicio	Trayecto
A	GigaEthernet (8xSTM-1) *"Diamond"*	A→B→C y A→D→C
A	GigaEthernet (4xSTM-1) *"Gold"*	A→D→C
A	4 STM-1 con tráfico variado *"Silver"*	A→D→B
B	4 STM-1 *"Silver"*	B→D→C
B	2 STM-1 *"Silver"*	B→D→C
B	GigaEthernet (4xSTM-1) *"Gold"*	B→D

Tabla 10.: Descripción de servicios maqueta 2

La ocupación ahora es diferente, el sistema cuenta con los enlaces STM-16 completos. Solo dos de los seis enlaces (3 y 4) están reservados por el enlace "*Diamond*"

Al realizar los cortes, esta vez, se pone atención al servicio GigaEthernet(8xSTM-1) el cual es configurado con alta prioridad ("*Diamond*").

Los resultados se muestran en la Tabla 11

Central	Servicio	Conmutación y Fallo
A	GigaEthernet (8xSTM-1) *"Diamond"*	-Corte en 1: Produce conmutación con tiempo < 3ms. -Corte en1 y en 5 →OK -Corte en1, en 5, y en 2 →OK -Corte en1, en 5, en 2, y en 6 → OK
A	GigaEthernet (4xSTM-1) *"Gold"*	-Corte en 1: Produce conmutación con tiempo < 50ms. -Corte en1 y en 5 →OK -Corte en1, en 5, y en 2 →OK -Corte en1, en 5, en 2, y en 6 → OK
A	4 STM-1 *"Silver"*	Corte en 1, en 5, en 2, y en 6 → FALLO

Tabla 11.: Tabla de resultados pruebas de corte maqueta 2

-Se somete a prueba la **maqueta 3**, la cual es levemente diferente a la anterior. En este caso, se traslado una tarjeta de línea desde la central D a la central A y otra desde la central B a la central C. Con este cambio, se encuentran todos los equipos con el mismo número de Interfaces de línea. El procedimiento de retiro e inserción de tarjetas se realiza con los equipos en operación y con los servicios activos, produciéndose conmutación en alguno de los enlaces, del orden de 4ms. En la Figura 43, se muestra la configuración, en donde se destacan dos puntos **1, 2, 3, 4 y 5** que representan las secciones de fibra que serán abiertas para simular cortes.

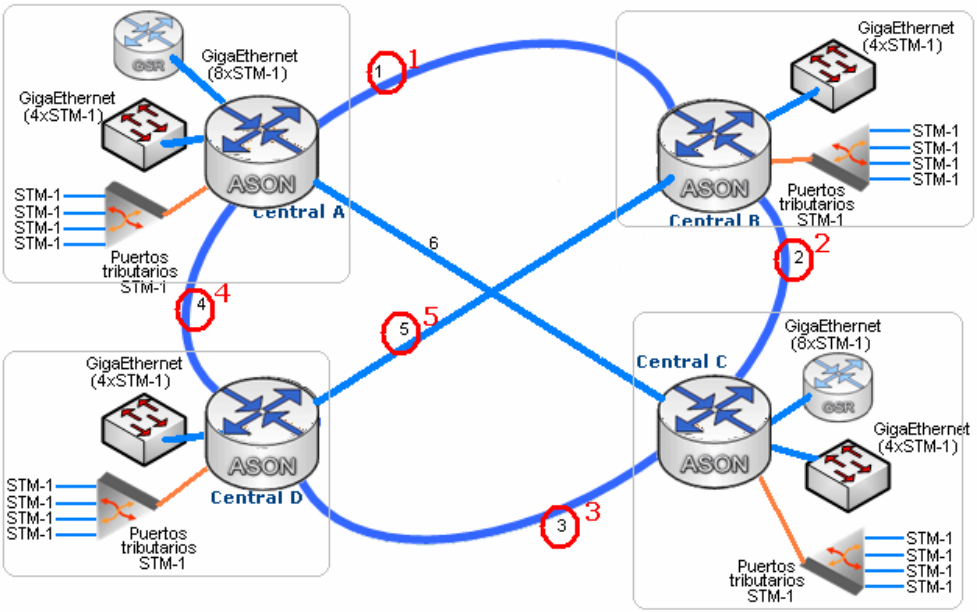


Figura 43.: Esquema general de maqueta 3 con puntos de intervención

En la Tabla 12 se describen los servicios configurados en los equipos de la maqueta 3.

Central	Servicio	Trayecto
A	GigaEthernet (8xSTM-1) "Diamond"	A→C y A→D→C
A	GigaEthernet (4xSTM-1) "Gold"	A→C
A	4 STM-1 con tráfico variado "Silver"	A→B
B	4 STM-1 "Silver"	B→C
B	2 STM-1 "Silver"	B→C
B	GigaEthernet (4xSTM-1) "Gold"	B→D

Tabla 12.: Descripción de servicios maqueta 3

Al realizar los cortes, nuevamente se pone atención al servicio GigaEthernet(8xSTM-1) el cual es configurado con alta prioridad (*Diamond*). Los resultados se muestran en la Tabla 13

Central	Servicio	Conmutación y Fallo
A	GigaEthernet (8xSTM-1) "*Diamond*"	-Corte en 1: OK -Corte en 1 y en 5 →OK -Corte en 1, en 5 y en 2 →OK -Corte en 1, en 5, en 2 y en 3→ OK -Corte en 1, en 5, en 2, en 3 y en 4 →Servicio OK, alarma por falla en creación de ruta de respaldo
A	GigaEthernet (4xSTM-1) "*Gold*"	-Corte en 1, en 5, en 2, en 3 y en 4 →Servicio OK, alarma por falla en creación de ruta de respaldo

Tabla 13.: Tabla de resultados pruebas de corte maqueta 3

El Servicio GigaEthernet (8xSTM-1) configurado con muy alta prioridad, se mantiene, sin conmutaciones después de los 5 cortes realizados. Los otros enlaces van conmutando con tiempos cercanos a los 50ms para luego ir paulatinamente enviando alarmas de falla en respaldo hasta quedar con perdida de señal. Los cortes que afectaron rutas con protección "*Gold*" y "*Silver*" conmutaron en promedio antes de los 50ms. Las fallas en la fibra, obligan al sistema a recalcular las rutas de protección. Esta función tardo en promedio 500ms. Al volver a conectar las rutas intervenidas, es decir, al reponer el corte, nuevamente el sistema recalcula los caminos de respaldo. Esto tarda en promedio 2s. desde que se produce la

reconexión. La restauración de enlaces vuelve a reponer los servicios de menor importancia en un tiempo de restauración equivalente.

4. RESULTADOS

4.1. MAQUETA 1

Los resultados eran los esperados, sobre todo en las plataformas ya conocidas, como SDH en configuración de anillo MS-PRING. Equipos de distintos proveedores (NEC, ERICSSON y ALCATEL) transfieren tráfico de manera transparente por la maqueta. Sin embargo, la debilidad del sistema se manifiesta en:

-El sistema de protección: Se determina que es MS-PRING y esto implica que todo servicio montado sobre él, contará con el mismo nivel de respaldo. Queda en reserva entonces, el 50% de la capacidad de los enlaces para este fin a pesar de que solo algunos servicios requieren de tal nivel de seguridad.

-Robustez ante cortes: El anillo solo resiste un corte ya que cada nodo solo dispone de dos caminos por donde trasladar su tráfico. Refiriéndonos a la Figura 44, se observa que, a pesar de que existen dos enlaces desde el Nodo B al Nodo D, si hay cortes o fallas en A→B y B→D del mismo anillo, el nodo B, quedará aislado para esa estructura.

-Compleja escalabilidad: Si se cuenta con más tarjetas de línea para aumentar la capacidad del nodo, no es posible incorporarlas sin afectar el tráfico y reconfigurar y reconstruir los esquemas de protección.

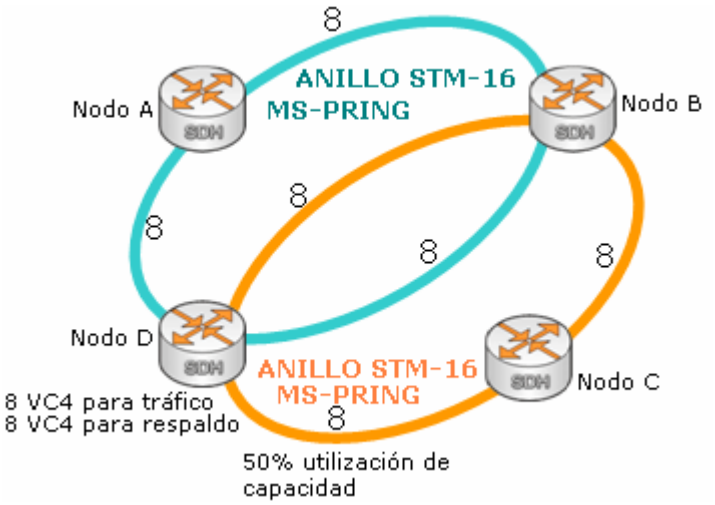


Figura 44.: Utilización de la capacidad en maqueta 1

4.2. MAQUETAS 2 Y 3

En la maqueta 2 y 3, podemos apreciar un drástico mejoramiento del ancho de banda disponible, condicionado eso si, por los tipos de servicios que se configuran. Es así, como ante muchos servicios "*Diamond*", el ancho de banda para respaldo es extraído de la capacidad disponible, no así con las otras categorías de calidad de servicio. En ASON, la configuración de los enlaces es muy simple, Origen, Destino y Calidad de servicio. Esto mejora el tiempo de habilitación y los cambios de prioridades en la red. Si bien en la situación anterior (Maqueta 1), también es posible redefinir los servicios para priorizar uno de otros ante una falla, este trabajo es altamente impactante sobre la red, pues produce indisponibilidades sobre trayectos en funcionamiento, por mucho tiempo y más de una vez (cerca de 30min, 2 o 3 veces). En las maquetas ASON, los cortes se cuadruplicaron (y quintuplicaron para el caso 3) antes de producir caídas de servicios críticos, situación que mejora la disponibilidad fuertemente. En efecto, La situación que produce aislamiento, en este caso, es cuando se originan cinco cortes, y teniendo en cuenta que las fallas de fibra deben ser atendidas, debemos agregar a esto que estos defectos se produzcan en un tiempo menor al necesario para reparar la anomalía. Este escenario es prácticamente imposible que se presente hoy en día. La Figura 45, ilustra lo descrito:

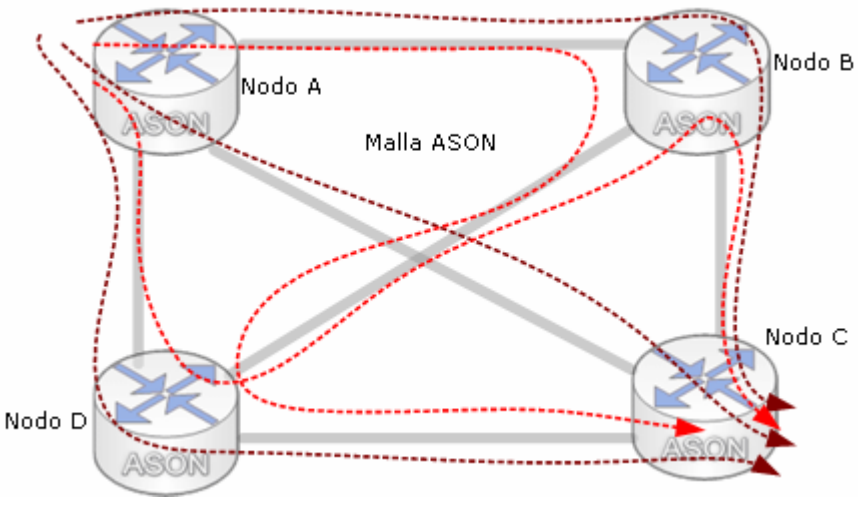


Figura 45.: Rutas disponibles en ASON para tráfico protegido desde Nodo A → Nodo C

Las intervenciones en la red, como inserción o retiro de tarjetas (observado al pasar de la maqueta 2 a la maqueta 3), produce mucho menos impactos ya que no es necesario crear las cross-conexiones en las maquinas. Estas son recalculadas una vez reconocidas.

4.3. COMPARACIÓN ENTRE SDH TRADICIONAL Y ASON

Es necesario hacer un análisis comparativo entre SDH tradicional y ASON, en referencia a la utilización de ancho de banda comercializable, confiabilidad de la red, inversión en repuestos y cuestiones referentes a la operación y mantenimiento. La Tabla 14 contiene el análisis:

Concepto	SDH Tradicional	ASON
Ancho de banda comercializable	Existen varios esquemas de protección implementables, sin embargo los que proveen de seguridad equivalente a ASON, producen una disponibilidad de 50% de ancho de banda comercializable, el otro 50%, es utilizado para el respaldo.	Se puede configurar en la medida que se requiere asegurar. Al contarse con varios niveles de protección, es posible disponer de mayor ancho de banda. Además permite utilizar la capacidad ociosa en enlaces de poca importancia. Fácilmente, se logran mejoras en un 30% de disponibilidad de ancho de banda en comparación con SDH tradicional
Disponibilidad de la red	El sistema soporta cortes solo en un tramo del anillo cuando se trata de protección MS-PRING. En caso de protección SNCP, el caso es similar. Es posible reenrutar el tráfico pero es necesaria la intervención humana, y prácticamente siempre provocará indisponibilidad y afectación de otros enlaces en servicio.	El sistema soporta múltiples cortes, el reenrutado es automático y no provoca indisponibilidad. La ganancia de continuidad en el servicio protegido es extremadamente superior a SDH tradicional
Inversión en repuestos	En algunas tecnologías, estos costos son altos. En equipos SDH Huawei NGN, se pueden utilizar tarjetas tributarias y de línea, en variados modelos.	Por tratarse prácticamente de los mismos equipos SDH Huawei NGN, con incorporaciones ASON, los costos son similares. Las tarjetas tributarias y de línea pueden ser utilizadas en varios modelos.
Inventario y provisión de servicios	La provisión de servicios debe realizarse en el sistema de gestión de manera detallada. Esto requiere de mucho conocimiento de la red y los equipos. Además es un proceso que requiere planificación previa y un lapso de tiempo considerable.	El inventario se realiza de manera automática. Así mismo, la provisión es simple y directa. Además no requiere de conocimientos detallados de la red ya que el sistema realiza las acciones de cross-conexión y selección de ruta.

Concepto	SDH Tradicional	ASON
Mantenimiento	Ante fallas de tarjetas, la intervención es moderada, si se interviene el equipo para realizar acciones correctivas de tráfico, la actividad es compleja y demorosa ya que se debe coordinar con el operador de la Gestión.	Ante falla de tarjetas, la intervención es sencilla, prácticamente *plug and play.* En el caso de acciones correctivas de tráfico, el proceso es similar. Casi no se requiere de intervención en la gestión.
Escalamiento	El escalamiento es muy engorroso. Este requiere nuevamente la intervención en la gestión para el reconocimiento de equipos y enlaces. Además es necesario intervenir en las estructuras existentes para crear la o las nuevas. Se expone a cortes en el tráfico en cada intervención	El escalamiento es directo y sencillo. Los elementos nuevos son reconocidos por la gestión y comunicados por los protocolos ASON a los otros equipos. Además mantiene la compatibilidad con SDH tradicional por medio de sus puertos tributarios multiservicios
Gestión	La gestión es centralizada, y esto requiere de computadoras de gran envergadura. La pérdida de información, bloqueo o pérdida de comunicación del software de gestión con los elementos de red, deja imposibilitado el reenrutamiento y las acciones correctivas en el tráfico. El tipo de gestión es de elementos y el de subred	La gestión es distribuida y reside en los nodos de la red. Esto permite que los equipos reaccionen ante cortes y reenrutamientos de manera autónoma. El tipo de gestión es de red, es decir, End to End.

Tabla 14.: Comparación entre tecnología SDH Tradicional v/s ASON/GMPLS

4.3.1. ESTIMACIÓN DE COSTOS OPERACIONALES

Las nuevas tecnologías como ASON/ASTN e interfaces estandarizadas prometen automatizar la operación y provisión de las redes de transporte. De esta forma mejorarán la utilización de ancho de banda y recursos humanos en el mantenimiento de servicios. En cuanto a las empresas proveedores de servicios de telecomunicaciones, se espera que esta tecnología permita mejoras en términos de gastos en inversión de capital (CAPEX) y gastos operacionales (OPEX). La influencia de ASON en el OPEX, solo puede ser estimada correctamente, teniendo en cuenta los cambios que involucra dicha tecnología en los procesos internos de operación de la red. Teniendo en cuenta lo observado en la etapa de implementación de este trabajo, se pueden hacer las estimaciones necesarias para el análisis.

4.3.2. PROCESOS CONSIDERADOS

La operación de la red, compromete varios procesos y actividades para entregar un servicio a cliente. Esto incluye a áreas comerciales, de ingeniería, de provisión, de explotación y mantenimiento. Los procesos técnicamente más relevantes son: oferta de servicios; activaciones; pruebas y entrega de soluciones; mantenimiento, reparación y bajas de prestaciones; y, supervisión y control.

El proceso tradicional con SDH contempla desde la solicitud de contrato del cliente, pasando por el estudio, la creación de proyecto, provisión, instalación, habilitación, pruebas de servicio, registro tanto de datos técnicos como administrativos para el mantenimiento y la facturación de la solución al cliente. La Figura 46 muestra este proceso:

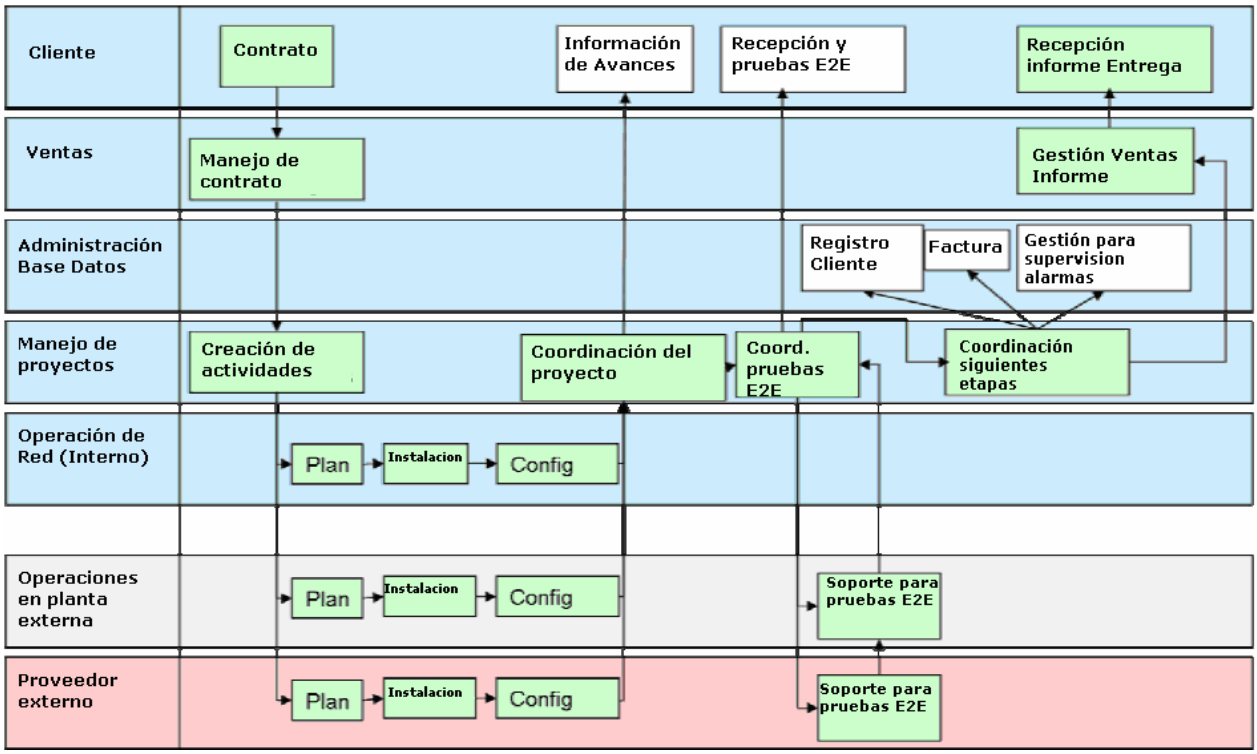


Figura 46.: Proceso de activación para un servicio E2E con SDH tradicional

En el escenario de ASON, la intervención manual está confinada a dar soluciones especiales en las que no se cuenta con recursos. Ahora el cliente puede contar con una medio que le permita acceder al plano de control de ASON y configurar el servicio que

requiere. No es necesaria la intervención manual para verificar si existen los recursos, ni tampoco se requiere de pruebas de verificación. Eso ya está contemplado por los planos de ASON. Además, ante fallas, estas se auto restauran y las modificaciones y bajas podrán ser realizadas por el cliente de la misma forma en como solicitó servicios. La Figura 47 muestra este proceso:

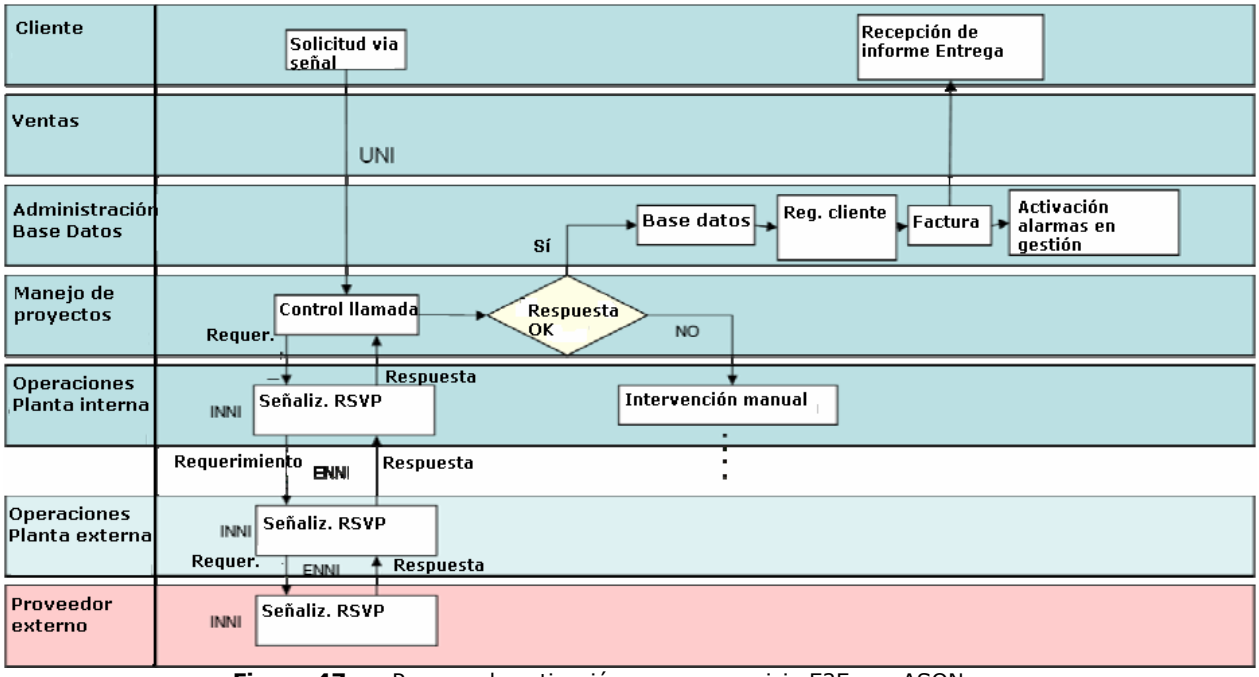


Figura 47.: Proceso de activación para un servicio E2E con ASON

Este proceso automatizado, asume que en toda la cadena de comunicación de equipos, existen las interfaces adecuadas y compatibles. De no ser así, se requiere intervención humana donde es necesario.

Al normalizar los costos por salarios y duración de la actividad, es posible estimar la reducción en OPEX del cambio tecnológico. Esto se muestra en las Tablas 15 y 16:

Área	Personal	Salario	Actividades	Duración	Costo
Ventas	Ejecutivo de Ventas	1	Venta, contratos, administración	1	1
Administración	Administrativo	0,8	Registro de clientes, facturación	0,25	0,2
Manejo Proyectos	Ingeniero de Proyectos	1	Creación de etapas del proyecto	2,5	2,5
Operaciones	Ingeniero Especialista	1	Coordinación ejecución y entrega proyecto	0,12	0,12
	Técnico en Terreno	0,8	Configuración e instalación equipos	0,37	0,296
	Técnico Operador	0,8	Configuración de gestión, conexión física y lógica, realización de pruebas	0,12	0,096
Costo Normalizado por Servicio para SDH tradicional					**4,212**

Tabla 15.: Estimación de costos normalizados con SDH tradicional

Área	Personal	Salario	Actividades	Duración	Costo
Ventas	Ejecutivo de Ventas	1	Venta, contratos, administración, solo contacto	0,1	0,1
Administración	Administrativo	0,8	Registro de clientes, facturación, actualización de base de datos	1	0,8
Manejo Proyectos	Ingeniero de Proyectos	1	Creación de etapas del proyecto	0	0
Operaciones	Ingeniero Especialista	1	Coordinación ejecución y entrega proyecto	0,12	0,12
	Técnico en Terreno	0,8	Configuración e instalación equipos	0	0
	Técnico Operador	0,8	Configuración de gestión, conexión física y lógica, realización de pruebas	0	0
Costo Normalizado por Servicio para ASON					**1,02**

Tabla 16.: Estimación de costos normalizados con ASON

Este análisis, a partir de los resultados y experiencias Europeas [26] da una referencia de los efectos favorables sobre el OPEX para la empresa al utilizar las nuevas tendencias en la red de transporte.

4.3.3. COMPARACIÓN DE LA INVERSIÓN CON SDH TRADICIONAL V/S ASON

En referencia a los costos normalizados en los que se debe incurrir para hacer frente a la demanda de mediano plazo, se revisa el siguiente cuadro comparativo, en base a datos de costos de inversión realizados con anterioridad por la empresa. Además se considera un factor de mejora en la utilización del ancho de banda de ASON sobre SDH, solo de un 20%. *(Normalmente la ganancia de ancho de banda esta entre 25% y 30%)*

La Tabla 17 Contiene la normalización de costos de inversión:

Concepto	SDH Tradicional			ASON		
	Valor Equipo	Nro. Elementos	Costo SDH	Valor Equipo	Nro. Elementos	Costo ASON
Equipamiento para el núcleo de la red	1	4,8	4.8	1,5	4	6
Infraestructura (Espacio, Energía, climatización, planta externa)	0,15	4.8	0,72	0,15	4	0,6
Costo Normalizado	SDH Tradicional		**5,52**	ASON		**6,6**

Tabla 17.: Cuadro comparativo de costos de inversión SDH v/s ASON

Se desprende entonces, que la inversión al optar por ASON en vez de SDH tradicional es un 20% más costosa.

5. CONCLUSIONES

5.1. UTILIZACIÓN DE RECURSOS

Las evidentes ventajas de la utilización de ASON en la red se ven fortalecidas con la flexibilidad de la tecnología para evolucionar las grandes y estables redes SDH, hacia esta red inteligente e integrada de transporte. Los servicios son soportados de manera transparente y con las mismas fortalezas de SDH. El plano de control es descentralizado lo que mejora la protección de la red. Al mismo tiempo, el protocolo GMPLS permite un uso eficiente e inteligente de los recursos de red, mejorando la disponibilidad de ancho de banda, al permitir utilizar las reservas para respaldo por servicios prescindibles. Las mayores ventajas se pueden apreciar a la hora de asegurar los servicios de alta prioridad, la ganancia de disponibilidad son muchas veces mejores que en las redes tradicionales. Estas afirmaciones se hacen evidentes al observar el comportamiento de las maquetas: La maqueta 1 con SDH tradicional, limitó el tráfico disponible a la mitad, y no fue capaz de soportar múltiples cortes en un mismo anillo. En contraposición, las maquetas 2 y 3, demostraron que permiten priorizar un servicio sobre otros y mantener el enlace a pesar de sufrir múltiples fallas.

5.2. CONFIGURACIÓN DE SERVICIOS

En SDH tradicional, la función de poner en operación los enlaces pasa por dos actividades altamente complejas y laboriosas: la selección del esquema de protección, el cual debe considerar muchas variables (niveles de tráfico, servicios soportados, importancia de enlaces, etc.) y esperar que estas, sean lo más estáticas posibles para mantener validez; y, la configuración de enlaces, lo que implica la habilitación de los recursos. En cambio, ASON integra estas tareas en un solo proceso: la configuración del servicio, el que debe especificar ancho de banda, nodo de origen, nodo destino y nivel de protección. Los demás aspectos

son cubiertos por el protocolo de la capa de control (GMPLS) y pueden variar y reconfigurarse con la misma facilidad con la que fueron creados. Las actividades de operación para la creación y mantención de enlaces es drásticamente mas baja que en SDH tradicional.

5.3. PROVISIÓN AUTOMÁTICA

Teniendo en cuenta que actualmente ya se está trabajando para realizar la provisión automática de prestaciones IP para clientes, la tecnología ASON podrá dar el soporte que se requiere en la red de Transporte. Este punto es de suma importancia tomando en cuenta el drástico y acelerado crecimiento de los servicios para clientes finales. Los impredecibles comportamientos del tráfico a los que se verán enfrentadas las plataformas de transmisión urbana y de larga distancia, requieren de una red inteligente y segura como ASON. En este nuevo escenario, la robusta red SDH tradicional no es aplicable. Si bien sus esquemas de protección le permiten dar grados de estabilidad y seguridad, estos no son lo suficientemente flexibles para permitir una escalabilidad rápida. Además, la configuración es en extremo lenta en comparación con ASON, lo que no permitirá manejar el volumen de solicitudes de enlaces sobre ella.

5.4. CLASIFICACIÓN DE TRÁFICO

En la actualidad, prácticamente todo el tráfico existente en las redes SDH está protegido, ya sea por conexiones en anillos o en buses con protección 1:n o 1:1. Por lo que se recomienda considerar en la migración desde SDH a ASON, una etapa de clasificación de Tráficos. En efecto, los cambios en los paradigmas y filosofías de ASON v/s SDH, deben ser aplicados también desde el principio en los niveles de seguridad que se provean a Clientes y enlaces críticos. El pasar de estructuras en donde todo el tráfico está protegido (por ejemplo en anillos SDH con MS-PRING) a una nueva red enmallada, en la que existen niveles de protección variados, puede terminar en prácticas poco eficientes y simplistas, como por

ejemplo, dar el nivel de servicio máximo a la mayor parte de los enlaces ("*Diamond*"). En este sentido, la recomendación es:

-Dar nivel de protección "*Diamond*" solo a enlaces estratégicamente críticos para el funcionamiento de la empresa. En esta categoría se cuenta los servicios intermedios (entre proveedores) como Tráfico Internet hacia los ISP, comunicación de DSLAMS con equipos agregadotes y autentificadotes y algunos servicios de clientes altamente estratégicos.

-Dar nivel de protección "*Gold*" a enlaces estratégicos de grandes clientes (corporativos, gobierno, fuerzas armadas). También clasifican los enlaces que dan soporte a servicios masivos de telefonía, televisión e Internet y todo servicio que produzca un gran impacto comercial por indisponibilidad extensa

-Dar nivel "*Silver*" a servicios de datos de clientes u otros de importancia que cuenten con mecanismos de recuperación de paquetes en los extremos del enlace (por ejemplo: basados en TCP/IP)

-Dar nivel "*Cooper*" a prestaciones de baja prioridad, en la que una indisponibilidad de servicio, tenga bajo efecto. En esta categoría podrían estar los enlaces de respaldo de SDH tradicionales y links redundantes de equipos de datos.

-Dar nivel "*Iron*" a enlaces de uso temporal, de baja prioridad y que permita fallas sin impacto importante.

5.5. INVERSIONES Y COSTOS DE MEDIANO PLAZO

En lo que se refiere a la operación de la red ASON, la simplificación es evidente y se estima que la liberación de recursos de las tareas de planificación, provisión, habilitación y mantención de la red, es de un 80%. Esto permite contar con recursos técnicos para actividades más relevantes (mejoramiento en la atención al cliente, planificación y ejecución de obras de expansión en la cobertura geográfica, mejoras en la calidad de servicio entre otras).

Por otra parte, las inversiones en CAPEX que son necesarias para cubrir la demanda en el mediano plazo (2 años), son equivalentes entre la tecnología SDH tradicional y la emergente G.ASON (ASON = 20% más costoso), comparando situaciones de capacidad y seguridad similares. La decisión entonces es determinada por las comparaciones estimativas en el OPEX de una solución u otra. En ese sentido, y sin más consideraciones técnicas, es rentable y económico, implementar ASON.

Existe también otros punto a favor de ASON: Las nuevas funcionalidades que permite el plano de gestión de red, en cuanto a las mejoras en tiempos de respuesta, funcionalidades comercializables y otras más, las que no han sido ponderadas económicamente y que sin duda, son de un alto valor agregado.

El primer trimestre del año 2007 puede ser un buen momento para comenzar a proyectar el nuevo núcleo de red de transporte digital, ya que existe una adecuada maduración de la tecnología. Con experiencias exitosas y operativas en otras partes del mundo.

5.6. EVOLUCIÓN DE LA RED

La conclusión a la que se llega respecto de la evolución de las redes de transporte para la integración de los servicios, y en lo que respecta a las redes SDH es: El empleo de la transmisión óptica en el núcleo de la red, llevando los elementos tradicionales de transmisión y agregación de tráfico hacia la frontera entre el núcleo y el acceso del cliente. La estructura resultante es conceptualmente mucho más simple, lo que redunda en una gestión más rápida, sencilla y económica. La evolución hacia esta realidad, ha sido lenta pero persistente, y comienza a tomar fuerza en América Latina (comenzando por Brasil).

5.7. TENDENCIAS FUTURAS

5.7.1. ARQUITECTURA DE RED

La tendencia en la arquitectura de red, está marcada por el incremento en la capacidad de transporte que debe hacer frente a la demanda creciente de servicios de clientes. Las aplicaciones multimediales y de comunicaciones tales como Televisión sobre IP, Telefonía sobre IP, Servicios en Internet (BitTorrent, Skype, Juegos en línea), etc., se vuelven rápidamente masivos y contribuyen considerablemente en el aumento de la demanda de ancho de banda. La tendencia muestra una sostenida migración de las aplicaciones hacia IP. Este punto, presiona para la evolución de la arquitectura de red hacia "IP sobre óptico". El núcleo de la red estará basada en la recomendación ASON y DWDM y SDH, esta ultima se justifica por la eficiencia y grado de estandarización que ha alcanzado. Proveerá enlaces multiservicios. La red de acceso irá evolucionando a mayores prestaciones de tráfico para culminar en interfaces ópticas en las dependencias del cliente.

5.7.2. SUPERVISIÓN Y CONTROL

Los proveedores de equipos están apostando por ASON/GMPLS para las redes de telecomunicaciones. Se espera cubrir funcionalidades de red muy complejas, a partir de los elementos de supervisión y control. La tendencia será a proveer características de optimización y máxima automatización de los recursos: Reorganización automática de circuitos que permita el uso óptimo de los recursos disponibles; Inventario Automático para auto detección de nodos; Provisionamiento automático de circuitos, con tal de permitir la auto configuración de servicios por parte del cliente; Optimización temporal de la utilización de ancho de banda, en donde la utilización de recursos de auto ajustará en base a las estadísticas de tráfico; Y, la existencia de gestores de red multiproveedor, en donde la gestión tenga los grados de estandarización necesarios para permitir sistemas independientes del proveedor.

6. GLOSARIO DE ACRÓNIMOS

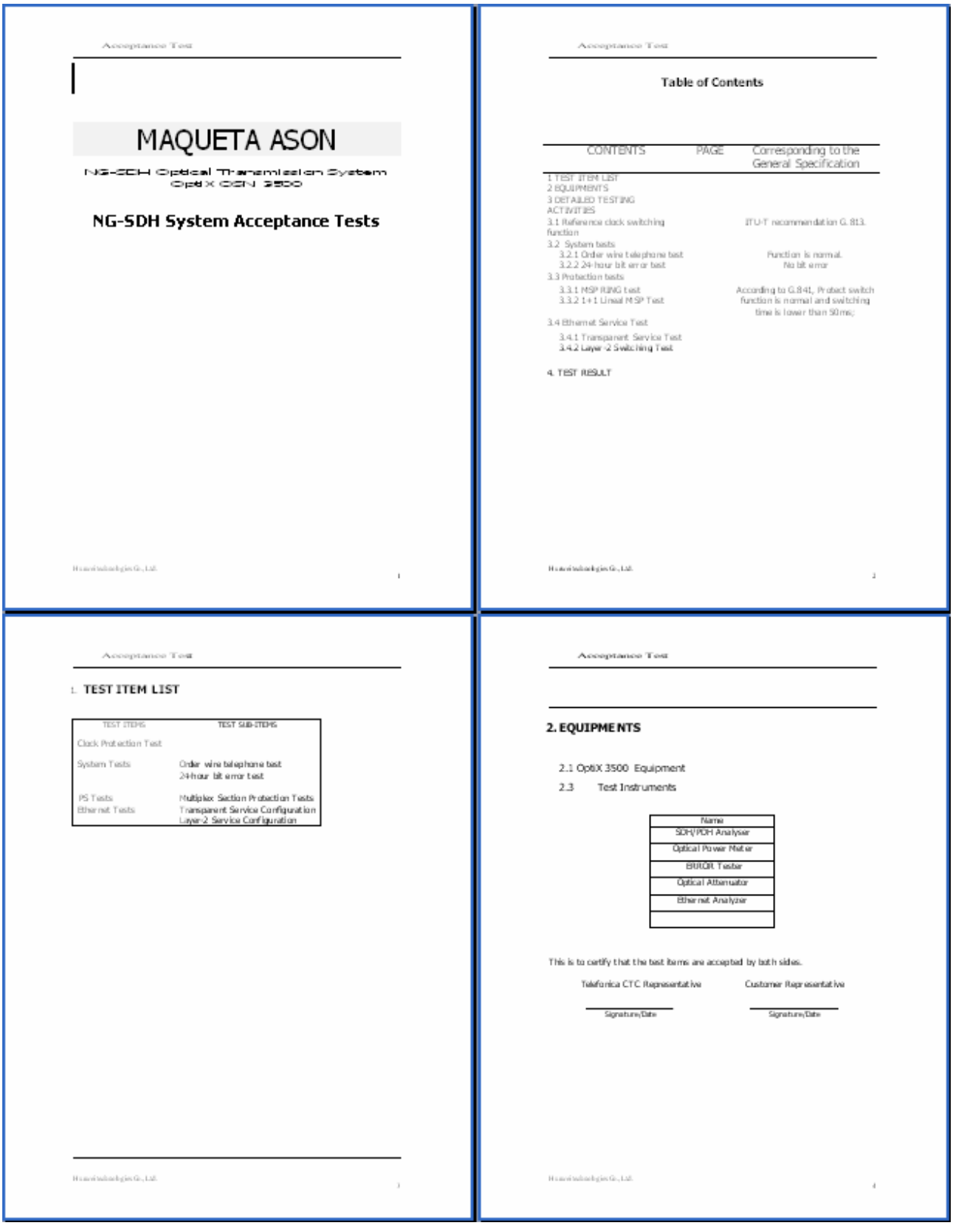
AAL	ATM Adaptation Layer
ACAC	Actual Call Admission Control
ADM	Add and Drop Multiplexing
AFI	Authority and Format Identifier
APRoPs	ATM PNNI Routing protocol Simulator
ASON	Automatic Switched Optical Networrk
ASTN	Atomatic Switched Transport Network
ATM	Asynchronous Transfer Mode
ATMF	ATM Forum
BBOR	BYPASS Based Opticañ Routing
BOX	Border OXC
BR	Border Router
Bw	Bandwidth
CAC	Call Admission Control
CC	Connection Controller
CCI	Connection Controller Interface
CoS	Class or Service
CR	Constraint-based Routing
CSPF	Constreaint Shortest Path First
CUG	Closed User Group
DSP	Domain Specific Part
DWDM	Dense WDM
DXC	Digital Coss-Connect
E-NNI	External Network-to-Network Interface
ERO	Explicit Routing Object
ESI	End System Identifier
GCAC	Generic Connection Admission Control
GIT	generic Identifier Element
GMPLS	Generalised Multi-protocol Label Switching
GoS	Grade of Service
IDI	Initial Domain Identifier
I-NNI	Internal Network-to-Network Interface
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4
Ipv6	Internet Protocol version 6
ISO	International Organization for Standarization
ITU-T	Internactional Telecommunication Union-Telecommunication Sector
IWU	Internetworking Signalling Unit
LC-ATM	Label-switched Controlled ATM
LDP	label Distribution Protocol
LRMA	Link Resource Manager-A
LRMZ	Link Resource Manager-Z
LSN	Logical Subnetwork Node
LSP	Label Switched Path
LSR	Label Switched Routers
LSRv	Virtual LSR

MPLS	Multiprotocol Label Switching
ND	Network Domain
NMS	Network Management System
NRBw	No Requested Bw
NSAP	NetworkService Access Point
OAM	Organization, Administration and Maintenance
OADM	Optical ADM
Och	Optical channel
ODXC	Optical DXC
OIF	Optical Internetworking Forum
OTN	Optical Transport Network
OXC	Optical Cross-Connet
PAR	PNNI Augmented Routing
PC	Protocol Controller
PDH	Plesiochronous Digital Hierarchy
PG	Peer group
PGL	Peer Group Leader
PNNI	Private Network-Network Interface
POAR	PNNI Optical Augmented Routing
POTSE	PNNI Opctical Topology State Element
POTSP	PNNI Optical Topology State Packet
PPAR	Proxy PAR
PPP	Point-toPoint Protocol
PTSE	PNNI Topology State Element
PTSP	PNNI Topology State Packet
PVC	Permanent Virtual Circuit
PVCC	Permanent Virtual Circuit Connection
PVPC	Permanent Virtual Path Connection
QoS	Quality of Service
RAIG	Resource Available Information Group
RBw	Requested Bw
RC	Routing Controller
RSVP	Resource Reservation Protocol
SDH	Synchronous Digital hierarchy
SID	Subnetwork Identifier
SL	Subnetwork Leader
SNC	Subnetwork Connection
SNP	Subnetwork Path
SNPP	Subnetwork Termination Point Pool
SPF	Shortest Path First
SPVC	Soft-Permanent Virtual Connection
SSCOP	Service-Specific Connection-Oriented Protocol
STM	Synchronous Transfer Mode
SVC	Switched Virtual Circuit
TDM	Time-Division Multiplexing
TE	Traffic Engineering
TED	Traffic Engineering Database
TLV	Type Length Value
TP	Traffic Policing
UNI	User Network Interface
VC	Virtual Circuit
VCI	Virtual Circuit Identifier
VCID	Virtual Connection Identifier

VPC	Virtual Path Connection
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WSP	Widest-Shortest Path
WDM	Wavelength Division Multiplexing

7. APÉNDICES

7.1. APÉNDICE A: FORMULARIO DE PRUEBAS DE SISTEMA



Acceptance Test

MAQUETA ASON

NG-SDH Optical Transmission System
OptiX OSN 3500

NG-SDH System Acceptance Tests

Huawei Industrial Co., Ltd.

1

Acceptance Test

Table of Contents

Huawei Industrial Co., Ltd.

2

Acceptance Test

1. TEST ITEM LIST

TEST ITEMS	TEST SUB-ITEMS
Clock Protection Test	
System Tests	Order wire telephone test 24-hour bit error test
PS Tests	Multiplex Section Protection Tests
Ethernet Tests	Transparent Service Configuration Layer-2 Service Configuration

Huawei Industrial Co., Ltd.

3

Acceptance Test

2. EQUIPMENTS

2.1 OptiX 3500 Equipment

2.3 Test Instruments

Name
SDH/PDH Analyser
Optical Power Meter
BER/BIR Tester
Optical Attenuator
Ethernet Analyzer

This is to certify that the test items are accepted by both sides.

Telefonica CTC Representative

Signature/Date

Customer Representative

Signature/Date

Huawei Industrial Co., Ltd.

4

3. DETAILED TESTING ACTIVITIES

3.1 REFERENCE CLOCK SOURCE SWITCHING AT SYNCHRONIZATION INTERFACE

No.	3.2	Item name	Reference clock source switching at synchronization interface

Item description:
To ensure that when some of clock source fails, the system clock can switch to another source clock of higher priority.

Test equipment:
1. SDH analyzer.

Test set-up:

Test procedures:

1. Establish the test connection as illustrated in figure;
2. Configure SEC from external clock to STM-N clock , tributary clock, internal SEC according to clock priority level ;
3. Disconnect external clock source artificially and observe whether clock source has switched from external clock to STM-N clock through NMS, and there should be no bit errors.
4. Disconnect STM-N optical signal, and observe whether clock source has switched from STM-N to tributary clock through NMS, and there should be no bit errors.
5. Disconnect tributary interface, and observe whether clock source has switched from tributary clock to keep mode, and there should be no bit errors.
6. Configure SEC from STM-N clock to tributary clock, internal SEC according to clock priority level only; And configure SEC from tributary clock to STM-N clock according to clock SSM level ;

7. Observe whether clock source has locked to tributary clock; Disconnect tributary interface, and observe whether clock source has switched from tributary clock to STM-N clock, and there should be no bit errors.

Test standard:
The clock source should switch properly, and service shouldn't be affected.

Remarks:

Test result:

NE Name	Pass/Not pass	Remarks

Test performed by :

Date :

Location :

3.2 SYSTEM TESTS

3.2.1 Order wire telephone test

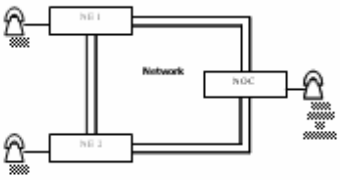
No.	3.3.1	Item name	Order wire telephone test

Item description:

To ensure that the order wire telephone function is normal, speech is clear and conference call service functions are normal.

Test equipment:
1. Order Wire Telephones

Test set-up:



Test procedures:

1. Establish the test connection as illustrated in the above figure;
2. Through the computer, use network management software to distribute configurations to set the network element to two fibers uni-directional path protection ring. Configure one order wire telephone for each station, and use OptiX iManager to configure different telephone numbers and conference call service telephone that's commonly accessible.
3. Dial the telephone numbers of other stations from any of the stations.

4. Dial the conference call service from any of the three sites.

Test standard:
Order wire phone service is normal.

Remarks:

Test result:

NE Name	Pass/Not pass	Remarks

Test performed by :

Date :

Location :

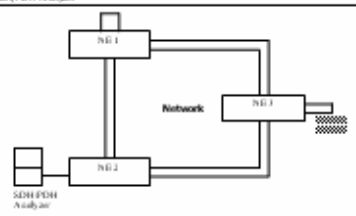
3.2.2 24-hour bit error test

No.	3.2	Item name	24 Hours Bit Error test

Item description:

Process 24 hours bit error test to find out the system holistic function.

Test equipment:
1. SDH/PDH Analyzer



Test procedures:

1. Establish the test connection as illustrated in the above figure;
2. Configure a E1/E4/STM-1 traffic pass through all the NEs selected for the test.
3. Make equipment running for 24 hours
4. Observe the bit error count and record it.

Pass standard:
No bit error.

Test results:

Bit error count	Pass/Not Pass	Remarks
STM-4 1+1 Linear MSP		

Test performed by :

Date :

Location :

3.3 PROTECTION SWITCHING TESTS

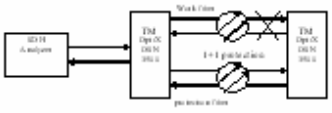
3.1 MSP 1+1 in the STM-4 line

No.		Item name	1+1 linear Multiplex section protection switch function

Item description:
To ensure that the 1+1 linear Multiplex section protection switching function and switching time of the OptiX equipment is in accordance with ITU-T recommendation clause 7.4.1/7.4.2/G.841 (10/1998)

Test equipment:
1. SDH analyzer;
2. Optical attenuator;

Test set-up:



Test procedures:
1. Establish the test connection as illustrated in the above figure;
2. Configure a VC-4 bidirectional connection
3. Check the protection state whether it is normal by the NMS;
4. Disconnect the work fiber and use the analyzer to see if the service switched to protection fiber in less than 50ms. Then connect fiber again and see if the service switches back to work fiber in less than 50ms.

Pass standard:
Refer to ITU-T recommendation clause 7.4.1/7.4.2/G.841.
Definition:
Linear Trail protection generically protects against failures in the server layer, and failures and degradations in the client layer. The protection scheme can be either 1 + 1, where the dedicated protection trail is only used for protection purposes, or 1:1 where the dedicated protection trail can be used to support extra traffic. Bidirectional protection switching and 1:1 protection switching require an APS protocol to coordinate between the local and remote switch and bridge operations.

Switch time: The APS algorithm for LO/HO VC trail protection shall operate as fast as possible. A value of 50 ms has been proposed as a target time. Concerns have been expressed over this proposed target time when many VCs are involved. This is for further study. Protection switch completion time excludes the detection time necessary to initiate the protection switch, and the hold-off time.

Remarks:

Test result:

Link	Switch time	Restore time	Pass/Not pass	Remark

Test performed by :

Date :

Location :

3.4 ETHERNET SERVICE TESTS

3.4.1 Transparent Ethernet Service Configuration

No.		Item name	Transparent Ethernet Service Configuration

Item description:

Test equipment:
1. Ethernet Analyzer

Test set-up:

Test procedures:
1. Create a VC-Trunk between two NEs using VC3 or VC12.
2. Configure a transparent Ethernet service between two NEs using NMS.
3. Testing RFC 2544
4. Use Ethernet analyzer to confirm throughput 100Mbps

Pass standard:
OSN1500 / OSN 3500 Ethernet board can be used, depending on its configuration, to transparent transmit any type of Ethernet frame regardless of its protocol.

Remarks:

Test result:

Ethernet Protocol	Result	Remark

Test performed by :

Date :

Location :

Acceptance Test

3.4.2 Ethernet Layer 2 Switching Service Configuration

No.		Item name	Ethernet Layer-2 Switching Service Configuration
Item description:			
Test equipment: 1. Ethernet Analyzer or Ethernet Switch			
Test set-up: 			
Test procedures: 1. Create a VC-Trunk between two or more NE's VC12 2. Configure an Ethernet service between two NE's using NMS 3. Test with different type of configurations (VLANID, LCAS) 4. Use Ethernet Analyzer to confirm whether OSN equipment can transport different types of services.			
Pass standard: OSN3500 Ethernet board can be used, depending on its configuration, to transmit different types of Ethernet services.			
Remarks:			

Test result:

Ethernet Service	Result	Remark

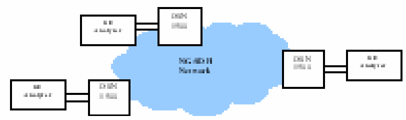
Test performed by :

Date :

Location :

Acceptance Test

3.4.3 Pruebas de Funcionalidad entre Redes WAN

No.		Item name	Pruebas de Funcionalidad entre Redes WAN
Item description:			
Test equipment: 1. Ethernet Analyzer			
Test set-up: 			
1.- Aplicando una trama IP de largo Fijo constante, a través de una VLAN definida en el momento, se procederá a realizar las siguientes pruebas de Conmutaciones: • Respaldos ópticos: desconectar jumper ópticos para bajar ruta regular y que funcione ruta de respaldo. • Respaldo de Tarjetas: Retirar tarjeta Controladora/Crossconnect regular para que funcione respaldo. Retirar tarjeta de alimentación regular para que funcione respaldo. • Funcionalidad LCAS. Bajar o subir un VC-4 del mapeo de cada Ethernet.			
Verificar que en ninguno de los casos anteriores se produce perdida significativa de paquetes			
Remarks:			

Test result:

Ethernet Service	Result	Remark

Test performed by :

Date :

Location :

Acceptance Test

4.- TEST RESULT

TEST ITEMS	TEST SUB-ITEMS	RESULT
Clock Protection Test		PASS FAIL
		PASS FAIL
System Tests	Order wire telephone test 24-hour bit error test	PASS FAIL
PS Tests	Multiplex Section Protection Tests	PASS FAIL
FE Tests	Transparent Service Configuration	PASS FAIL
	Layer-2 Service Configuration	PASS FAIL

Test performed by :

Signature :

Location :

Date :

Telefonica CTC Representative

Signature / Date : ____________________

Huawei Representative

Signature / Date : ____________________

7.2. APÉNDICE B: FORMULARIOS DE PRUEBAS DE EQUIPOS

Telefonica CTC

Protocolo de Aceptación
Equipos OSN 3500
MAQUETA ASON

Huawei (Chile) S.A.

Septiembre 2006

Contenido

1. INFORMACION GENERAL

1.1 Listado de Pruebas

Item	Sub-Item
Inspección Visual	
Inventario de Tarjetas Instaladas	
Pruebas Técnicas	
Pruebas de Interfaces	Potencias Ópticas Transmitida en Interfaces SDH
	Sensibilidad Óptica en la Recepción en Interfaces SDH
	Saturación Óptica en la Recepción en Interfaces SDH
	Tolerancia al Jitter en Interfaces SDH
	Desviación de Frecuencias en Interfaces SDH
	Potencias Ópticas Transmitida en Interfaces GE
	Sensibilidad Óptica en la Recepción en Interfaces GE
	Saturación Óptica en la Recepción en Interfaces GE
Pruebas de Cables	Conectividad entre el ODF y las Interfaces Ópticas
	Conectividad entre el IDF y las Interfaces Eléctricas
Conmutación de Tarjetas	Conmutación de Tarjeta EXCS
	Conmutación de Tarjeta SCC
	Conmutación de Puerto de Alimentación
Verificación de Estado de Tarjetas	
Prototipo Entrada y Salida	
Pruebas de Sistema	Conectividad NMS

1.2 Instrumentos de Prueba

Nombre	Modelo	Fabricante
Analizador SDH		
Atenuador Óptico Variable		
Medidor de Potencia Óptica		
Analizador Gigabit Ethernet		

2. Inspección Visual

Serial No.	Items	Estado	Comentarios
1	Inventario de Racks		
2	Inventario de Cables Opticos y Eléctricos		
3	Inventario de Cables de Energía		

3. Inventario de Tarjetas Instaladas

Nombre del Sitio : _____
Tipo de Equipo : OSN 3500
Nombre del Elemento de Red : _____

Slot	Versión de Hardware	Número de Serie	Versión de Software	Descripción

Fecha :
Firma :

4. Pruebas Técnicas

4.1 Pruebas de Interfaces

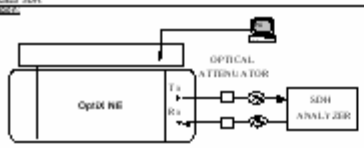
4.1.1 Potencias Máximas de Salida, Sensibilidad y Saturación de las Interfaces SDH

No.	4.1.1	Item	Potencias Máximas de Salida, Sensibilidad y Saturación de las Interfaces SDH

Descripción:
Verificar que la Potencia Máxima de Salida, Sensibilidad y Saturación de las interfaces ópticas SDH cumplan con lo recomendado en ITU-T G.2.3 y Telcordia GR-253-CORE (08/1994).

Instrumentos y Herramientas:
1. Medidor de Potencia Óptica.
2. Atenuador Óptico Variable.
3. Analizador SDH.

Procedimiento:



Observaciones:
1) Establecer una conexión como se muestra en la figura.
2) Medir la potencia óptica antes del atenuador.
3) Ajustar la potencia hasta que la tasa de error empiece a aumentar y anotar la potencia en la escala.
4) Aumentar la potencia hasta que la tasa de error empiece a aumentar y anotar la potencia en la escala.

Slot	Tarjeta	Puerto	Potencia (dBm)	Sensibilidad (dBm)	Saturación (dBm)

Fecha :
Firma :

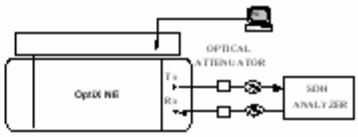
4.1.2 Tolerancia al Jitter en las Interfaces SDH

No.	4.1.2	Item	Tolerancia al Jitter en las Interfaces SDH

Descripción:
Asegurar que la conexión al jitter cumple con lo recomendado en UIT-T.

Instrumentos y Herramientas:
1. Analizador SDH.

Procedimiento:



Observaciones:
1) Establecer una conexión como se muestra en la figura.
2) Medir la tolerancia al jitter en las interfaces ópticas.
3) Anotar los resultados.

Slot	Tarjeta	Puerto	Resultado

Fecha :
Firma :

4.1.3 Desviación de Frecuencias en las Interfaces SDH

No.	4.1.3	Item	Desviación de Frecuencias en las Interfaces SDH

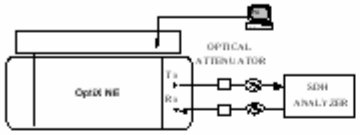
Objetivo:

Asegurarque la desviación de frecuencia cumpla con lo especificado en la UIT-T clausula 6.1.1 y tabla 2/G.8251 (2001/11).

Instrumentos requeridos:

1. Analizador SDH.

Configuración:



Procedimiento:

1) Establezca una conexión como se muestra en la figura.
2) Verifique el buen funcionamiento del SDH hasta que el sistema empiece a recibir.
3) Anote los resultados.

Slot	Tarjeta	Puerto	Resultado

Fecha :
Firma :

4.1.4 Potencias Máximas de Salida, Sensibilidad y Saturación de las Interfaces GE

No.	4.1.4	Item	Potencias Máximas de Salida, Sensibilidad y Saturación de las Interfaces GE

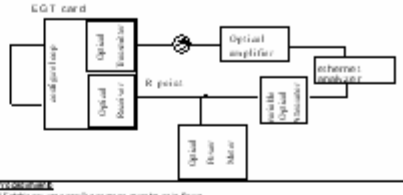
Objetivo:

Verificar que la Potencia Máxima de Salida, Sensibilidad y Saturación de las interfaces en SDH cumplan con lo especificado en la tarjeta.

Instrumentos requeridos:

1. Medidor de Potencia Óptica.
2. Atenuador Óptico Variable.
3. Analizador GE.

Configuración:



Procedimiento:

1) Establezca una conexión como se muestra en la figura.
2) Mida la potencia óptica antes del atenuador.
3) Aumente la potencia hasta que el tráfico no sea estable y medir la potencia en la escala.
4) Amplifique la potencia hasta que el tráfico sea estable y medir la potencia en la escala.

Slot	Tarjeta	Puerto	Potencia (dBm)	Sensibilidad (dBm)	Saturación (dBm)

Fecha :
Firma :

4.2 Pruebas de Cables

4.2.1 Conectividad entre el ODF y las Interfaces Ópticas

No.	4.2.1	Item	Conectividad entre el ODF y las Interfaces Ópticas

Objetivo:

Asegurarque todas las fibras ópticas se encuentren correctamente conectadas en el ODF.

Instrumentos requeridos:

Medidor de Potencia Óptica.

Procedimiento:

1. Verificar que exista conectividad entre todos los puertos del ODF y cada una de las tarjetas.

Slot	Tarjeta	Puerto	Resultado

Fecha :
Firma :

4.3 Conmutación de Tarjetas

4.3.1 Conmutación de Tarjetas EXCS, SCC y PIU

No.	4.3.1	Item	Conmutación de Tarjetas EXCS, SCC y PIU

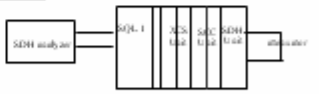
Objetivo:

Asegurarque las tarjetas con protección 1+1 conmuten correctamente.

Instrumentos requeridos:

1. Analizador SDH.

Configuración:



Procedimiento:

1. Configurar una conexión como se muestra en la figura.
2. Retirar la tarjeta EXCS activa. Verificar que conmute, reportar cambios ocurridos y retirar tarjeta stand-by.
3. Retirar la tarjeta SCC activa. Verificar conmutación, reportar cambios ocurridos y retirar tarjeta stand-by.
4. Desconectar una fuente de alimentación. Conectarla nuevamente y desconectar la otra fuente de alimentación.
5. Anotar los resultados

No.	Tarjeta	Resultado
	EXCS	
	SCC	
	Fuente de Alimentación	

Fecha :
Firma :

4.4 Verificación de Estado de Tarjetas

No.	4.4	Item	Verificación de Estado de Tarjetas

Descripción:

Asegurar que todas las tarjetas se encuentren activadas correctamente y se desplieguen sin errores.

Instrumentos de Prueba:

1.- OptiX iManager T2000

Configuración:

Procedimiento:

1. Ver estado de las tarjetas.
2. Configurar un Elemento de Red utilizando el iManager T2000.
3. Verificar el correcto funcionamiento de las tarjetas.

Slot#	Tarjeta	Resultado

Fecha :
Firma :

4.5 Reloj de Entrada y Salida

No.	4.5	Item	Reloj de Entrada y Salida

Descripción:

Verificar el correcto funcionamiento de las interfaces de entrada y salida de reloj.

Instrumentos de Prueba:

1. OptiX iManager T2000
2. Generador de Reloj
3. Medidor de Frecuencia

Configuración:

Procedimiento:

1. Configurar el reloj de 2MHz.
2. Conectar medidor de frecuencia en salida de reloj y verificar.
3. Conectar generador de reloj a la entrada de reloj y configurar que lo reconozca.
4. Configurar el reloj de 2Mbps.
5. Conectar señal de PDH a la salida de reloj y verificar.
6. Conectar señal de PDH a la entrada de reloj y verificar que lo reconozca.

No.	Resultado

Fecha :
Firma :

4.6 Prueba NMS Funciones de Conectividad y Alarmística

No.	4.6	Item	Prueba NMS Funciones de Conectividad y Alarmística

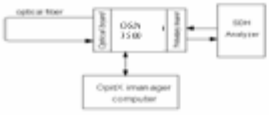
Descripción:

Asegurar que el elemento de red puede ser supervisado y configurado a través del sistema de gestión T2000.

Instrumentos de Prueba:

1. Analizador SDH
2. OptiX T2000 Imanager.

Configuración:



Procedimiento:

1. Establecer una configuración como se muestra en la figura.
2. Crear el NE utilizando el T2000.
3. Crear servicios SDH y monitorearlo con el instrumento.
4. Desconectar las fibras y verificar que se muestren las alarmas correctamente.
5. Conectar las fibras y verificar que la alarma desaparezca.

No.	Resultado

Fecha :
Firma :

5.- RESULTADO DE ENSAYOS

Se certifica que todas las pruebas detalladas en el presente documento fueron realizadas de acuerdo a los procedimientos y los resultados esperados fueron obtenidos durante el desarrollo de las mismas.

Huawei (Chile) S.A.

Ingeniero a Cargo : _____

Firma : _____

Telefonica CTC

Ingeniero a Cargo : _____

Firma : _____

Santiago de Chile, _____ **, 2006**

8. REFERENCIAS BIBLIOGRÁFICAS

[1] Mayer M. Ed, «Requirements for Automatic Switched Transport Network (ASTN)», ITU G.8070/Y1301, V1,0, Mayo 2001.

[2] Magd, Samoussi, Grammel, Belotti, «Automatic Switched Optical Network (ASON), Architecture and its Related Protocols », Internet Draft, draft-ietfipo-ason-o2.txt.

[3] Mayer M. Ed, «Architecture for Automatic Switched Optical Network (ASON)», ITU G.8080/Y1304, V1,0, Octubre 2001.

[4] Lazar M. et al, «Alternate Addressing Proposal», OIF Contribution, OIF 2001.21, Enero 2001.

[5] Ashwood-Smith P. et al, «Generalized MPLS-Signaling Functional Description», draftietf-mpls-generalized-signaling- 04.txt, work in progress, Mayo 2001.

[6] Recomendación UIT G.807/Y.1302, «Requisitos de la Red de Transporte con Conmutación Automática», Julio 2001.

[7] Recomendación UIT G.872 «Arquitectura de las Redes de transporte Ópticas», Febrero 1999.

[8] Recomendación UIT G.8080/Y.1304 «Arquitectura Conmutadas Automáticamente ASON», Noviembre 2001.

[9] Peter Tomsu, Christian Schmutzer, «Next Generation Optical Networks», Prentice Hall 2002.

[10] John Strand, Yong Xue, «Routing for Optical Networks with Multiple Routing Domains», Contribution number: OIF2001.046, Enero 2001.

[11] McBride, R. D. Awduche et al. "Requirements for Traffic Engineering over MPLS". IETF RFC 2702, September 1999

[12] E. Rosen, A. Viswanathan, R. Callon. "Multiprotocol Label Switching Architecture". Internet Draft <draft-ietf-mpls-arch-06.txt>, August 1999

[13] B. Jamoussi et al. "Multiprotocolo Label Switching Arquitecture". IETF RFC 3031, January 2001

[14] B. Jamoussi et al. "Constraint-Based LSP Setup using LDP". IETF RFC 3212, January 2002

[15] V.J. Friesen, J.J. Harms, J.W. Wong, "Resource Management with Virtual Paths in ATM networks". IEEE Network, vol 10 no 5, September/October 1996

[16] J. L. Marzo, E .Calle, C. Scoglio, T. Anjali "Adding QoS Protection in Order to Enhance MPLS QoS Routing" In proceedings of ICC 2003. Anchorage, Alaska (USA).

[17] J. Bigham, L.G. Cuthbert, A.L.G. Hayzelden, Z. Luo, "Multi-Agent System for Network Resource Management. Internat. Conference on Intelligence in Services and Networks", IS&N'99, Barcelona (Spain), April 1999

[18] Greg Osinaike, R.Bourne, C.Phillips, "Agent-Based Dynamic Configuration of Differentiated Traffic using MPLS with CR-LDP Signalling". 17th UK Teletraffic Symposium UKTS 2001, May 16-18, Dublin, Ireland

[19] Eusebi Calle, Pere Vilà, Jose L. Marzo, Santiago Cots "Arquitectura del sistema de gestión de ancho de banda y protección para entornos de redes MPLS (SGBP)" Symposium on Informatics and Telecommunications, SIT 2002. September 2002. Sevilla, Spain

[20] J.Ash et al. "Applicability Statement for CRLDP". IETF RFC 3213, January 2002

[21] B. Thomas et al. "LDP Applicability". IETF 3037, January 2001.

[22] G.Y.Cho and J.M. Chung. "Analysis of MPLS vs. MPLambdaS Next Generation Networking Technologies". IEEE 2001.

[23] M. Klinkowski and M. Marciniak. "QoS Guarantees in IP Optical Networks Using MPLS/MPLambdaS". IEEE – ICTON, 2001.

[24] H. Christiansen and H. Wessing. "Modeling GMPLS and optical MPLS networks". IEEE, 2003.

[25] Rick Gallaher. "Introduction to Multi-Protocol Lambda Switching (MPλS) and Generalized Multi-Protocol Label Switching (GMPLS). 2001.

[26] A. Kirstädter / A. Iselt. "Business Models for Next Generation Transport Networks", Norwell, MA, USA, July 2004