UNIVERSIDAD NACIONAL DE INGENIRÍA.

FACULTAD DE ELECTROTECNIA Y COMPUTACIÓN.

IMPLEMENTACIÓN A ESCALA DE LABORATORIODE UNA RED DE TRANSPORTE CON TECNOLOGÍA MIXTA SDH-IP.

Autor: Br. Alejandro Túpac Escobar Torres.

Tutor: MSc. Oscar Napoleón Martínez
Asesor: Ing. Pablo Ampie V. – Supervisor de Red de Transporte Claro Nicaragua

Managua, Agosto 2015.

Para mis padres Mariano y Martha y mi hermana Belén.

Pero en especial al más grande de todos, mi Señor JESUCRISTO.

Porque el Señor da la sabiduría; conocimiento y ciencia brotan de sus labios.

Proverbios 2:6.

AGRADECIMIENTOS.

"Deseo agradecer con todo mi corazón a mi Dios el Señor Jesucristo por su bondad y misericordia, reconociendo públicamente que soy lo que soy únicamente por él y para él".

A mis padres Mariano de Jesús Escobar Cortez y Martha Lorena Torres Sunsin, a mi hermana Belén de los Ángeles Escobar Torres y a mi novia Pamela María Cony Carballo Valverde, han sido de gran inspiración y me han brindado su apoyo y paciencia y sobre todo han creído en mí.

A mi tutor el Msc. Oscar Napoleón Martínez Zapata y al ingeniero Pablo Fernando Ampie por su apoyo y ejemplo, no solo como lo que es un gran profesional sino también como una maravillosa persona.

Y a todos los que hicieron posible y contribuyeron a la realización de este trabajo…

"Muchas Gracias"

ABSTRACT.

IP Transport Networks have been developed as a solution to provide greater capabilities to networks of mobile and fixed telephony, the development of IP over SDH has excelled for the facilities of implementation and high performance transport especially by Internet service.

SDH and IP network are networks that evolved to work with each other to maintain continuity of services, but with inadequate implementation can cause catastrophic effects difficult adjustments.

The main objective of this monograph is to implement a laboratory scale with a transport network based on SDH (Synchronous Digital Hierarchy) and (Internet Protocol) IP technology using low-ranking teams mixed technology. Milestones towards the issues raised are four: Determine the technical advantages and disadvantages of transport SDH technology (Synchronous Digital Hierarchy) technology and IP (Internet Protocol); Define the technical requirements to implement within the transport network mixed technology: SDH and IP; Mounting a mixed transport network, laboratory scale, equipment transportation low hierarchy and ultimately determine the most appropriate type for transporting data packets in a mixed transport network configuration.

The purpose of having divided the monograph thesis in these stages is to demonstrate the applicability of a mixed SDH-IP network within the transport network that solves this problem and ability to address future challenges: increased drastically and scalable width band; support services and transparent manner that is compatible with multi-elements; strong growth of the indicators of network availability; simplification of the provision, qualification, management and maintenance as many of these tasks are provided by the distributed control plane of the SDH technology; and exploitation of idle capacity links without affecting the quality of services offered by telephone operators.

All this is because the future trend is towards IP applications in the core transport network, SDH maintain supremacy. This technology (SDH) will be strengthened systems allow highly intelligent inventory management, provision and reorganization circuit fully automated manner.

RESUMEN.

Las Redes de Transporte IP Se han desarrollado como una solución para proveer mayores capacidades a las redes de servicios de telefonía móvil y fijas, el desarrollo de IP sobre SDH ha sobresalido por las facilidades de implementación y gran desempeño en especial por transporte del servicio de Internet.

La red SDH e IP son redes que fueron evolucionando para trabajar unas con otras para poder mantener la continuidad de los servicios, pero con una implementación inadecuada puede causar efectos catastróficos con difíciles adaptaciones.

El objetivo principal de este trabajo monográfico es implementar a escala de laboratorio una red de transporte con tecnología mixta basada en tecnología SDH (Synchronous Digital Hierarchy) y tecnología IP (Internet Protocol) utilizando equipos de baja jerarquía. Las etapas para lograr lo planteado son cuatro: Determinar las Ventajas y Desventajas técnicas de tecnología de transporte SDH (Synchronous Digital Hierarchy) y tecnología IP (Internet Protocol); Definir los requerimientos técnicos para implementar dentro de la red de transporte tecnología mixta: SDH e IP; Montar una red de transporte mixta, a escala de laboratorio, con equipos de baja jerarquía de transporte y finalmente Determinar el tipo de configuración más adecuada para transportar paquetes de datos en una red de transporte mixta.

El propósito de haber dividido la tesis monográfica en estas etapas es la de demostrar la aplicabilidad de una red mixta SDH-IP dentro de la red de transporte 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 SDH; y, explotación de la capacidad ociosa de enlaces, sin afectar la calidad de servicios ofrecidos por las operadoras de telefonía.

Todo esto se debe a que la tendencia futura apunta hacia aplicaciones IP en el núcleo de red de transporte, SDH mantendrá la supremacía. Esta tecnología (SDH) será fortalecida con sistemas de gestión altamente inteligentes que permitirán inventario, provisión y reorganización de circuitos de manera totalmente automatizada.

Tabla de Contenido

LISTA DE FIGURAS.

LISTA DE TABLAS.

LISTA DE ACRÓNIMOS.

IP	*Protocolo de Internet.*
SDH	*Jerarquia digital Sincrona.*
CAPEX	*Capital Expenditure*
OPEX	*OperationalExpediture.*
ATM	*Asynchronous Transfer Mode*
NGN	*Next Generation Network*
OSI	*Open System Interconnection.*
ANSI	*American National Standards Institute.*
SONET	*Synchronous Optical Network*
UIT	*Unión Internacional de Telecomunicaciones.*
STM-1	*Synchronous Transport Module – Level 1.*
PDH	*Plesiochronous Digital Hierarchy.*
Mbps	*Mega Bits por Segundo.*
POH	*Path Overhead.*
TU	*Tributary Unit*
GSM	*Global System for Mobile; Originally, GROUPE SPÉCIAL MOBILE.*
VC	*Virtual Container.*
AU	*unidades administrativas*
TUG	*Tributary Unit Group.*
SOH	*Section Overhead*
SLA	*Service Level Agreement.*
WDM	*Dense Wavelength Division Multiplexing.*
RIP	*Interior Gateway Protocol.*
HTTP	*Protocolo de Transferencia de Hipertexto*
UDP	*Protocolo de Datagrama de Usuario*
DNS	*Sistema de Nombres de Dominio.*
MPLS	*Multiprotocol Label Switching.*
LAN	*Local Area Network*
WAN	*Wide Area Network.*
TDM	*multiplexación por división de tiempo.*
LTE	*Long Term Evolution*
RADIUS	*Remote Access Dial In User Server*
PCM	*pulse code modulation*
RAN	*Red de Acceso Radio*
UMTS	*Universal Mobile Telecommunications Service*
CDMA	*Code Division Multiple Access*

1 Introducción.

1.1. Avances Tecnológicos

Una de las necesidades del hombre sin duda de las más importantes es la de comunicarse con sus semejantes. Para ello ha utilizado todos los recursos que ha podido, tales como el habla, la escritura, el dibujo etc. Hoy en día las telecomunicaciones forman parte del cotidiano vivir, ya que por medio de estas podemos acceder a muchos servicios y beneficios como lo es el caso del internet.

Con el aumento del tráfico por el uso de servicios de Internet y datos en telefonía móvil y fija [1] y con el crecimiento en la demanda por mayor ancho de banda exigen que se busquen nuevas tecnologías de transmisión, por esa razón se ha ido implementando tecnología IP[1], por las facilidades de capacidad y velocidades que esta ofrece en los servicios demandados, el uso de la tecnología se debe a la popularidad y sencillez que esta ofrece, de manera que poco a poco ha logrado sustituir la antigua tecnología SDH como tecnología de transporte absoluta. El uso del IP también ha venido a reducir los costos operativos de las empresas tanto en su presupuesto CAPEX[2] como el OPEX[3] [2]. La tecnología inicial SDH[4] debido a su estabilidad, robustez y su calidad de servicio se ha mantenido aún vigente como tecnología implementada en transporte de servicios de telecomunicaciones.

Actualmente, y desde hace ya algún tiempo nos encontramos en una situación de gran crecimiento de tráfico de datos, como consecuencia, principalmente, de la generalización del uso de internet. Este aumento de tráfico no viene solo determinado por el cada vez mayor número de personas conectadas a la red, sino también influye el

1 IP: Internet Protocol, es un protocolo de comunicación de datos digitales clasificado funcionalmente en la Capa de Red según el modelo internacional OSI, Su función principal es el uso bidireccional en origen o destino de comunicación para transmitir datos mediante un protocolo no orientado a conexión que transfiere paquetes conmutados a través de distintas redes físicas.

2 CAPEX:Capital Expenditure, es un gasto de negocio incurrido para crear el beneficio futuro es decir, la adquisición de activos que tienen una vida útil más allá del año fiscal.

3 OPEX: OperationalExpediture, es el dinero que el negocio gasta con el fin de convertir el inventario en el rendimiento. Los gastos de explotación también incluyen la depreciación de plantas y maquinaria que se utilizan en el proceso de producción.

4 SDH: Synchronous Digital Hierarchy, sistema que permite el transporte de los servicios de telecomunicaciones de alta capacidad sincronizándolos bajo una única referencia reloj para ser transportado de forma efectiva y estable bajo un medio de transporte sea Fibra Óptica o radio hasta si destino final.

hecho de que cada vez los usuarios acceden a ella con mayor frecuencia y transmiten un mayor volumen de información de forma percapita[5] [3].

Para comprender esta problemática en función de la demanda de ancho de banda, muchas empresas han comenzado a migrar a redes de transporte con protocolo IP, debido a que estas en su origen eran tecnología SDH. Debido a las tendencias de implementar nuevas tecnologías que permita mejorar las capacidades y desarrollar un mejor desempeño en los servicios, la tecnología IP ha logrado dar esas mejoras operativas en el desempeño y permite que las empresas que proveen estos servicios sean más competitivas en el mercado de las telecomunicaciones.

Dar una solución sin complicar la operación de la red, sería la implementación de una red mixta, SDH e IP dentro de la red de transporte, ya que migrar la red de transporte a full IP de una manera brusca generaría gastos excesivo para la empresa proveedora de servicios, de manera que lo natural es hacer las migraciones de SDH a IP de manera gradual, y el mantener mucho tiempo el uso de redes de transporte SDH incurren en ofrecer ciertas limitantes en las simetría de los enlace de Internet a los clientes.

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 aporten ventajas competitivas.

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 ha visto una evolución global tendiente a simplificar e integrar las redes, llevando drásticamente todo a IP. [19] En la Figura 1.1, se aprecia este perfeccionamiento.

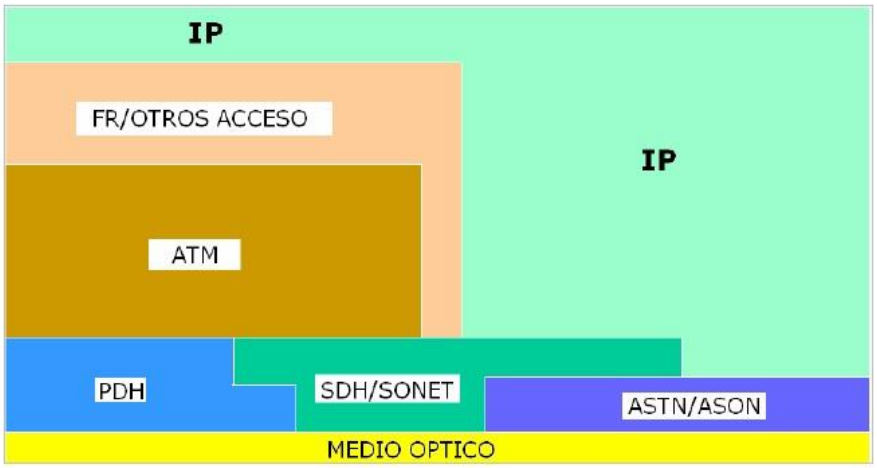


Figura 1.1: Evolución Hacia "Todo IP", Sobre una red SDH.

5 Generalmente se utiliza para indicar la media por persona en una estadística social determinada.

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. [3]

Los requerimientos para los cuales se diseñaron las redes actuales han cambiado como se muestra en la Tabla 1:

Tabla 1.1: comparación de requerimiento de la Red.

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

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[6], las que en definitiva llevan los servicios de un cliente final. Estas implementaciones son ineficientes. Se deben preparar las redes para la integración de las tecnologías SDH e IP como red mixta dentro de la red de transporte y esto se debe realizar con miras a reutilizar las inversiones existentes.

6 El Modo de Transferencia Asíncrona (Asynchronous Transfer Mode, ATM) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

1.3. Etapas para la Implementación de Tecnologías Mixta SDH-IP dentro de la red de Transporte.

Sin duda los nuevos elementos de NGN[7] ("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. [17]

1.4 Antecedentes.

El actual uso de las telecomunicaciones va tomando auge basándose en mayor consumo de ancho de bandas para transmisión de paquetes, y esto por el crecimiento del uso de la Internet más que en el uso de planes de voz. Es aquí donde se da la necesidad de implementar tecnología IP como transporte, debido a que la anterior tecnología que aún se encuentra en uso como es el caso de SDH, no logra cubrir las demandas requeridas para los nuevos servicios y futuras tendencias del mercado.

En la red de transporte de otros países se han venido trabajando en la integración de diferentes tecnologías que permitan la armonía en la red, como lo es el caso de ANATEL (Asociación Nacional de Televisión de Chile) que ha venido trabajando en la implementación de tecnología IP/MPLS, con el propósito de mejorar la calidad del transporte de tráfico y ser más robusta a posibles fallas en la red.

En julio de 2012 el Banco Interamericano de Desarrollo público un documento para debate en donde se presenta un argumento sobre el rol de las Tecnologías de la Información y Comunicación (TIC) en Nicaragua en donde se describe un diagnóstico del estado actual de la penetración y uso de las TIC en Nicaragua, e identifica los principales retos y desafíos. Siendo la banda ancha una de las grandes alternativas para que el país logre su desarrollo, esto conllevaría a la necesidad de migrar de tecnología de manera paulatina. [6]

Publicaciones por el gobierno a través de ENATREL en Marzo del 2008, hacen referencia a integraciones con redes de transporte IP independientes en nuevos proyectos con respecto a las redes SDH que ya tenían en existencia, esta empresa buscando su proyección en ámbito tecnológico, ya estaba previendo el uso mixto de tecnologías. [7]

7 Se refiere a la evolución de la actual infraestructura de redes de telecomunicación y acceso telefónico con el objetivo de lograr la convergencia tecnológica de los nuevos servicios multimedia (voz, datos, video...) en los próximos 5-10 años.

Tesis monográficas se han realizado en otros países en donde se le da una alternativa a la necesidad de ancho de banda llegando a implementar una red mixta de diferentes tecnologías dentro de la red de transporte como lo es el caso del ingeniero Jorge Pozo de origen chileno que en 2006 su tesis se basó en proponer una integración de tecnología de transporte digital como lo es ASON8/GMPLS9, ya que es compatible con elementos multiservicios y posibles crecimientos de la red de transporte de Chile.

1.5 Planteamiento de Problema.

En Nicaragua se han desarrollado en su mayoría redes de transporte bajo tecnología SDH, debido a que fue instalada desde hace más de 12 años, en aquel entonces el SDH era la tecnología más predominante y el IP no había desarrollado todas las ventajas con las que actualmente cuenta. También se debe considerar que muchos clientes corporativos al que se le provee servicio de voz fija y datos, aún mantienen en sus equipos propios conexión con transporte bajo tecnología SDH. La sustitución de la tecnología SDH a nivel mundial se completará hasta tener opciones totales con tecnología IP, ya que en la actualidad la tecnología IP como transporte en redes de telefonía aún no ha desarrollado su máxima capacidad [9], y se espera que muchas limitantes sean superadas al cabo de algunos años, este podría ser un detalle sobresaliente que de momento mantiene en vida a los equipos de transporte SDH.

Esto mismo ha ocurrido en diferentes países del mundo como es el caso de Colombia que por el crecimiento de tráfico en las redes de acceso, el abaratamiento del ancho de banda y los canales dedicados a servicios gubernamentales y a grandes empresas han tenido que implementar tecnologías mixtas en las redes de transporte. [10], por lo que Nicaragua no puede quedarse atrasada ya que con el uso de las TIC suponen una oportunidad para el desarrollo y el cambio social. Esto representa un tema de mucho interés en el sector de las telecomunicaciones de nuestro país, por lo que surgen muchas interrogantes al respecto tales como:

¿Dicha implementación mejoraría o afectaría el nivel de calidad en los servicios de voz y datos en la interconexión de tecnología LTE, 3G y 2G?

¿Cómo será la calidad de servicio que se le brindaría a las empresas de telecomunicaciones?

¿Qué ventajas técnicas tendrían las empresas de telecomunicaciones en integrar ambas tecnologías dentro de la red de transporte?

[8] ***automatically switched optical network es un concepto en la evolución de redes de transporte que permite un control dinámico dirigido por políticas en una red óptica o una SONET basada en señales entre usuario y los componentes de la red***

[9] ***General Multiprotocol Label Switching está enfocado al plano de control de las distintas capas ya que cada una de ellas pueden usar físicamente diferentes tipos de datos. Por lo tanto, la intención es cubrir tanto la señalización como la parte de enrutamiento de este plano de control.***

1.6 Objetivos.

1.6.1 Objetivo General.

- ✓ Implementar a escala de laboratorio una red de transporte mixta basada en tecnología SDH (Synchronous Digital Hierarchy) y tecnología IP (Internet Protocol) utilizando equipos de baja jerarquía.

1.6.2 Objetivos específicos.

- ✓ Determinar las Ventajas y Desventajas técnicas de tecnología de transporte SDH (Synchronous Digital Hierarchy) y tecnología IP (Internet Protocol).
- ✓ Definir los requerimientos técnicos para implementar dentro de la red de transporte tecnología mixta: SDH e IP.
- ✓ Montar una red de transporte mixta, a escala de laboratorio, con equipos de baja jerarquía de transporte.
- ✓ Determinar el tipo de configuración más adecuada para transportar paquetes de datos en una red de transporte mixta.

1.7 JUSTIFICACIÓN.

Las actuales empresas de telecomunicaciones a nivel nacional aún mantienen vigente equipos de transporte con tecnología SDH en gran parte de la red, en especial equipos nodales de alta jerarquía que permiten la conexión entre centrales. La mayoría son equipos que manejan el tráfico de los concentradores de voz fija, servicios de ADSL hacia las centrales y la interconexión entre sitios BTS10 hacia la BSC11 o de las BSC hacia la central de telefonía celular MSC, todas las modificaciones que se efectúen a este nivel son complejas y las afectaciones críticas, debido a la alta concentración de servicios. La integración con la tecnología de transporte IP da garantía de mayores anchos de bandas en los servicios por su estandarización con los protocolos TCP/IP en datos e Internet.

El crecimiento de tráfico en las redes de acceso y la necesidad de ancho de banda han obligado a los operadores a fortalecer sus redes en sintonía con los desarrollos tecnológicos globales, lo que empuja a las empresas nacionales a invertir por una nueva tecnología que les proporcione las mejoras requeridas, muchas de las cuales se complican en el proceso de integración, siendo el caso de adaptar tecnología de transporte IP con tecnología SDH existente, ya que en casos muy graves pueden dejar los servicios operativos con bajo nivel de calidad por detalles de incompatibilidad que no fueron analizados ni identificados previamente, por lo que las migraciones no deben verse como un proceso de sustitución sencillo que se puedan elaborar en lapsos de tiempo autorizados dentro de la red.

[10] BTS: Base Transiever Station, son las repetidoras que emiten las señales inalámbricas para generar la cobertura del servicio de telefonía celular.

[11] BSC: Base Swithing Center, es la central local que maneja a un grupo de BTS, es la que se encarga de conmutar las llamadas y asignar las frecuencias en el grupo.

CAPÍTULO I.

2. El presente de las Redes de Transporte y su Evolución hacia una integración de Tecnologías Mixtas

2.1. Descripción Del Capítulo.

En esta parte se hará una descripción de la actual tecnología de transmisión y los servicios que esta soporta, en particular, el estándar SDH ("Synchronous Digital Hierarchy") para comprender las funcionalidades de las actuales redes y los cambios que debe sufrir en su posible integración como red mixta, hablaremos sobre el protocolo IP y su gran utilidad como tecnología de transporte, abordaremos los 2 tipos de modelo, modelo OSI[12] y modelo TCP/IP[13] y haremos una breve comparación entre ambos modelos 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 está 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[14] publicó su estándar SONET[15]. (Red óptica síncrona). Las

12 El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), más conocido como "modelo OSI" (en inglés, Open System Interconnection), es el modelo de red descriptivo, que fue creado en el año 1980 por la Organización Internacional de Normalización (ISO, International Organization for Standardization).[
13 El modelo TCP/IP describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red.
14 American National Standards Institute es una organización sin fines de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos.
15 Synchronous Optical Network, cuyo acrónimo es SONET) es un estándar para el transporte de telecomunicaciones en redes de fibra óptica.

recomendaciones de la UIT-T[16] 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 más baja jerarquía como las provenientes del estándar PDH[17] ("Plesiochronous Digital Hierarchy") por medio de puertos tributarios adecuados La formación de la señal sincrónica es la que se muestra en la figura2.1. [18]

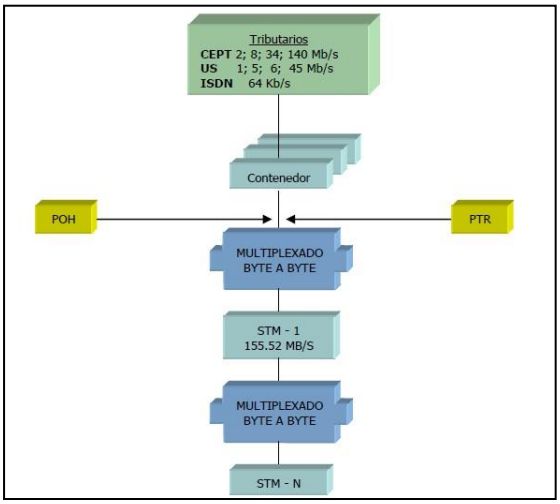


Figura 2.1: Formación de la señal sincrónica a partir de jerarquías menores

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 van volviendo a multiplexar byte a byte N módulos STM-1.

16 Union Internacional de Telecomunicaciones es el órgano permanente de la Unión Internacional de Telecomunicaciones (UIT) que estudia los aspectos técnicos, de explotación y tarifarios, y publica normativas sobre los mismos, con vista a la normalización de las telecomunicaciones a nivel mundial.
17 PDH es una tecnología usada en telecomunicación tradicionalmente para telefonía que permite enviar varios canales telefónicos sobre un mismo medio (ya sea cable coaxial, radio o microondas) usando técnicas de multiplexación por división de tiempo y equipos digitales de transmisión

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 crossconnects 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. [18]

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. [18]

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. [18]

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 2.2.

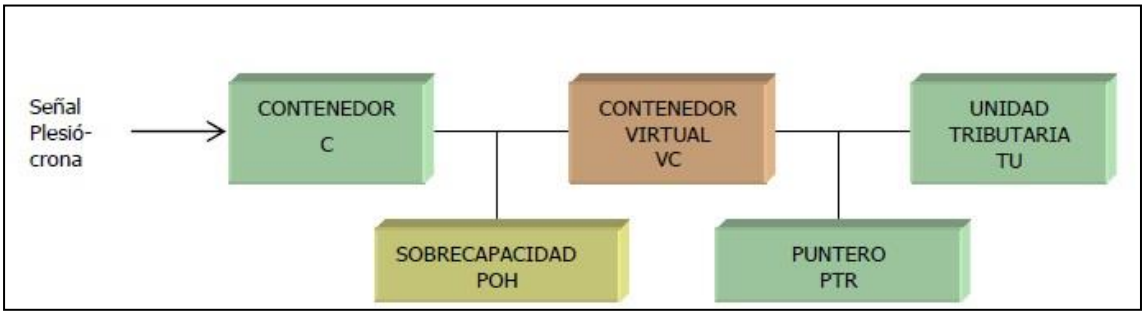


Figura 2.2.: Proceso de creación de la señal tributaria

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 2.3 se grafican las distintas alternativas para obtener un módulo STM-1 a partir de múltiples señales tributarias.

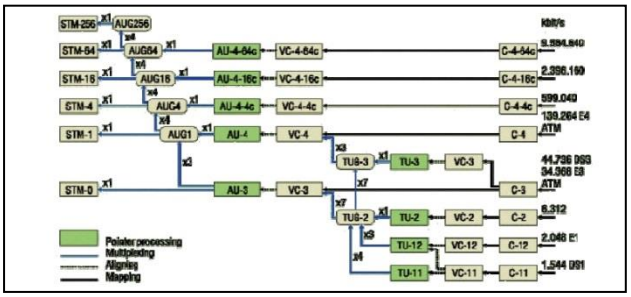


Figura 2.3.: Alternativas para la obtención de señales SDH

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 2.4:

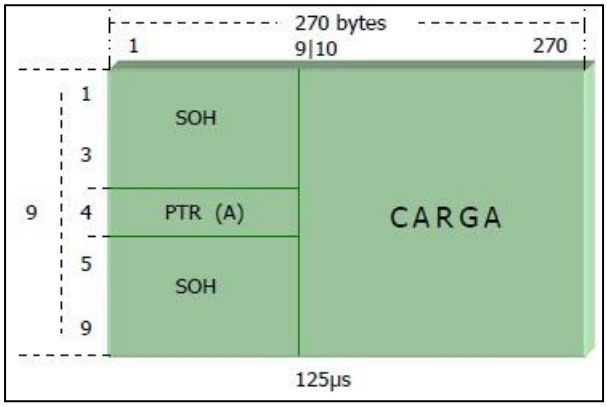


Figura 2.4.: Estructura de la trama STM-1

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[18]). [18]

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 2.5.

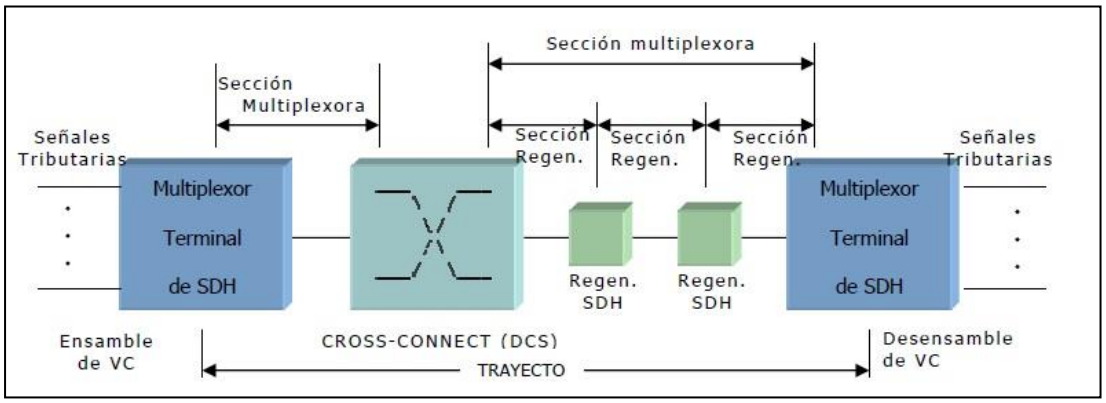


Figura 2.5.: Secciones de una red SDH

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.

18 PCM es un procedimiento de modulación utilizado para transformar una señal analógica en una secuencia de bits (señal digital)

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 [18]

+ 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 qué 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 crossconexiones 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 MSSPRing, 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.

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. [18]

2.2.1.5.7. Protección de Conexión de Subred (SNCP)

SNCP es similar al 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 2.6 muestra la forma en que opera:

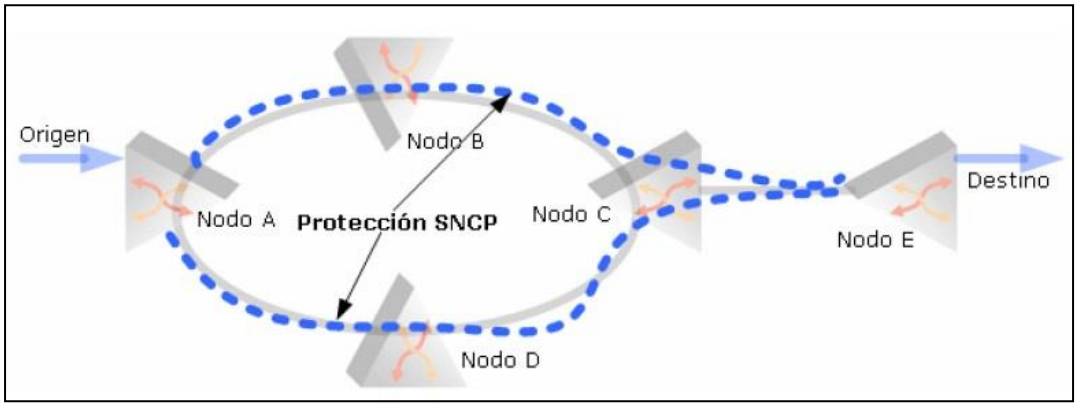


Figura 2.6.: Protección SNCP de trayecto

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. [18]

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 2.7, se ilustra esta situación:

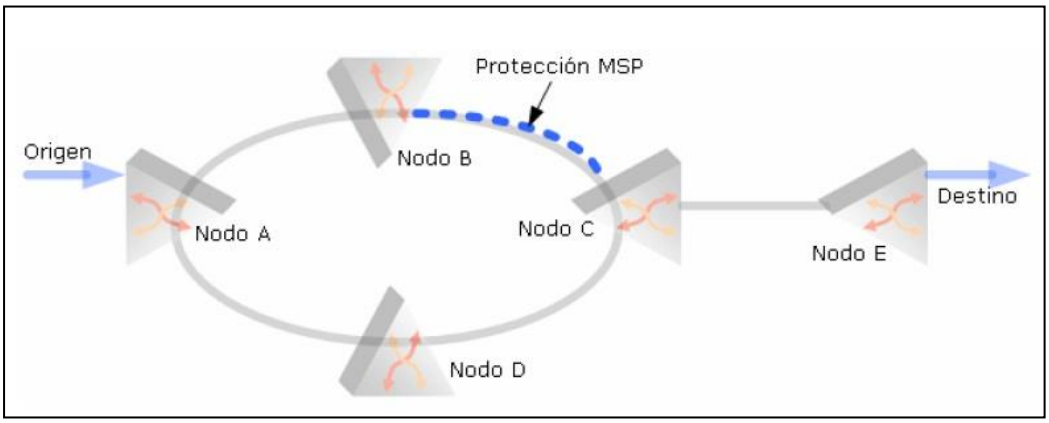


Figura 2.7.: Protección MSP de sección

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. [18]

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 2.8 muestra la operación de esta protección:

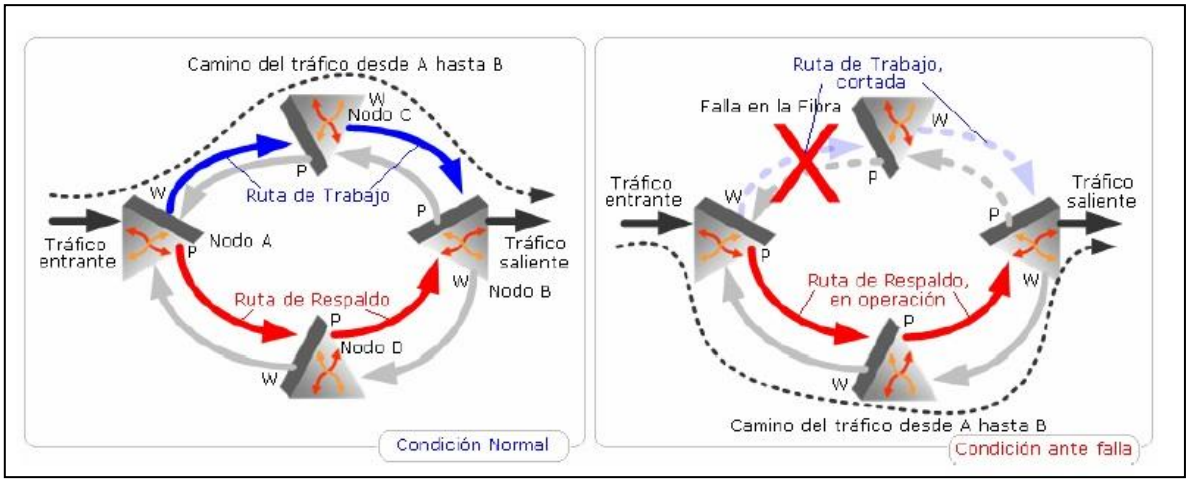


Figura 2.8.: Anillo de protección dedicada

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 está 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 2.9 representa tal configuración: [18]

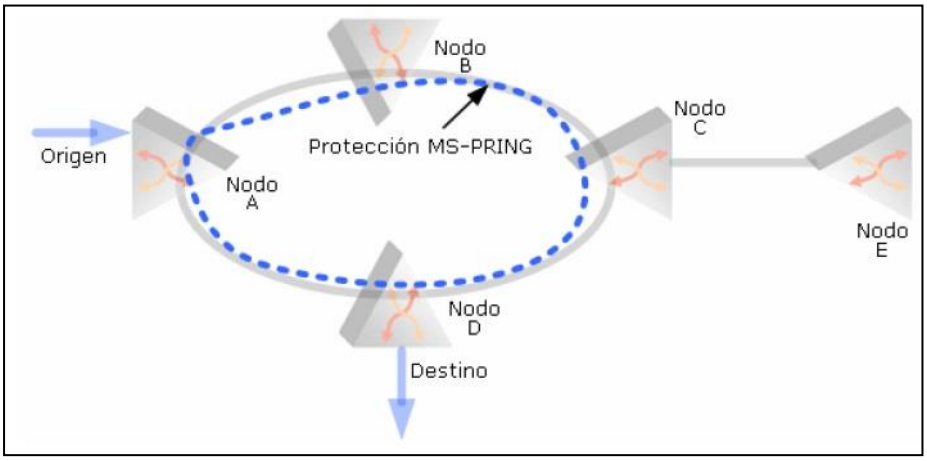


Figura 2.9.: Protección MS-PRING, en la configuración de anillo

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. [18]

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 2, 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.

Tabla2.1.: Cuadro comparativo entre esquemas de protección SDH.

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*

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. [18]

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. Interfaces de Línea de SDH

Se definen para SDH interfaces físicas tanto ópticas como eléctricas.

2.2.1.6.1. Interfaces ópticas

Hay tres grados de aplicación distintos:

- 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.

- 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.

- 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. Interfaces 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.- DXCs. (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[19] 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.

19 WDM es el acrónimo, en inglés, de Dense Wavelength Division Multiplexing, que significa multiplexado compacto por división en longitudes de onda. DWDM es una técnica de transmisión de señales a través de fibra óptica usando la banda C (1550 nm).

2.3. IP (Protocolo de Internet)

2.3.1Definicion

IP es el principal protocolo de la capa red. Define la unidad básica para la transferencia de datos en una interred, especificando el formato exacto de un Datagrama IP.

IP es un protocolo no orientado a conexión debido a que cada uno de los paquetes puede seguir rutas distintas entre el origen y el destino, es por esto que los paquetes pueden llegar duplicados o desordenados. Es no confiable, porque los paquetes pueden perderse, dañarse o llegar retrasados.

El software IP es el encargado de elegir la ruta más adecuada por la que los datos serán enviados. Representa, la conectividad y la estrategia de la flexibilidad aunque no puede priorizar, ni reservar recursos.

Los routers, indispensables en de toda red IP, son los encargados de reenviar, en tiempo real, datagramas a otros routers basándose en su tabla local parametrizada por distancia (RIP[20]) o camino óptimo (OSPF[21]). La tabla que puede llegar a tener muchos miles de entradas y la caótica dispersión de las direcciones disminuyen su eficacia. Si el ancho de banda es limitado IP no puede por sí mismo ofrecer servicios diferenciados. Diversos protocolos como el RSVP, DiffServ y otros, pretenden proporcionar garantía de calidad a las redes IP reservando recursos, marcando los datagramas, priorizando colas y diferenciando rutas. Sin embargo, estos protocolos tienen serias dificultades a la hora de escalar en la WAN o no permiten realmente diferenciar servicios ni garantizar su calidad, simplemente son un método de priorización

2.3.2 Datagrama IP

Un datagrama IP consiste en una parte de encabezado y una parte de texto. El encabezado tiene una parte fija de 20 bytes y una parte opcional de longitud variable. El formato del encabezado se muestra en la figura 2.10. Se transmite en orden de big endian: de izquierda a derecha, comenzando por el bit de orden mayor del campo de Versión. (SPARC es big endian; Pentium es little endian.). [13]

El transporte en modo datagrama permite la agregación de todo tipo de tráficos, independientemente del tipo de servicio. De hecho, estructura la información

20 RIP Es un protocolo de puerta de enlace interna o IGP (Interior Gateway Protocol) utilizado por los routers (encaminadores) para intercambiar información acerca de redes IP a las que se encuentran conectados.

21 OSPF es un protocolo de encaminamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo SmoothWall Dijkstra enlace-estado (LSE - Link State Algorithm) para calcular la ruta más idónea.

separando perfectamente el contenido del continente, organizándose este último como un datagrama que es encaminado extremo a extremo y de forma individualizada, sin necesidad de ningún procedimiento de señalización.

Esto proporciona una total flexibilidad en el transporte de la información, permitiendo que un determinado servicio pueda manejar flujos de información de naturaleza diferente. El enrutamiento de la información se realiza a partir de la dirección destino del datagrama y de acuerdo a las tablas de encaminamiento de los nodos de conmutación de la red. Estas tablas son establecidas de forma automática por los procedimientos de encaminamiento.

El campo de **Versión** lleva el registro de la versión del protocolo al que pertenece el datagrama. Al incluir la versión en cada datagrama, es posible hacer que la transición entre versiones se lleve meses, o incluso años, ejecutando algunas máquinas la versión vieja y otras la versión nueva. En la actualidad, se está trabajando en una transición entre IPv4 e IPv6, la cual ha tomado años, y no está cerca de terminarse (Durand, 2001; Wiljakka, 2002, y Waddington y Chang, 2002). Algunas personas incluso piensan que nunca se terminará (Weiser, 2001). Como una adición a la numeración, IPv5 fue un protocolo de flujo experimental en tiempo real que no se utilizó ampliamente.

Dado que la longitud del encabezado no es constante, se incluye un campo en el encabezado, **IHL**, para indicar la longitud en palabras de 32 bits. El valor mínimo es de 5, cifra que se aplica cuando no hay opciones. El valor máximo de este campo de 4 bits es 15, lo que limita el encabezado a 60 bytes y, por lo tanto, el campo de Opciones a 40 bytes. Para algunas opciones, por ejemplo para una que registre la ruta que ha seguido un paquete, 40 bytes es muy poco, lo que hace inútil esta opción.

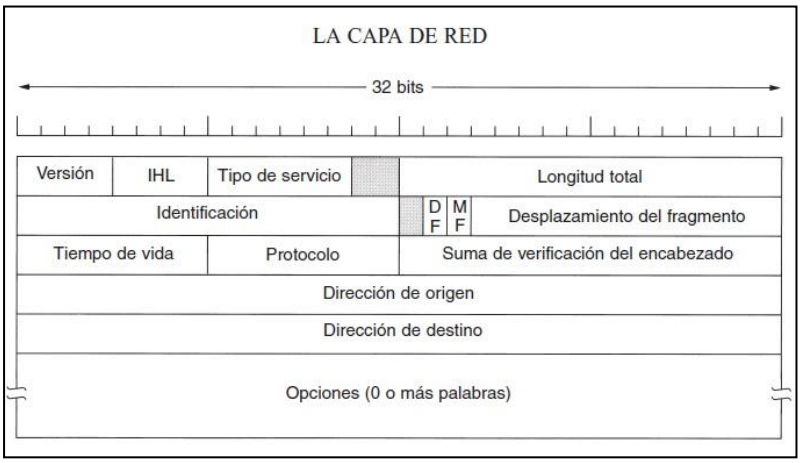


Figura 2.10. El encabezado de IPv4 (Protocolo Internet).

El campo de **Tipo de servicio** es uno de los pocos campos que ha cambiado su significado (levemente) durante años. Su propósito aún es distinguir entre las

diferentes clases de servicios. Son posibles varias combinaciones de confiabilidad y velocidad. Para voz digitalizada, la entrega rápida le gana a la entrega precisa. Para la transferencia de archivos, es más importante la transmisión libre de errores que la rápida.

Originalmente, el campo de 6 bits contenía (de izquierda a derecha) un campo de Precedencia de tres bits y tres banderas, D, T y R. El campo de Precedencia es una prioridad, de 0 (normal) a 7 (paquete de control de red). Los tres bits de bandera permiten al host especificar lo que le interesa más del grupo retardo (delay), velocidad real de transporte (throughput), confiabilidad (reliability). En teoría, estos campos permiten a los enrutadores tomar decisiones entre, por ejemplo, un enlace satelital de alto rendimiento y alto retardo o una línea arrendada con bajo rendimiento y poco retardo. En la práctica, los enrutadores actuales ignoran por completo el campo de Tipo de servicio, a menos que se les indique lo contrario.

En algún momento, la IETF tiró la toalla y cambió el campo ligeramente para acomodar los servicios diferenciados. Seis de los bits se utilizan para indicar a cuáles de las clases de servicios analizadas anteriormente pertenece cada paquete. Estas clases incluyen las cuatro propiedades de encolamiento, tres posibilidades de eliminación y las clases históricas. [13]

La **Longitud total** incluye todo el datagrama: tanto el encabezado como los datos. La longitud máxima es de 65,535 bytes. Actualmente este límite es tolerable, pero con las redes futuras de gigabits se requerirán datagramas más grandes.

El campo de **Identificación** es necesario para que el host de destino determine a qué datagrama pertenece un fragmento recién llegado. Todos los fragmentos de un datagrama contienen el mismo valor de Identificación.

A continuación viene un bit sin uso y luego dos campos de 1 bit. **DF** significa no fragmentar (Don't Fragment); es una orden para los enrutadores de que no fragmenten el datagrama, porque el destino es incapaz de juntar las piezas de nuevo. Por ejemplo, al arrancar una computadora, su ROM podría pedir el envío de una imagen de memoria a ella como un solo datagrama. Al marcar el datagrama con el bit DF, el transmisor sabe que llegará en una pieza, aún si significa que el datagrama debe evitar una red de paquete pequeño en la mejor ruta y tomar una ruta subóptima. Se requiere que todas las máquinas acepten fragmentos de 576 bytes o menos.

MF significa más fragmentos. Todos los fragmentos excepto el último tienen establecido este bit, que es necesario para saber cuándo han llegado todos los fragmentos de un datagrama. El Desplazamiento del fragmento indica en qué parte del datagrama actual va este fragmento. Todos los fragmentos excepto el último del datagrama deben tener un múltiplo de 8 bytes, que es la unidad de fragmentos

elemental. Dado que se proporcionan 13 bits, puede haber un máximo de 8192 fragmentos por datagrama, dando una longitud máxima de datagrama de 65,536 bytes, uno más que el campo de Longitud total. Una vez que la capa de red ha ensamblado un datagrama completo, necesita saber qué hacer con él. El campo de Protocolo indica el protocolo de las capas superiores al que debe entregarse el paquete. TCP es una posibilidad, pero también está UDP[22] y algunos más.

La **Suma de verificación del encabezado** verifica solamente el encabezado. Tal suma de verificación es útil para la detección de errores generados por palabras de memoria erróneas en un enrutador. El algoritmo es sumar todas las medias palabras de 16 bits a medida que llegan, usando aritmética de complemento a uno, y luego obtener el complemento a uno del resultado. Para los fines de este algoritmo, se supone que la suma de verificación del encabezado es cero cuando llega el paquete al destino. Este algoritmo es más robusto que una suma normal. Observe que la suma de verificación del encabezado debe recalcularse en cada salto, pues cuando menos uno de los campos siempre cambia (el campo de Tiempo de vida), pero pueden usarse trucos para acelerar el cálculo.

La **Dirección de origen y la Dirección de destino** indican el número de red y el número de host. Estudiaremos las direcciones de Internet en la siguiente sección. El campo de **Opciones** se diseñó para proporcionar un recurso que permitiera que las versiones subsiguientes del protocolo incluyeran información no presente en el diseño original, para permitir que los experimentadores prueben ideas nuevas y para evitar la asignación de bits de encabezado a información pocas veces necesaria. Las opciones son de longitud variable. Cada una empieza con un código de 1 byte que identifica la opción. Algunas opciones van seguidas de un campo de longitud de la opción de 1 byte, y luego de uno o más bytes de datos. El campo de Opciones se rellena para completar múltiplos de cuatro bytes. Originalmente se definieron cinco opciones, como se lista en la figura 2.11, pero se han agregado otras más. [13]

Opción	Descripción
Seguridad	Especifica qué tan secreto es el datagrama
Enrutamiento estricto desde el origen	Indica la ruta completa a seguir
Enrutamiento libre desde el origen	Da una lista de los enrutadores que no deben evitarse
Registrar ruta	Hace que cada enrutador agregue su dirección IP
Marca de tiempo	Hace que cada enrutador agregue su dirección y su marca de tiempo

Figura 2.11. Algunas de las opciones del IP.

La opción de **seguridad** indica qué tan secreta es la información. En teoría, un enrutador militar puede usar este campo para especificar que no se enrute a través de

22 UDP es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI).

ciertos países que los militares consideren "malos". En la práctica, todos los enrutadores lo ignoran, por lo que su única función real es la de ayudar a los espías a encontrar la información importante con mayor facilidad.

La opción de **enrutamiento estricto desde el origen** da la ruta completa desde el origen hasta el destino como secuencia de direcciones IP. Se requiere que el datagrama siga esa ruta exacta. Esta opción se usa sobre todo cuando los administradores de sistemas envían paquetes de emergencia porque las tablas de enrutamiento se han dañado, o para hacer mediciones de tiempo. La opción de **enrutamiento libre desde el origen** requiere que el paquete pase por los enrutadores indicados en la lista, y en el orden especificado, pero se le permite pasar a través de otros enrutadores en el camino. Normalmente, esta opción sólo indicará algunos enrutadores, para obligar a una ruta en particular. Por ejemplo, si se desea obligar a un paquete de Londres a Sydney a ir hacia el oeste en lugar de hacia el este, esta opción podría especificar enrutadores en Nueva York, Los Ángeles y Honolulú. Esta opción es de mucha utilidad cuando las consideraciones políticas o económicas dictan pasar a través de, o evitar, ciertos países. La opción de **registrar ruta** indica a los enrutadores a lo largo de la ruta que agreguen su dirección IP al campo de opción. Esto permite a los administradores del sistema buscar fallas en los algoritmos de enrutamiento ("¿por qué todos los paquetes de Houston a Dallas pasan por Tokio primero?"). Al establecer inicialmente ARPANET, ningún paquete pasaba nunca por más de nueve enrutadores, por lo que 40 bytes de opciones eran más que suficientes. Como se mencionó antes, ahora esto es demasiado poco. Por último, la opción de **marca de tiempo** es como la opción de registrar ruta, excepto que además de registrar su dirección IP de 32 bits, cada enrutador también registra una marca de tiempo de 32 bits. Esta opción también es principalmente para búsquedas de fallas en los algoritmos de enrutamiento. [13]

2.3.3. Direcciones IP

Cada host y enrutador de Internet tiene una dirección IP, que codifica su número de red y su número de host. La combinación es única: no hay dos máquinas que tengan la misma dirección IP.

Todas las direcciones IP son de 32 bits de longitud y se usan en los campos de Dirección de origen y de Dirección de destino de los paquetes IP. En importante mencionar que una dirección IP realmente no se refiere a un host. En realidad se refiere a una interfaz de red, por lo que si un host está en dos redes, debe tener dos direcciones IP. Sin embargo, en la práctica, la mayoría de los hosts se encuentran en una red y, por lo tanto, tienen una dirección IP.

Por varias décadas, las direcciones IP se dividieron en cinco categorías, las cuales se listan en la figura 2.12. Esta asignación se ha llamado direccionamiento con clase

(classful addressing). Ya no se utiliza, pero en la literatura aún es común encontrar referencias. Más adelante analizaremos el reemplazo del direccionamiento con clase.

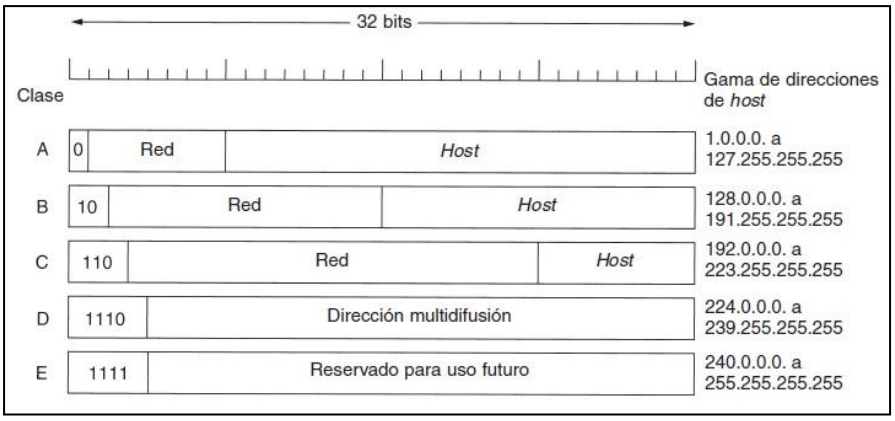


Figura 2.12. Formatos de dirección IP.

Los formatos de clase A, B, C y D permiten hasta 128 redes con 16 millones de hosts cada una, 16,382 redes de hasta 64K hosts, 2 millones de redes (por ejemplo, LANs) de hasta 256 hosts cada una (aunque algunas son especiales). También soportan la multidifusión, en la cual un datagrama es dirigido a múltiples hosts. Las direcciones que comienzan con 1111 se reservan para uso futuro. Hay cerca de 500,000 redes conectadas a Internet, y la cifra se duplica cada año. Los números de redes son manejados por una corporación no lucrativa llamada ICANN (Corporación de Internet para la Asignación de Nombres y Números) para evitar conflictos. A su vez, ICANN ha delegado partes del espacio de direcciones a varias autoridades regionales, las cuales han repartido direcciones IP a los ISPs y a otras compañías.

Las direcciones de red, que son números de 32 bits, generalmente se escriben en notación decimal con puntos. En este formato, cada uno de los 4 bytes se escribe en decimal, de 0 a 255. Por ejemplo, la dirección hexadecimal C0290614 se escribe como 192.41.6.20. La dirección IP menor es 0.0.0.0 y la mayor 255.255.255.255.

Los valores 0 y −1 (todos 1s) tienen significado especial, como se muestra en la figura 2.13. El valor 0 significa esta red o este host. El valor −1 se usa como dirección de difusión para indicar todos los hosts de la red indicada.

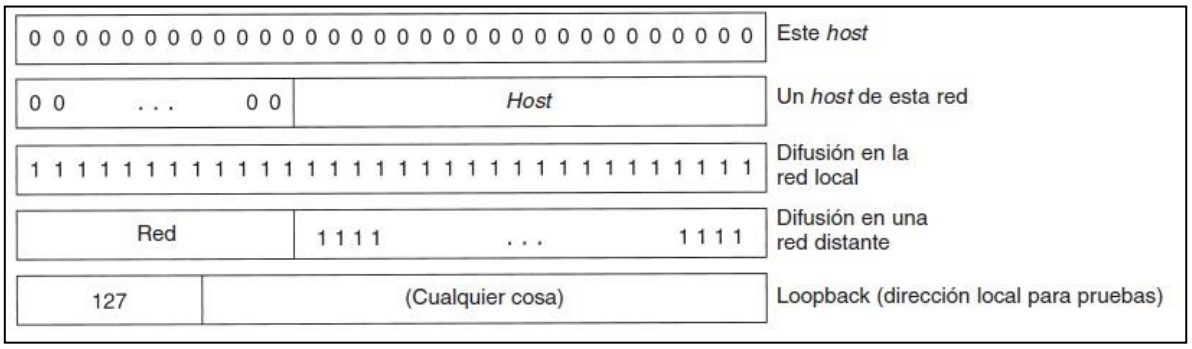


Figura 2.13. Direcciones IP especiales.

La dirección IP 0.0.0.0 es usada por los hosts cuando están siendo arrancados, pero no se usa después. Las direcciones IP con 0 como número de red se refieren a la red actual. Estas direcciones permiten que las máquinas se refieran a su propia red sin saber su número (pero tiene que saber su clase para saber cuántos 0s hay que incluir). La dirección que consiste solamente en 1s permite la difusión en la red local, por lo común una LAN. Las direcciones con un número de red propio y solamente unos en el campo de host permiten que las máquinas envíen paquetes de difusión a LANs distantes desde cualquier parte de Internet. Por último, todas las direcciones de la forma 127.xx.yy.zz se reservan para direcciones locales de prueba (loopbacks). Los paquetes enviados a esa dirección no se colocan en el cable; se procesan localmente y se tratan como paquetes de entrada. Esto permite que los paquetes se envíen a la red local sin que el transmisor conozca su número.

2.3.4. Subredes

Como hemos visto, todos los hosts de una red deben tener el mismo número de red. Esta propiedad del direccionamiento IP puede causar problemas a medida que crezcan las redes. Por ejemplo, considere una universidad que inició con una red de clase B utilizada por el Depto. De Ciencias de la Computación para las computadoras de su Ethernet. Un año más tarde, el Depto. de Ingeniería Eléctrica deseó conectarse a Internet, por lo que adquirió un repetidor para ampliar la Ethernet CS hasta su edificio. Conforme pasó el tiempo, muchos otros departamentos adquirieron computadoras y rápidamente se alcanzó el límite de cuatro repetidores por Ethernet. Se requirió una organización diferente. Obtener una segunda dirección de red sería difícil debido a que las direcciones de red son escasas y la universidad ya tiene suficientes direcciones para aproximadamente 60,000 hosts. El problema es la regla de que una sola dirección de clase A, B o C haga referencia a una red, no a una colección de LANs. Conforme más y más organizaciones se encontraron en esta situación, se hizo un pequeño cambio al sistema de direccionamiento para manejar tal situación. La solución a este problema es permitir la división de una red en varias partes para uso interno, pero aún actuar como una sola red ante el mundo exterior. En la actualidad, una red típica de un campus podría lucir como la que se muestra en la figura 2.14, con un enrutador principal conectado a un ISP o a una red regional, y numerosas Ethernets dispersas en diferentes

departamentos del campus. Cada una de las Ethernets tiene su propio enrutador conectado al enrutador principal (posiblemente mediante una LAN de red dorsal, pero la naturaleza de la conexión entre enrutadores no tiene relevancia aquí). [13]

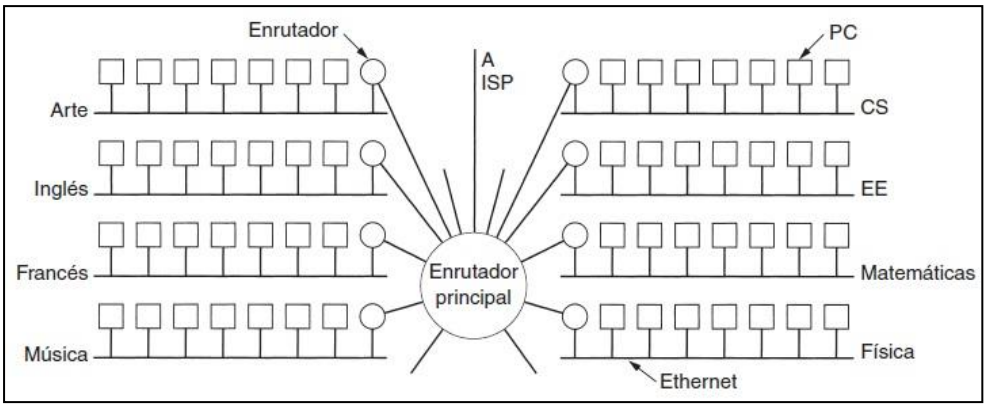


Figura 2.14. Una red de un campus que consiste de LANs para varios departamentos.

En la literatura sobre Internet, a estas partes de la red (en este caso Ethernets) se les llama subredes. Como mencionamos en el capítulo 1, este uso entra en conflicto con la "subred" cuyo significado es el grupo de todos los enrutadores y líneas de comunicación de una red. Esperamos que el contexto deje en claro el significado de que se trata. En esta y en la siguiente sección, la nueva definición será la que utilizaremos de manera exclusiva.

Cuando un paquete entra en el enrutador principal, ¿cómo sabe a cuál subred pasarlo (Ethernet)? Una forma sería tener una tabla con 65,536 entradas en el enrutador principal que indiquen cuál enrutador utilizar para cada host en el campus. Esta idea funcionaría, pero requeriría una tabla muy grande en el enrutador principal y mucho mantenimiento manual conforme se agregaran, movieran o eliminaran hosts.

En su lugar, se inventó un esquema diferente. Básicamente, en lugar de tener una sola dirección de clase B con 14 bits para el número de red y 16 bits para el número de host, algunos bits se eliminan del número de host para crear un número de subred. Por ejemplo, si la universidad tiene 35 departamentos, podría utilizar un número de subred de 6 bits y un número de host de 10 bits, lo que permitiría hasta 64 Ethernets, cada una con un máximo de 1022 hosts (0 y −1 no están disponibles, como se mencionó anteriormente). Esta división podría cambiarse posteriormente en caso de que no fuera correcta. [13]

Para implementar subredes, el enrutador principal necesita una máscara de subred que indique la división entre el número de red + el número de subred y el host, como se muestra en la figura 16. Las máscaras de subred también se pueden escribir en notación decimal con puntos, o agregando a la dirección IP una diagonal seguida del

número de bits usados para los números de red y subred. Para el ejemplo de la figura 2.15, la máscara de subred puede escribirse como 255.255.252.0. Una notación alternativa es /22 para indicar que la máscara de subred tiene una longitud de 22 bits.

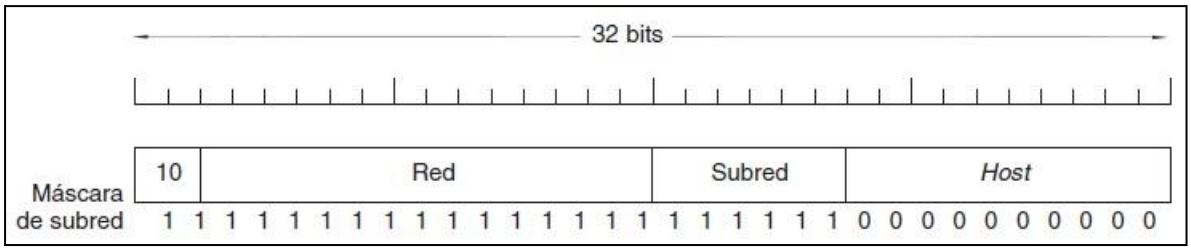


Figura 2.15. Una red de clase B dividida en 64 subredes.

Fuera de la red, la subred no es visible, por lo que la asignación de una subred nueva no requiere comunicación con el ICANN ni la modificación de bases de datos externas. En este ejemplo, la primera subred podría usar direcciones IP a partir de 130.50.4.1, la segunda podría empezar en 130.50.8.1, la tercera podría empezar en 130.50.12.1, etcétera. Para ver por qué las subredes se cuentan en grupos de cuatro, observe que las direcciones binarias correspondientes son como se muestra a continuación:

Subred 1: 10000010 00110010 000001|00 00000001
Subred 2: 10000010 00110010 000010|00 00000001
Subred 3: 10000010 00110010 000011|00 00000001

La barra vertical (|) muestra el límite entre el número de subred y el número de host. A su izquierda se encuentra el número de subred de 6 bits; a su derecha, el número de host de 10 bits. Para ver el funcionamiento de las subredes, es necesario explicar la manera en que se procesan los paquetes IP en un enrutador. Cada enrutador tiene una tabla en la que se lista cierto número de direcciones IP (red, 0) y cierto número de direcciones IP (esta red, host). El primer tipo indica cómo llegar a redes distantes. El segundo tipo indica cómo llegar a redes locales. La interfaz de red a utilizar para alcanzar el destino, así como otra información, está asociada a cada tabla.

Cuando llega un paquete IP, se busca su dirección de destino en la tabla de enrutamiento. Si el paquete es para una red distante, se reenvía al siguiente enrutador de la interfaz dada en la tabla; si es para un host local (por ejemplo, en la LAN del enrutador), se envía directamente al destino. Si la red no está en la tabla, el paquete se reenvía a un enrutador predeterminado con tablas más extensas. Este algoritmo significa que cada enrutador sólo tiene que llevar el registro de otras redes y hosts locales (no de pares red-host), reduciendo en gran medida el tamaño de la tabla de enrutamiento. [13]

Al introducirse subredes, se cambian las tablas de enrutamiento, agregando entradas con forma de (esta red, subred, 0) y (esta red, esta subred, host). Por lo tanto, un enrutador de la subred k sabe cómo llegar a todas las demás subredes y a todos los hosts de la subred k; no tiene que saber los detalles sobre los hosts de otras subredes. De hecho, todo lo que se necesita es hacer que cada enrutador haga un AND booleano con la máscara de subred de la red para deshacerse del número de host y buscar la dirección resultante en sus tablas (tras determinar de qué clase de red se trata).

Por ejemplo, a un paquete dirigido a 130.50.15.6 que llega a un enrutador de la subred 5 se le aplica un AND con la máscara de subred 255.255.252.0/22 para dar la dirección 130.50.12.0. Esta dirección se busca en las tablas de enrutamiento para averiguar la manera de llegar a los hosts de la subred 3. Por lo tanto, la división de redes reduce espacio en la tabla de enrutamiento creando una jerarquía de tres niveles, que consiste en red, subred y host.

2.3.5 Fragmentación de paquetes IP

Un paquete IP teóricamente puede tener un tamaño de hasta 65536 bytes, sin embargo las tecnologías de las capas inferiores imponen un límite al tamaño de los datagramas que pueden ser transmitidos.

Cada red impone un tamaño máximo a sus paquetes. Estos límites tienen varias razones, entre ellas:

- El hardware, por ejemplo, el ancho de una ranura de trasmisión TDM[23].
- El sistema operativo, todos los buffers son de 512 bytes.
- Los protocolos, por ejemplo, la cantidad de bits en el campo de longitud de paquete.
- El cumplimiento de algún estándar.
- Evitar que un paquete ocupe un canal por demasiado tiempo.

Este límite dado por la tecnología de la red se conoce como MTU (Maxímun Transfer Unit), el MTU de Ethernet es 1500 bytes por trama, la de FDDI es 4497 bytes por trama.

Para resolver el problema del cambio de capa de Enlace, y por tanto MTU, en la transmisión de un paquete IP provee un mecanismo de fragmentación. Figura 2.16.

23 TDM es una técnica que permite la transmisión de señales digitales y cuya idea consiste en ocupar un canal de transmisión a partir de distintas fuentes, de esta manera se logra un mejor aprovechamiento del medio de transmisión.

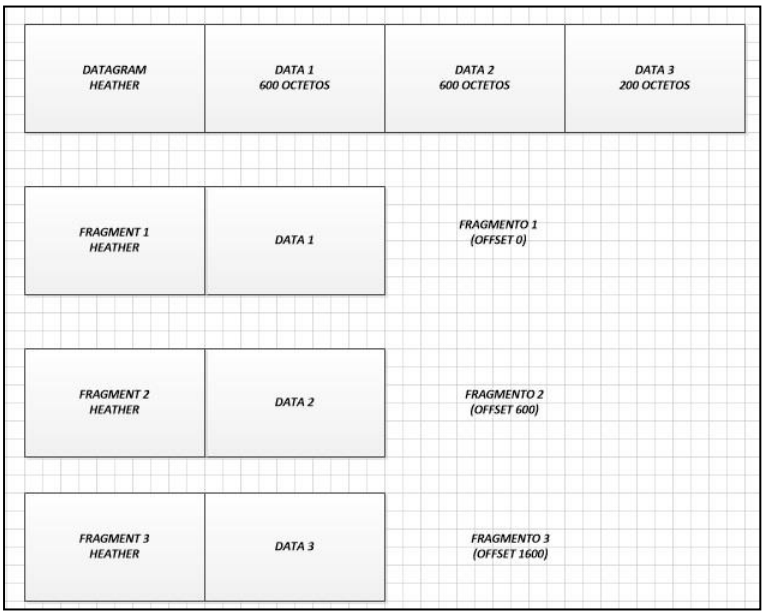


Figura 2.16. Proceso de Fragmentación

2.3.6. Reensamblado de fragmentos

El control de la fragmentación de un Datagrama IP se realiza con los campos de la segunda palabra de su cabecera:

- Identificación: Número de 16 bits que identifica al Datagrama, que permite implementar números de secuencias y que permite reconocer los diferentes fragmentos de un mismo Datagrama, pues todos ellos comparten este número.

- Banderas: Un campo de tres bits donde el primero está reservado. El segundo, llamado bit de No Fragmentación significa: 0 = Puede fragmentarse el Datagrama o 1 = No puede fragmentarse el Datagrama. El tercer bit es llamado más fragmentos y significa: 0 = Único fragmento o Último fragmento, 1 = aún hay más fragmentos. Cuando hay un 0 en más fragmentos, debe evaluarse el campo despliegue. De Fragmento: si este es cero, el datagrama no está fragmentado, si es diferente de cero, el Datagrama es un último fragmento.

- Desplazamiento De Fragmento: A un trozo de datos se le llama Bloque Fragmento. Este campo indica el tamaño del desplazamiento en bloques de fragmento con respecto al Datagrama original, empezando por el cero

2.4. El modelo OSI

El modelo OSI se muestra en la figura 2.17 (sin el medio físico). Este modelo está basado en una propuesta desarrollada por la ISO (Organización Internacional de Estándares) como un primer paso hacia la estandarización internacional de los protocolos utilizados en varias capas (Day y Zimmermann, 1983). Fue revisado en 1995 (Day, 1995). El modelo se llama OSI (Interconexión de Sistemas Abiertos) de ISO porque tiene que ver con la conexión de sistemas abiertos, es decir, sistemas que están abiertos a la comunicación con otros sistemas. Para abreviar, lo llamaremos modelo OSI. [17]

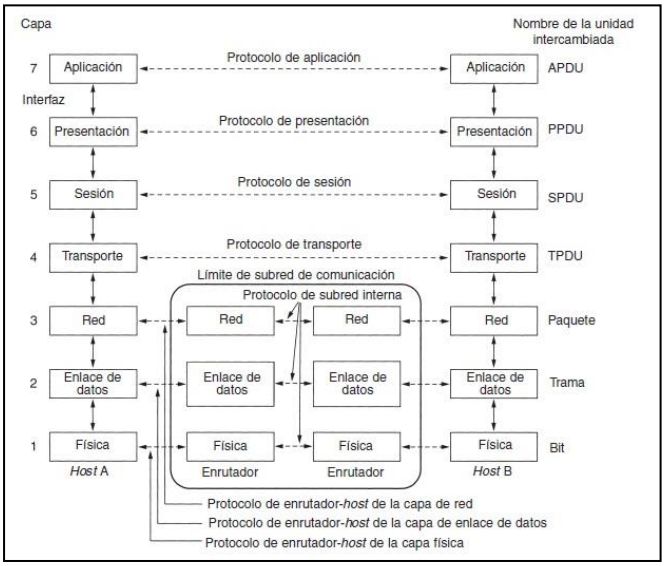


Figura 2.17. El modelo OSI.

El modelo OSI tiene siete capas. Podemos resumir brevemente los principios que se aplicaron para llegar a dichas capas:

- Una capa se debe crear donde se necesite una abstracción diferente.
- Cada capa debe realizar una función bien definida.
- La función de cada capa se debe elegir con la intención de definir protocolos estandarizados internacionalmente.
- Los límites de las capas se deben elegir a fin de minimizar el flujo de información a través de las interfaces.
- La cantidad de capas debe ser suficientemente grande para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

A continuación analizaremos una por una cada capa del modelo, comenzando con la capa inferior. Observe que el modelo OSI no es en sí una arquitectura de red, debido a

que no especifica los servicios y protocolos exactos que se utilizarán en cada capa. Sólo indica lo que debe hacer cada capa. Sin embargo, ISO también ha producido estándares para todas las capas, aunque éstos no son parte del modelo de referencia mismo. Cada uno se ha publicado como un estándar internacional separado.

2.4.1 Capa física

En esta capa se lleva a cabo la transmisión de bits puros a través de un canal de comunicación. Los aspectos del diseño implican asegurarse de que cuando un lado envía un bit 1, éste se reciba en el otro lado como tal, no como bit 0. Las preguntas típicas aquí son: ¿cuántos voltios se deben emplear para representar un 1 y cuántos para representar un 0?, ¿cuántos nanosegundos dura un bit?, ¿la transmisión se debe llevar a cabo en ambas direcciones al mismo tiempo?, ¿cómo se establece la conexión inicial y cómo se finaliza cuando ambos lados terminan?, ¿cuántos pines tiene un conector de red y para qué se utiliza cada uno? Los aspectos de diseño tienen que ver mucho con interfaces mecánicas, eléctricas y de temporización, además del medio físico de transmisión, que está bajo la capa física.

2.4.2 Capa de enlace de datos

La tarea principal de esta capa es transformar un medio de transmisión puro en una línea de comunicación que, al llegar a la capa de red, aparezca libre de errores de transmisión. Logra esta tarea haciendo que el emisor fragmente los datos de entrada en tramas de datos (típicamente, de algunos cientos o miles de bytes) y transmitiendo las tramas de manera secuencial. Si el servicio es confiable, el receptor confirma la recepción correcta de cada trama devolviendo una trama de confirmación de recepción.

Otra cuestión que surge en la capa de enlace de datos (y en la mayoría de las capas superiores) es cómo hacer que un transmisor rápido no sature de datos a un receptor lento. Por lo general se necesita un mecanismo de regulación de tráfico que indique al transmisor cuánto espacio de búfer tiene el receptor en ese momento. Con frecuencia, esta regulación de flujo y el manejo de errores están integrados.

2.4.3. Capa de red

Esta capa controla las operaciones de la subred. Un aspecto clave del diseño es determinar cómo se enrutan los paquetes desde su origen a su destino. Las rutas pueden estar basadas en tablas estáticas (enrutamiento estático) codificadas en la red y que rara vez cambian.

Si hay demasiados paquetes en la subred al mismo tiempo, se interpondrán en el camino unos y otros, lo que provocará que se formen cuellos de botella. La responsabilidad de controlar esta congestión también pertenece a la capa de red, aunque esta responsabilidad también puede ser compartida por la capa de transmisión. De manera más general, la calidad del servicio proporcionado (retardo, tiempo de tránsito, inestabilidad, etcétera) también corresponde a la capa de red. Cuando un paquete tiene que viajar de una red a otra para llegar a su destino, pueden surgir muchos problemas. El direccionamiento utilizado por la segunda red podría ser diferente del de la primera. La segunda podría no aceptar todo el paquete porque es demasiado largo. Los protocolos podrían ser diferentes, etcétera. La capa de red tiene que resolver todos estos problemas para que las redes heterogéneas se interconecten. En las redes de difusión, el problema de enrutamiento es simple, por lo que la capa de red a veces es delgada o, en ocasiones, ni siquiera existe.

2.4.4. Capa de transporte

La función básica de esta capa es aceptar los datos provenientes de las capas superiores, dividirlos en unidades más pequeñas si es necesario, pasar éstas a la capa de red y asegurarse de que todas las piezas lleguen correctamente al otro extremo. Además, todo esto se debe hacer con eficiencia y de manera que aísle a las capas superiores de los cambios inevitables en la tecnología del hardware. [17]

La capa de transporte también determina qué tipo de servicio proporcionar a la capa de sesión y, finalmente, a los usuarios de la red. El tipo de conexión de transporte más popular es un canal punto a punto libre de errores que entrega mensajes o bytes en el orden en que se enviaron. Sin embargo, otros tipos de servicio de transporte posibles son la transportación de mensajes aislados, que no garantiza el orden de entrega, y la difusión de mensajes a múltiples destinos. El tipo de servicio se determina cuando se establece la conexión. (Como observación, es imposible alcanzar un canal libre de errores; lo que se quiere dar a entender con este término es que la tasa de error es tan baja que se puede ignorar en la práctica.). La capa de transporte es una verdadera conexión de extremo a extremo, en toda la ruta desde el origen hasta el destino. En otras palabras, un programa en la máquina de origen lleva a cabo una conversación con un programa similar en la máquina de destino, usando los encabezados de mensaje y los mensajes de control. En las capas inferiores, los protocolos operan entre cada máquina y sus vecinos inmediatos, y no entre las máquinas de los extremos, la de origen y la de destino, las cuales podrían estar separadas por muchos enrutadores. En la figura 18 se muestra la diferencia entre las capas 1 a 3, que están encadenadas, y las capas 4 a 7, que operan de extremo a extremo.

2.4.5. Capa de sesión.

Esta capa permite que los usuarios de máquinas diferentes establezcan sesiones entre ellos. Las sesiones ofrecen varios servicios, como el control de diálogo (dar seguimiento de a quién le toca transmitir), administración de token (que impide que las dos partes traten de realizar la misma operación crítica al mismo tiempo) y sincronización (la adición de puntos de referencia a transmisiones largas para permitirles continuar desde donde se encontraban después de una caída).

2.4.6. Capa de presentación

A diferencia de las capas inferiores, a las que les corresponde principalmente mover bits, a la capa de presentación le corresponde la sintaxis y la semántica de la información transmitida. A fin de que las computadoras con diferentes representaciones de datos se puedan comunicar, las estructuras de datos que se intercambiarán se pueden definir de una manera abstracta, junto con una codificación estándar para su uso "en el cable". La capa de presentación maneja estas estructuras de datos abstractas y permite definir e intercambiar estructuras de datos de un nivel más alto (por ejemplo, registros bancarios).

2.4.7. Capa de aplicación

Esta capa contiene varios protocolos que los usuarios requieren con frecuencia. Un protocolo de aplicación de amplio uso es HTTP (Protocolo de Transferencia de Hipertexto), que es la base de World Wide Web. Cuando un navegador desea una página Web, utiliza este protocolo para enviar al servidor el nombre de dicha página. A continuación, el servidor devuelve la página. Otros protocolos de aplicación se utilizan para la transferencia de archivos, correo electrónico y noticias en la red. [17]

2.5. Modelo TCP/IP

ARPANET fue una red de investigación respaldada por el DoD (Departamento de Defensa de Estados Unidos). Con el tiempo, conectó cientos de universidades e instalaciones gubernamentales mediante líneas telefónicas alquiladas. Posteriormente, cuando se agregaron redes satelitales y de radio, los protocolos existentes tuvieron problemas para interactuar con ellas, por lo que se necesitaba una nueva arquitectura de referencia. De este modo, la capacidad para conectar múltiples redes en una manera sólida fue una de las principales metas de diseño desde sus inicios. Más tarde, esta arquitectura se llegó a conocer como el modelo de referencia TCP/IP, de acuerdo con sus dos protocolos primarios. Ante el temor del DoD de que algunos de sus valiosos hosts, enrutadores y puertas de enlace de interredes explotaran en un instante, otro

objetivo fue que la red pudiera sobrevivir a la pérdida de hardware de la subred, sin que las conversaciones existentes se interrumpieran. En otras palabras, el DoD quería que las conexiones se mantuvieran intactas en tanto las máquinas de origen y destino estuvieran funcionando, aunque algunas de las máquinas o líneas de transmisión intermedias quedaran fuera de operación repentinamente. Además, se necesitaba una arquitectura flexible debido a que se preveían aplicaciones con requerimientos divergentes, desde transferencia de archivos a transmisión de palabras en tiempo real.

2.5.1. Capa de interred

Todos estos requerimientos condujeron a la elección de una red de conmutación de paquetes basada en una capa de interred no orientada a la conexión. Esta capa, llamada capa de interred, es la pieza clave que mantiene unida a la arquitectura. Su trabajo es permitir que los hosts inyecten paquetes dentro de cualquier red y que éstos viajen a su destino de manera independiente (podría ser en una red diferente). Tal vez lleguen en un orden diferente al que fueron enviados, en cuyo caso las capas más altas deberán ordenarlos, si se desea una entrega ordenada. Observe que aquí el concepto "interred" se utiliza en un sentido genérico, aun cuando esta capa se presente en Internet.

Aquí la analogía es con el sistema de correo tradicional. Una persona puede depositar una secuencia de cartas internacionales en un buzón y, con un poco de suerte, la mayoría de ellas se entregará en la dirección correcta del país de destino. Es probable que durante el trayecto, las cartas viajen a través de una o más puertas de enlace de correo internacional, pero esto es transparente para los usuarios. Además, para los usuarios también es transparente el hecho de que cada país (es decir, cada red) tiene sus propios timbres postales, tamaños preferidos de sobre y reglas de entrega.

La capa de interred define un paquete de formato y protocolo oficial llamado IP (Protocolo de Internet). El trabajo de la capa de interred es entregar paquetes IP al destinatario. Aquí, el enrutamiento de paquetes es claramente el aspecto principal, con el propósito de evitar la congestión. Por estas razones es razonable decir que la capa de interred del modelo TCP/IP es similar en funcionalidad a la capa de red del modelo OSI. La figura 2.18 muestra esta correspondencia.

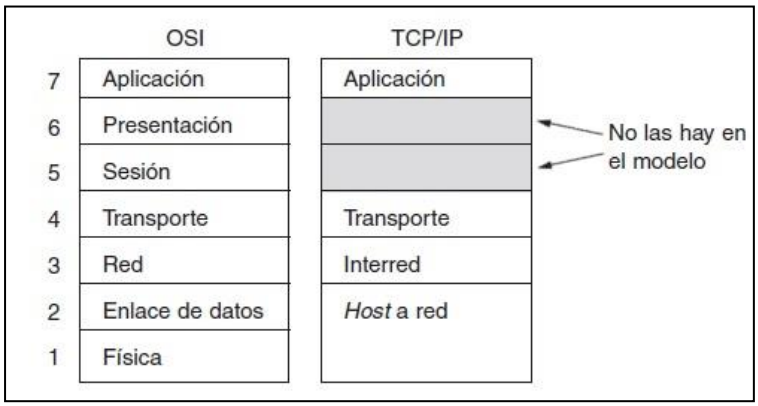


Figura 2.18. El modelo TCP/IP.

2.5.2. Capa de transporte

La capa que está arriba de la capa de interred en el modelo TCP/IP se llama capa de transporte. Está diseñada para permitir que las entidades iguales en los hosts de origen y destino puedan llevar a cabo una conversación, tal como lo hace la capa de transporte OSI. Aquí se han definido dos protocolos de transporte de extremo a extremo. El primero, TCP (Protocolo de Control de Transmisión), es un protocolo confiable, orientado a la conexión, que permite que un flujo de bytes que se origina en una máquina se entregue sin errores en cualquier otra máquina en la interred. Divide el flujo de bytes entrantes en mensajes discretos y pasa cada uno de ellos a la capa de interred. En el destino, el proceso TCP receptor reensambla en el flujo de salida los mensajes recibidos. TCP también maneja el control de flujo para asegurarse de que un emisor rápido no sature a un receptor lento con más mensajes de los que puede manejar.

El segundo protocolo de esta capa, UDP (Protocolo de Datagrama de Usuario), es un protocolo no confiable y no orientado a la conexión para aplicaciones que no desean la secuenciación o el control de flujo de TCP y que desean proporcionar el suyo. También tiene un amplio uso en consultas únicas de solicitud-respuesta de tipo cliente-servidor en un solo envío, así como aplicaciones en las que la entrega puntual es más importante que la precisa, como en la transmisión de voz o vídeo. La relación de IP, TCP y UDP se muestra en la figura 2.19. Puesto que el modelo se desarrolló, se ha implementado IP en muchas otras redes.

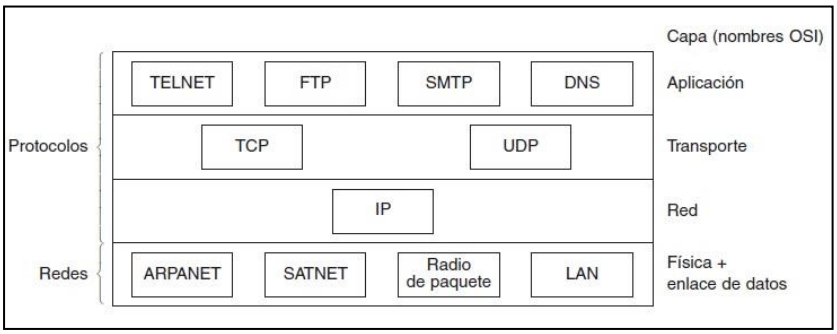


Figura 2.19. Protocolos y redes en el modelo TCP/IP inicialmente.

2.5.3. Capa de aplicación

El modelo TCP/IP no tiene capas de sesión ni de presentación. No se han necesitado, por lo que no se incluyen. La experiencia con el modelo OSI ha probado que este punto de vista es correcto: son de poco uso para la mayoría de las aplicaciones. Arriba de la capa de transporte está la capa de aplicación. Contiene todos los protocolos de nivel más alto. Los primeros incluyeron una terminal virtual (TELNET), transferencia de archivos (FTP) y correo electrónico (SMTP), como se muestra en la figura 20. El protocolo de terminal virtual permite que un usuario en una máquina se registre en una máquina remota y trabaje ahí. El protocolo de transferencia de archivos proporciona una manera de mover con eficiencia datos de una máquina a otra. El correo electrónico era originalmente sólo un tipo de transferencia de archivos, pero más tarde se desarrolló un protocolo especializado (SMTP) para él. Con el tiempo, se han agregado muchos otros protocolos: DNS (Sistema de Nombres de Dominio) para la resolución de nombres de host en sus direcciones de red; NNTP, para transportar los artículos de noticias de USENET; HTTP, para las páginas de World Wide Web, y muchos otros.

2.5.4. Capa host a red

Debajo de la capa de interred hay un gran vacío. El modelo de referencia TCP/IP en realidad no dice mucho acerca de lo que pasa aquí, excepto que puntualiza que el host se tiene que conectar a la red mediante el mismo protocolo para que le puedan enviar paquetes IP. Este protocolo no está definido y varía de un host a otro y de una red a otra. Este tema rara vez se trata en libros y artículos sobre TCP/IP.

2.6. Comparación entre los modelos OSI y TCP/IP

Los modelos OSI y TCP/IP tienen mucho en común. Los dos se basan en el concepto de una pila de protocolos independientes. Asimismo, la funcionalidad de las capas es muy parecida. Por ejemplo, en ambos modelos las capas que están arriba de, incluyendo a, la capa de transporte están ahí para proporcionar un servicio de transporte

independiente de extremo a extremo a los procesos que desean comunicarse. Estas capas forman el proveedor de transporte. De nuevo, en ambos modelos, las capas que están arriba de la de transporte son usuarias orientadas a la aplicación del servicio de transporte. [17]

Tres conceptos son básicos para el modelo OSI:

- Servicios.
- Interfaces.
- Protocolos.

Probablemente la contribución más grande del modelo OSI es que hace explícita la distinción entre estos tres conceptos. Cada capa desempeña algunos servicios para la capa que está arriba de ella. La definición de servicio indica qué hace la capa, no la forma en que la entidad superior tiene acceso a ella, o cómo funciona dicha capa. Define el aspecto semántico de la capa.

La interfaz de una capa indica a los procesos que están sobre ella cómo accederla. Especifica cuáles son los parámetros y qué resultados se esperan. Incluso, no dice nada sobre cómo funciona internamente la capa.

Por último, una capa es quien debe decidir qué protocolos de iguales utilizar. Puede usar cualesquier protocolos que desee, en tanto consiga que se haga el trabajo (es decir, proporcione los servicios ofrecidos). También puede cambiarlos cuando desee sin afectar el software de las capas superiores. Estas ideas encajan muy bien con las ideas modernas sobre la programación orientada a objetos. Un objeto, como una capa, cuenta con un conjunto de métodos (operaciones) que pueden ser invocados por procesos que no estén en dicho objeto. La semántica de estos métodos define el conjunto de servicios que ofrece el objeto. Los parámetros y resultados de los métodos forman la interfaz del objeto. El código interno del objeto es su protocolo y no es visible o no tiene importancia fuera del objeto. Originalmente, el modelo TCP/IP no distinguía entre servicio, interfaz y protocolo, aunque las personas han tratado de readaptarlo con el propósito de hacerlo más parecido al OSI. Por ejemplo, los únicos servicios ofrecidos realmente por la capa de interred son SEND IP PACKET y RECEIVE IP PACKET. [17]

Como consecuencia, los protocolos del modelo OSI están mejor ocultos que los del modelo TCPI/IP y se pueden reemplazar fácilmente conforme cambia la tecnología. La facilidad para realizar tales cambios es uno de los objetivos principales de tener protocolos en capas. El modelo de referencia OSI se vislumbró antes de que se inventaran los protocolos correspondientes. Esta clasificación significa que el modelo no estaba diseñado para un conjunto particular de protocolos, un hecho que lo hizo general. Una deficiencia de esta clasificación es que los diseñadores no tenían mucha experiencia con el asunto y no tenían una idea concreta de qué funcionalidad poner en

qué capa. Por ejemplo, originalmente la capa de enlace de datos sólo trataba con redes de punto a punto. Cuando llegaron las redes de difusión, se tuvo que extender una nueva subcapa en el modelo. Cuando las personas empezaron a construir redes reales utilizando el modelo OSI y los protocolos existentes, se descubrió que estas redes no coincidían con las especificaciones de los servicios solicitados (maravilla de maravillas), por lo que se tuvieron que integrar subcapas convergentes en el modelo para proporcionar un espacio para documentar las diferencias. Por último, el comité esperaba en un principio que cada país tuviera una red, controlada por el gobierno y que utilizara los protocolos OSI, pero nunca pensaron en la interconectividad de redes. Para no hacer tan larga la historia, las cosas no sucedieron como se esperaba.

Con TCP/IP sucedió lo contrario: los protocolos llegaron primero y el modelo fue en realidad una descripción de los protocolos existentes. No había problemas para ajustar los protocolos al modelo. Encajaban a la perfección. El único problema era que el modelo no aceptaba otras pilas de protocolos. Como consecuencia, no era útil para describir otras redes que no fueran TCP/IP. Volviendo de los asuntos filosóficos a los más específicos, una diferencia patente entre los dos modelos es el número de capas: el modelo OSI tiene siete y el TCP/IP sólo cuatro. Los dos tienen capas de (inter)red, transporte y aplicación, pero las otras capas son diferentes. Otra diferencia está en el área de la comunicación orientada a la conexión comparada con la no orientada a la conexión. El modelo OSI soporta ambas comunicaciones en la capa de red, pero sólo la de comunicación orientada a la conexión en la capa de transporte, donde es importante (porque el servicio de transporte es transparente para los usuarios). El modelo TCP/IP sólo tiene un modo en la capa de red (no orientado a la conexión) pero soporta ambos modos en la capa de transporte, lo que da a los usuarios la oportunidad de elegir. Esta elección es importante especialmente para protocolos sencillos de solicitud-respuesta.

2.7 Fases de implantación [18]

No es necesario realizar toda la implantación de IP en una determinada arquitectura de red. Para empezar, IP 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 IP 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 IP.

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 IP 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. IP 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.

CAPÍTULO II.

3. Ventajas y Desventajas de tecnologías SDH e IP

3.1. Descripción del Capitulo

En este capítulo abordaremos las ventajas y desventajas que presentan cada una de las tecnologías SDH e IP como red de transporte.

3.2. Ventajas y Desventajas de tecnología SDH[18]

Actualmente estamos viviendo una gran explosión en la demanda de servicios sofisticados de Telecomunicaciones, servicios tales como video-conferencias, acceso a bases de datos remotas y transferencia de archivos multimedia, por lo que se requiere de una red que tenga la habilidad de ser lo suficientemente flexible para tener virtualmente un ancho de banda ilimitado. Por lo tanto surge la necesidad de definir una tecnología internacional de comunicaciones que permita manejar y supervisar con facilidad esta capacidad de transporte, cada tecnología que se utiliza para transportar datos a nivel mundial puede tener un sin números de ventajas al igual que carencias a la hora de adaptarse a nuevas necesidades o a nuevos requerimientos dentro de una red, en este caso dentro de la red de transporte. A continuación detallaremos las utilidades y obstáculos que presentan cada una de las tecnologias que hemos estado abordando, SDH e IP

3.2.1. Ventajas

- Altas velocidades de transmisión: Los modernos sistemas SDH logran velocidades de 10 Gbit/s. SDH es la tecnología más adecuada para los "backbones", que son realmente las superautopistas de las redes de telecomunicaciones actuales.

- Función simplificada de inserción/extracción: Comparado con los sistemas PDH tradicionales, ahora es mucho más fácil extraer o insertar canales de menor velocidad en las señales compuestas SDH de alta velocidad. Ya no hace falta demultiplexar y volver a multiplexar la estructura plesiócrona, procedimiento que en el mejor de los casos era complejo y costoso. Esto se debe a que en la

jerarquía SDH todos los canales están perfectamente identificados por medio de una especie de "etiquetas" que hacen posible conocer exactamente la posición de los canales individuales.

- Alta disponibilidad y grandes posibilidades de ampliación: La tecnología SDH permite a los proveedores de redes reaccionar rápida y fácilmente frente a las demandas de sus clientes. Por ejemplo, conmutar las líneas alquiladas es sólo cuestión de minutos. Empleando un sistema de gestión de redes de telecomunicaciones, el proveedor de la red puede usar elementos de redes estándar controlados y monitorizados desde un lugar centralizado.

- Fiabilidad: Las modernas redes SDH incluyen varios mecanismos automáticos de protección y recuperación ante posibles fallos del sistema. Un problema en un enlace o en un elemento de la red no provoca el colapso de toda la red, lo que podría ser un desastre financiero para el proveedor. Estos circuitos de protección también se controlan mediante un sistema de gestión.

- Plataforma a prueba de futuro: Hoy día, SDH es la plataforma ideal para multitud de servicios, desde la telefonía tradicional, las redes RDSI o la telefonía móvil hasta las comunicaciones de datos (LAN24, WAN25, etc.) y es igualmente adecuada para los servicios más recientes, como el video bajo demanda (VOD) o la transmisión de video digital vía ATM.

- Interconexión: Con SDH es mucho más fácil crear pasarelas entre los distintos proveedores de redes y hacia los sistemas SONET. Las interfaces SDH están normalizadas, lo que simplifica las combinaciones de elementos de redes de diferentes fabricantes. La consecuencia inmediata es que los gastos en equipamiento son menores en los sistemas SDH que en los sistemas PDH. El motor que genera toda esta evolución es la creciente demanda de más ancho de banda, mejor calidad de servicio y mayor fiabilidad, junto a la necesidad de reducir costos manteniendo la competitividad.

- Asegura un alto grado de protección: tiempos de restauración de servicio inferiores a 50 ms.

---

24 LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios).
25 WAN es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes.

- Garantiza la calidad de servicio, mediante establecimiento de circuitos.
- Supervisión de calidad, operación y mantenimiento completos basados en TDM.
- El proceso de multiplexación es mucho más directo.
- La utilización de punteros permite una localización sencilla y rápida de las señales tributarias de la información.
- El procesamiento de la señal se lleva a cabo a nivel de STM-1.
- Las señales de velocidades superiores son síncronas entre sí y están en fase por ser generadas localmente por cada nodo de la red.
- Las tramas tributarias de las señales de línea pueden ser subdivididas para acomodar cargas pre síncronas, tráfico ATM o unidades de menor orden. Esto supone mezclar tráfico de distinto tipo dando lugar a redes flexibles.
- Compatibilidad eléctrica y óptica entre los equipos de los distintos proveedores gracias a los estándares internacionales sobre interfaces eléctricos y ópticos.
- Un STM1 tiene la capacidad de agrupar varios E1 y T1 de forma multiplexada, es decir, se universaliza las velocidades ocupando los VC correspondientes, la capacidad del STM1 es suficiente.

3.2.2. Desventajas

Las actuales redes de transporte SDH tienen ciertas limitaciones a la hora de afrontar el crecimiento de las redes metropolitanas y estas carencias empujan hacia una futura migración de tecnología dentro de la red de transporte. Dentro de las desventajas de esta tecnología esta:

- El coste de los equipos es mucho mayor que para redes Ethernet.
- Altamente ineficiente para el transporte de datos. Al haber sido diseñadas inicialmente para tráfico de voz TDM, estas redes no están optimizadas para tráfico LAN, ya que el ancho de banda empleado es fijo Y de granuladidad gruesa, por lo que no se adapta a los requerimientos de las aplicaciones.
- Restringido a topología en anillo.

- Se pueden aprovechar los mecanismos de multiplexación estadística montando ATM sobre SDH/SONET, pero se trata de una solución de coste económico elevado.

- Deja sin utilizar el 50% del ancho de banda, ya que una de las fibras debe estar libre para entrar en servicio cuando se produzca el fallo y suministrar el respaldo correspondiente.

- Necesidad de una gestión fácil en la Oficina Central. (CO).

- Siguen surgiendo problemas sobre todo cuando se combinan elementos de redes de distintos fabricantes

- Los problemas de transmisión en las pasarelas que conectan redes de operadores.

- Necesidad de sincronismo entre los nodos de la red SDH, se requiere que todos los servicios trabajen bajo una misma referencia de temporización.
- La estructura de trama de las centrales hecha por entrelazamiento de octetos a 64 Kbits/s. es síncrona, por tanto el empleo de la justificación para adoptar temporización se vuelve innecesario.

- El entrelazamiento de bits hace que canales a 64 Kbits/s. pertenecientes a un tramo de trafico solo se puedan bifurcar hasta que se demultiplexa a nivel de multiplex primario.

- Los canales de n 64Kbits/s que no se puedan incluir bajo el multiplex primario no se pueden tramitar de ninguna otra forma por la red.

- La información de mantenimiento no está asociada a vías completas de tráfico, sino a enlaces individuales, por lo cual el procedimiento de mantenimiento para una vía completa es complicado

- Necesita sincronismo entre los nodos de la red, requiere que todos los servicios trabajen bajo una misma referencia de temporización.

- Se pierde eficiencia, ya que, el número de bytes destinados a la cabecera de sección es demasiado grande.

3.3. Ventajas y Desventajas de tecnología IP. [16]

La creciente necesidad de reducir costes, aumentar la productividad, soportar más aplicaciones y elevar la seguridad está jugando fuerte a favor del cambio corporativo hacia esta nueva tecnología. A continuación se presentan las ventajas y desventajas de la tecnología IP.

3.3.1. Ventajas

El principal propósito del Proveedor de Servicios es ofrecer distintos tipos de Servicios y Seguridad para las conexiones y aplicaciones teniendo en cuenta los siguientes parámetros: disponibilidad de Servicios, garantía del tiempo de funcionamiento y latencia, garantía en cada tipo de servicio (retardo, variación de retardo, tasa de perdidas, etc.), soporte al servicio. Dentro de las ventajas podemos mencionar:

- Está diseñado para enrutar y tiene un grado muy elevado de fiabilidad, además es compatible con las herramientas estándar para analizar el funcionamiento de la red.
- Enorme disponibilidad de aplicaciones y servicios adaptables a la mayoría de las necesidades y expectativas
- Ambiente único de operación y administración.
- Aplicaciones que generan ingresos a los clientes.
- Facilidades para el intercambio de información en cualquier nivel de la pirámide.
- Bajos costos de adquisición de aplicaciones y servicios.
- Absorción de la cultura IP desde la oficina, centros de educación, intercambio social, puntos de servicios.
- Convergencia de Servicios (Voz, Datos y Video) utilizando la concentración de diversas tecnologías de acceso que utilizan los usuarios.
- Tipos de acceso que podría ofrecer un Proveedor de Servicios:

- ✓ ADSL con Backups RDSI 128K (sobre líneas Analógicas).
- ✓ Líneas Dedicadas.
- ✓ Líneas Dedicadas con Backups RDSI[26] 128K, 256K.
- ✓ Líneas Dedicadas con Backups ADSL[27].
- ✓ RDSI enrutada 128k.
- ✓ SDSL.
- ✓ SDSL con Backups RDSI 128k, 256K.
- ✓ Líneas Dedicadas con Backup SDSL.
- ✓ SDSL con Backup ADSL.

- Unificación de Servicios (Ahorro en Costos).

- Se puede reconfigurar con facilidad para suprimir o introducir nuevos usuarios y/o servicios adicionales utilizando un punto a la nube (Point-to-Cloud), concepto en el que sólo se configurará este nuevo punto con la gestión y procesos del Proveedor de Servicios y no habrá necesidad de reconfigurar toda la red como es el caso de redes basadas en ATM o Frame Relay (Principio de Escalabilidad de las Redes actuales).

- Gran flexibilidad al poder conectar cualquier punto de una VPN con quien desee, utilizando el mejor camino entre cada punto combinando los beneficios de la transmisión de datos entre dos puntos cualquiera (sin conexión) y de la transmisión con conexión punto a punto eliminando sus inconvenientes.

- Los LSPs pueden ser reemplazados para proporcionar QoS, definiendo grupos de usuarios privados específicos y garantizando los SLAs comprometidos, utilizando definición de Políticas centralizadas de Seguridad y Políticas de Priorización a medida, donde el tráfico que más interesa será priorizado por encima de los servicios para mejorar la eficiencia en las comunicaciones. Así entonces, se utilizan decisiones de prioridad para Recursos disponibles y Flujo de tráfico (Traffic Trunk).

- Se enruta el tráfico basado en restricciones CSPF (Constrained Shortest Path First) y se utilizan ER-LSPs para pasarlo, así el camino puede obtener optimización de la ruta y/o puentear un enlace que ha fallado.

- En IP, la QoS está soportada mediante etiquetas que permiten a los conmutadores de la red identificar los requisitos de cada paquete y darles la prioridad adecuada, así por ejemplo, los requisitos de la empresa Mexicana

26 RDSI red que procede por evolución de la Red Digital Integrada y que facilita conexiones digitales extremo a extremo para proporcionar una amplia gama de servicios, tanto de voz como de otros tipos.
27 ADSL Línea digital de banda ancha con gran capacidad para la transmisión de datos a través de la red de telefonía básica.

Alestra – AT&T atiende cuatro (4) tipos de QoS: Para tráfico prioritario del cliente, tiempo real para video y Voz sobre IP, para paquetes de datos, y para bases de datos, con esto el cliente tiene garantizado el Ancho de Banda que contrató y puede monitorear todas sus aplicaciones.

- Las etiquetas añadidas a los paquetes IP identifican la ruta que se debe seguir y evitan tener que comprobar las tablas en cada paso.

- Logra el mismo nivel de seguridad que el tunneling IP sobre ATM o Frame Relay (VPNs) y es totalmente compatible con procedimiento de seguridad avanzada como IPSec para aumentar la seguridad del Cliente. No necesita superposición al mantener una separación estricta entre cada VPN[28] y asegura que cada paquete IP del cliente se coloca correctamente en la red.

- Se puede utilizar el sistema de reservas de tráfico por medio de RSVP (Reserv Service Virtual Path) dentro de IP, donde el protocolo LDP asociará etiquetas a aquellos flujos que tienen reserva.

- Con el fin de ofrecer Calidad de Servicio (QoS), el proveedor monitoriza constantemente el tráfico en la red evitando que sobrepase su límite, clasifica el tráfico, configura las colas de salida asignándole a cada una un porcentaje de memoria que el enrutador de acceso soporta, delimitando así el tamaño de la cola para cada clase.

- Es una tecnología escalable, gracias a la estructura de la pila de etiquetas MPLS es fácil construir jerarquías de dominios MPLS por lo que se puede pasar de ámbitos más reducidos a ámbitos más globales de forma casi transparente.

- Permite aplicar técnicas de ingeniería de tráfico con lo que la red deja de ser un simple elemento físico de transporte de información y se vuelve mucho más versátil.

- Realiza una única clasificación de los paquetes entrantes al dominio MPLS por lo que éste proceso se reduce enormemente con respecto a tecnologías como IP.

28 VPN es una tecnología de red que se utiliza para conectar una o más computadoras a una red privada utilizando Internet.

3.3.2. Desventaja

- Es más difícil de configurar y de mantener.
- Es algo más lento en redes con un volumen de tráfico medio bajo. puede ser más rápido en redes con un volumen de tráfico grande donde haya que enrutar un gran número de tramas.
- Se utiliza tanto en redes empresariales como por ejemplo en campus universitarios o en complejos empresariales, en donde utilizan muchos enrutadores y conexiones a mainframe o a ordenadores UNIX, como así también en redes pequeñas o domésticas, y hasta en teléfonos móviles y en domótica.
- Obliga a depender de servicios que redirigen un host a una IP.
- En primer lugar, uno de los argumentos esgrimidos a favor de desarrollar MPLS, el incremento en la velocidad de proceso en los dispositivos de encaminamiento, ha declinado con la aparición de nuevos equipos más rápidos y potentes, como los denominados "Gigabit routers".
- La Internet actual se caracteriza por poseer un elevado grado de fiabilidad, derivado de la naturaleza sin conexión del protocolo IP. Por otra parte, los protocolos de encaminamiento dinámico han sido diseñados para reaccionar frente a los potenciales fallos modificando las rutas seguidas por lo paquetes. Sin embargo, el esquema MPLS es orientado a la conexión, lo que implica una mayor vulnerabilidad en situaciones de fallo. Por esta razón, resulta conveniente introducir mecanismos de recuperación de faltas asociadas a la arquitectura MPLS: notificación a los dispositivos de encaminamiento afectados, búsqueda de rutas alternativas, desvío del tráfico a las mismas, etc.
- Si bien la posibilidad de apilar múltiples etiquetas aporta beneficios indudables, el incremento de la proporción de cabecera transportada contribuye a reducir el rendimiento de la red.
- Identificar mediante una etiqueta la calidad de servicio deseada no implica que esta solicitud se satisfaga. Es imprescindible que las tecnologías de red subyacentes provean los mecanismos necesarios para garantizar dicha calidad.
- IP está limitado al ámbito de conectividad de la Red del proveedor de Servicios.

3.4. Ventajas con Respecto a Otras Tecnologías [16]

- IP es un esquema de reenvío que es independiente tanto de la tecnología de nivel de red que esté sobre él, como de la de enlace que este por debajo. Ésto

posibilita que se puedan aprovechar las tecnologías existentes mientras se migra a otras más modernas, facilitando así la recuperación de las inversiones en infraestructura de red.

- Es una tecnología escalable, gracias a la estructura de la pila de etiquetas IP es fácil construir jerarquías de dominios IP por lo que se puede pasar de ámbitos más reducidos a ámbitos más globales de forma casi transparente.

- Permite usar cualquier protocolo de encaminamiento tradicional o de última generación.

- Permite usar cualquier protocolo de distribución tradicional o de última generación.

- Soporta el modelo de servicios diferenciados del IETF.

- Permite aplicar técnicas de ingeniería de tráfico con lo que la red deja de ser un simple elemento físico de transporte de información y se vuelve mucho más versátil.

- Realiza una única clasificación de los paquetes entrantes al dominio IP por lo que éste proceso se reduce enormemente con respecto a otras tecnologías.

- Proporciona una conmutación basada en etiquetas que es muy rápida y eficiente.

3.5. Ventajas sobre la Prestación de IP en Servicios Multimedia.

En los últimos años una de las grandes limitantes en las empresas ha sido la comunicación, debido a que si se deseaba tener diferentes servicios como es telefonía, transmisión de datos y videoconferencia, era necesario tener un proveedor para cada tipo de servicio, es decir tener en la empresa 3 proveedores diferentes ofreciendo diferentes productos conllevaba a un gasto múltiple y poco rentable.

Cosa contraria se observa hoy en día, ya que los proveedores de servicios están ofreciendo sobre el mismo canal servicios como datos, servicios de voz y conexión a Internet, este paquete de servicios recibe el nombre de Convergencia y donde se tiene como principal característica Calidad del Servicio, Priorización y Anchos de Banda garantizados para cada uno de los servicios que se presta en la red.

Las empresas de hoy en día se preocupan por contar con una infraestructura escalable, de gran flexibilidad, que les permita conectarse con quien deseen (entre empresas,

sucursales, clientes y proveedores) con una excelente calidad, entre estos servicios encontramos:

- Videoconferencia.
- Transmisión de datos a altas velocidades.
- Telefonía.
- Transacciones Electrónicas.

Cuando un proveedor desea cumplir con todas las características anteriormente nombradas se hace necesario que se trabaje sobre redes MPLS basadas en IP que garanticen la seguridad, confiabilidad y Calidad de Servicio (QoS). Las plataformas con tecnologías MPLS permiten integrar todos los servicios en un mismo canal incrementando la capacidad de interconexión haciéndola más fácil y flexible

CAPÍTULO III.

4. Implementación.

4.1. Descripción del Capítulo

En este capítulo, se comienza con una breve caracterización de los servicios de telecomunicaciones que se pueden implementar con la red de transporte mixto, las redes que les dan soporte. Se continúa con una pequeña descripción del equipamiento a utilizar, diseño, construcción y configuración de las maquetas y determinar cuál sería la mejor configuración de la maqueta.

4.2. 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 que pueden soportar estas tecnologías mixtas (SDH-IP) son muy variados como por ejemplo LTE, Nodos B, internet, servicios privados, telefonía fija etc.

Con la llegada de 4G, a lo que se podría definir como "all-IP" se busca un sistema que permita conjugar una capacidad multimedia con una movilidad plena.

Con LTE se introduce una gran variedad de novedades con los anteriores estándares, pero la mayor novedad es que por primera vez, todos los servicios, incluida la voz, sean soportados por el protocolo IP. Las velocidades que se pueden llegar a conseguir en la interfaz radio con LTE también aumentan respecto a la última generación, llegando a un rango de 100 Mb/s y 1 Gb/s.

El nodo b realiza las mismas funciones que las estaciones base de GSM, dan cobertura radioeléctrica y se comunican directamente con los terminales, cada nodo b está controlado por un único RNC, el cual controla un número determinado de nodos b. En UMTS, un terminal puede comunicarse simultáneamente con varios nodos B. La RNC29 combina/selecciona las señales que recibe del móvil a través de varios Nodos B

29 RNC Controlador de la red radio es un elemento de red de alta jerarquía de la red de acceso de la tecnología UMTS, responsable del control de los nodos b que se conectan a ella

obteniéndose una ganancia en la calidad de la comunicación. (Macro diversidad en Recepción). En la figura 4.2 podemos ver en donde se encuentra ubicado el nodo b.

Internet: Para enlazar al suscriptor a Internet, la línea de acceso del cliente se conecta a un DSLAM (Digital Subscriber Line Access Multiplexer). 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 4.1 muestra el esquema de conexión.

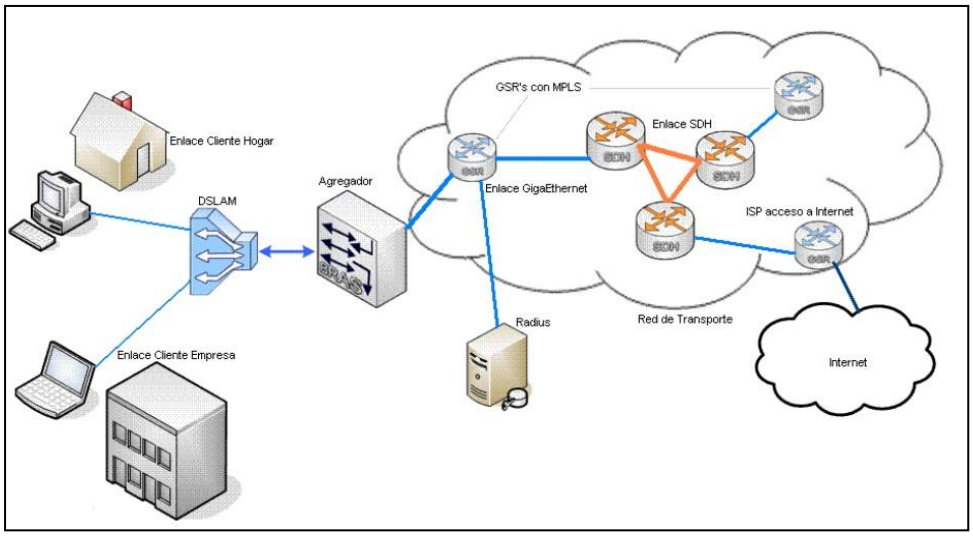


Figura 4.1.: Esquema de conexión a Internet

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. Los dispositivos involucrados en esta configuración, son Switchs Ethernet y nuevamente SDH. El esquema resumido de la red, se muestra en la Figura 4.2.

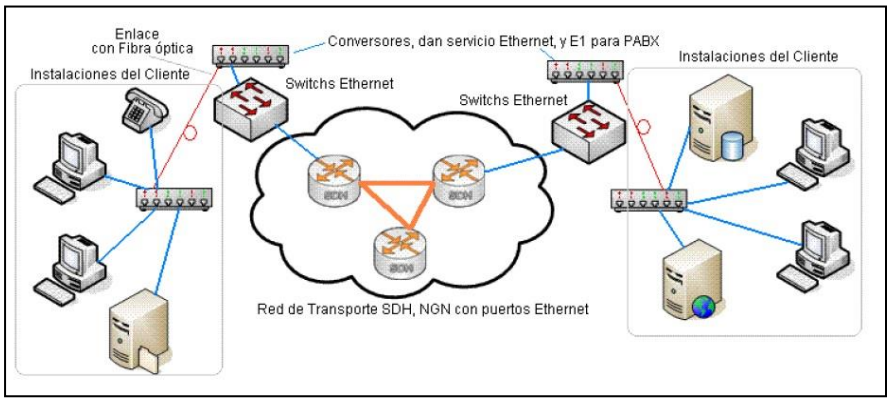


Figura 4.2: Esquema de red con servicios a empresas

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 más 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 (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.

4.3. Maqueta.

4.3.1. Propuesta de Topología.

El objetivo de esta topología, es ver el tipo de configuración en los equipos que se requiere para transportar paquetes de datos en una red mixta con tecnología SDH-IP. También se podría aplicar para ver los procedimientos y requisitos al momento de migrar hacia una red full IP. Las pruebas utilizan equipos de transporte marca Coriant-Siemens Hit7020, equipos ECI-BG20 y equipo IP CISCO ASR 901, para el instrumento de medición se contará con equipos ANT-5 JDSU o ANT-20 para generar las tramas de prueba o utilización básica de un par de Laptops con pruebas de conectividad mediante PING extendido.

También se utilizará medición del medio de transporte físico en este caso Fibra Óptica por medio de un equipos Optical Time Domain Reflectometer (OTDR, por sus silabas en inglés), para determinar las atenuaciones que deban considerarse con la distancia del medio de transporte físico (en este caso 3 Km de FO).

La topología que utilizaremos para la configuración de nuestra maqueta para esta tesis será de tipo lineal, dicha topología nos permitirá demostrar de una manera más detallada y concisa el tipo de configuración que requiere cada equipo en una red de

transporte que integrara tecnología mixta SDH-IP, en la figura 5 se ve la topología a utilizar.

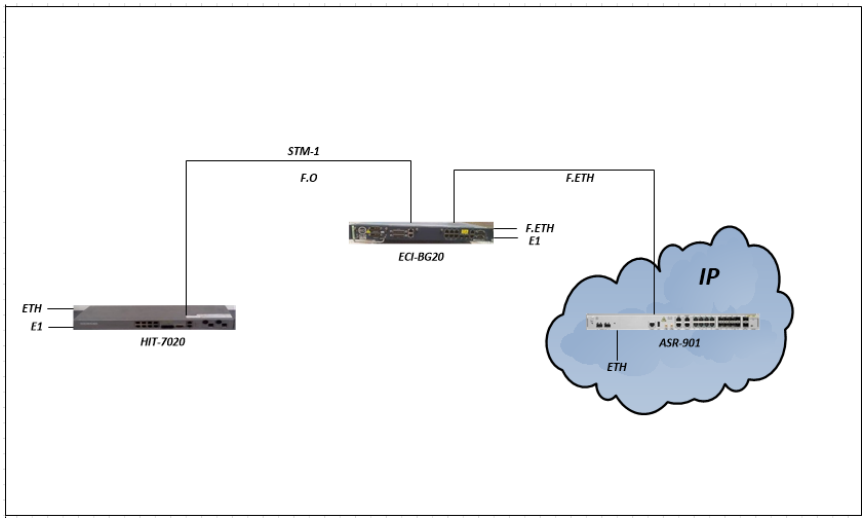


Figura 4.3: Maqueta de laboratorio Lineal con tecnología Mixta SDH-IP

En la figura 4.3 podemos observar la distribución de los equipos de transporte, la comunicación la iniciaremos con el equipo HIT7020, este equipo se conectara al equipo ECI-BG20 mediante fibra óptica, estos dos equipos tendrán salida Ethernet y E1s, la comunicación hacia el equipo CISCO ASR 901 será mediante cable Ethernet y su salida será por Fast Ethernet.

4.3.2. Generalidades de Equipos a Utilizar.

4.3.2.1. CISCO ASR 901

Las Series de los equipos de agregación Routers Cisco ASR 901 son equipos de alta velocidad , optimizados para cualquier sede celular Red de Acceso Radio (RAN) backhaul y acceso Ethernet . Mediante el uso de los routers Cisco ASR 901 , los operadores pueden reducir los costos de operación de retorno , simplificar y converger su RAN y las redes de acceso de Ethernet , y mejorar sus oportunidades de obtener ganancias con servicios Ethernet móviles y premium .

Cisco ASR 901ofrece una variedad de soluciones de transporte backhaul para operadores de Internet móvil con el Sistema Global para Móviles (GSM) , Code Division Multiple Access (CDMA) , Universal Mobile Telecommunications Service (UMTS) , y las redes WiMAX .

4.3.2.1.1. Características y Capacidades.

- ✓ Formato pequeño para sitios celulares con temperatura de funcionamiento extendido
- ✓ Acceso Panel frontal cableado y los indicadores LED
- ✓ Alimentación redundante y refrigeración
- ✓ Tecnología nV capaces
- ✓ Opciones de reloj flexibles: TDM , BITS , 1588v2 y SyncE Cell- sitio RAN plataforma de transporte diseñado para ayudar a satisfacer las necesidades futuras
- ✓ Apoyo a todas las tecnologías de sincronización de reloj
- ✓ Bajo consumo de energía

En la figura 4.4 y 4.5 podemos observar el chasis del equipo CISCO ASR 901 y también se observa el comportamiento del equipo ASR 901 en una red de transporte.

Figura 4.4: Equipo CISCO ASR 901

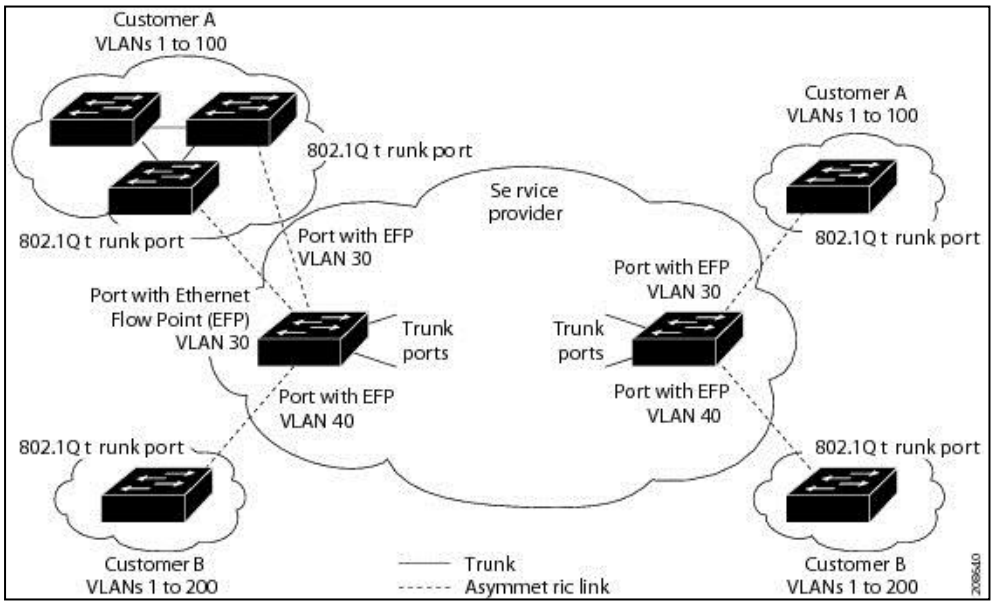


Figura 4.5: Equipo BG 20

4.3.2.2. Coriant-Siemens Hit7020

El Suprass HIT 7020 está diseñado como un multiplexor compacto, el elemento de red HIT 7020 es un diseño "pizza box", viene con todas las funciones de hardware instaladas en una caja con todas las funciones dentro de una unidad. El HIT 7020 viene con configuración de transmitir señales STM-1 o STM-4 en interfaces de líneas y con interfaces 8 x E1 (2Mb) a 75 o 120 Ohm y la interfaz con o sin 4xFe/T. El HIT 7020 se puede adquirir con fuentes de alimentación DC o AC.

4.3.2.2.1. Características

Interfaces:

- ✓ 4 Fast Ethernet (L2/T): Permite la transmisión de datos Ethernet
- ✓ 8xE1: Acceso a la señal PDH de 2 Mb
- ✓ STM-1: Dos conexiones de interfaz STM-1 para la conexión con otro elemento de red.
- ✓ STM-4: Dos conexiones de interfaz STM-4 para la conexión con otro elemento de red.
- ✓ Consola: El puerto de consola se usa para la interfaz CLI con el elemento de red. Un operador puede configurar los parámetros de comunicación usando solo CLI.
- ✓ Alarma Externa: Se usa para conectividad con un panel de alarmas externo. Se usa para iniciar la severidad de las alarmas.

- ✓ Interfaz de Gestión de Red: Este puerto se puede usar para conectividad con el TNMS-M LCT o con el servidor TNMS-M.
- ✓ Small Form Pluggable (SFP): En los NE de la serie suprass HIT 70XX todos los transceptores ópticos para STM-1, STM-4, STM-16, Fast Ethernet son conectables. Cada módulo SFP almacena toda la información relevante del módulo. Cuando un SFP se conecta a un puerto, el controlador lee los datos internos del módulo a través de una interfaz serial digital de dos cables . Los modulos de SFP del suprass 7070 y 7050 se pueden usar en los elementos de red suprass 7060 HC, 7060, 7030 y 7020

Conectores de Fuente de Energía:

Elchasis del suprass HIT 7020 incluye las entradas de energía redundante -48V a -60V DC o una entrada de energía 110/220 AC. El chasis del suprass HIT 7020 requiere por lo menos una fuente de alimentación DC o 110/220 V AC para operar. Las dos entradas de energía DC comparten la carga. El chasis puede operar indefinidamente si la energía de cualquier entrada.

En la figura 4.6 observamos el chassis del Suprass HIT 7020 y en la figura 4.7 observamos la ubicación del NE HIT7020 dentro de una red.

Figura 4.6: Suprass HIT 7020

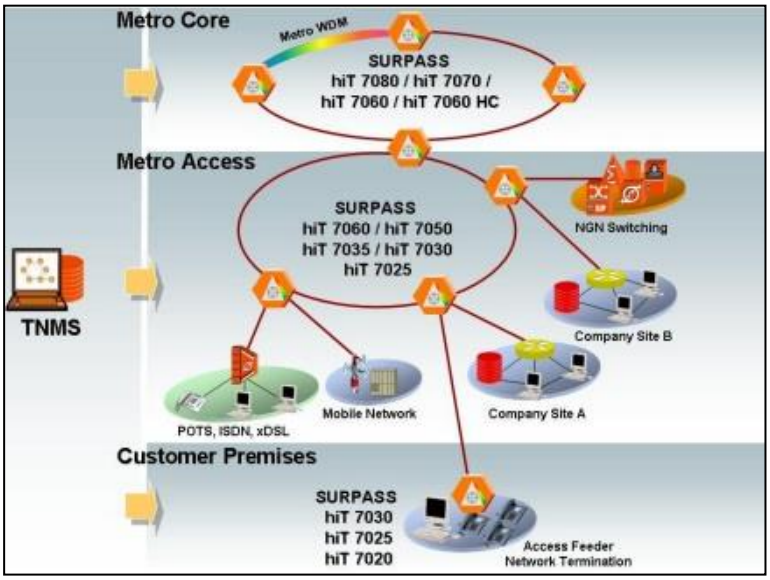


Figura 4.7: Utilidad de Suprass HIT 7020

4.3.2.3. Eci-BG 20

El equipo ECI-BG20 es un equipo que proporciona una combinación de tecnologías como Ethernet sobre sdh. El equipo BG20 es compatible con los servicios de triple play: IPTV , VoD , VoIP y HSI para NGN aplicaciones residenciales.

4.3.2.3.1 Interfaces, Topologías y Protección.

- ✓ Interfaces SDH: STM-1 y STM-4.
- ✓ Interfaces PDH: E1, E3 y DS3.
- ✓ Interfaces de Datos: 10/100/1000 Mbps. Ethernet sobre SDH (EoS). Ethernet sobre PDH (EoP). IP, MPLS.
- ✓ Interfaces PCM: FXO, FXS, 2/4W E&M, V24, V35, G.703 64K, V11/X21
- ✓ Topologías: Mesh, multi-ring, ring, star, linear

4.3.2.3.2 Capacidad del Sistema.

- ✓ Ethernet: Capa1-40 x 10/100 8 x 1000SX/LX/ZX; Capa 2- 40 x 10/100 8 x 1000SX/LX/ZX
- ✓ SDH: 18 x STM-1 3 x STM-4
- ✓ PDH/PCM: 252 x E1, 18 x E3, 18 x DS-3, 72 x PCM I/F

En la figura 4.8 y 4.9 podemos observar el chasis del equipo BG20 y la utilidad de dicho equipo dentro de una red.

Figura 4.8: Equipo Eci BG20

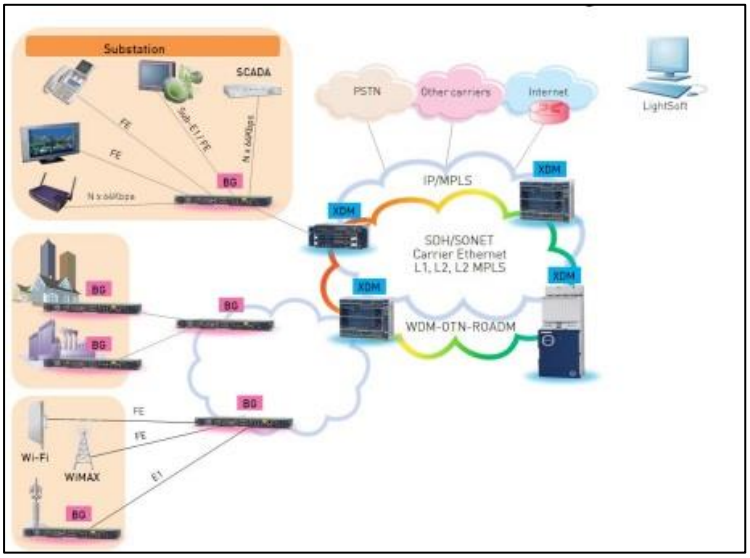


Figura 4.9: Utilidad de Equipo Eci BG20 dentro de la red

4.4. Configuración de Maquetas.

4.4.1. Configuración de HIT 7020.

Primeramente lo que realizaremos será la configuración del HIT 7020. Para realizar la configuración de la IP de Gestión y la IP remota en el equipo se puede acceder a Hyper terminal o a Putty, en nuestro caso utilizaremos el programa putty. En la figura 4.10 se muestra el icono del programa Putty. El tipo de cable que usaremos para la conexión será de tipo USB a Serial, esto se hace desde el puerto consola del HIT7020.

Figura 4.10: Inicio de sesión en programa Putty

Al abrir el programa putty, tenemos que seleccionar que tipo de conexión necesitaremos, en este caso será de tipo serial, el COM que nos asignó la pc fue el número 13. Figura 4.11

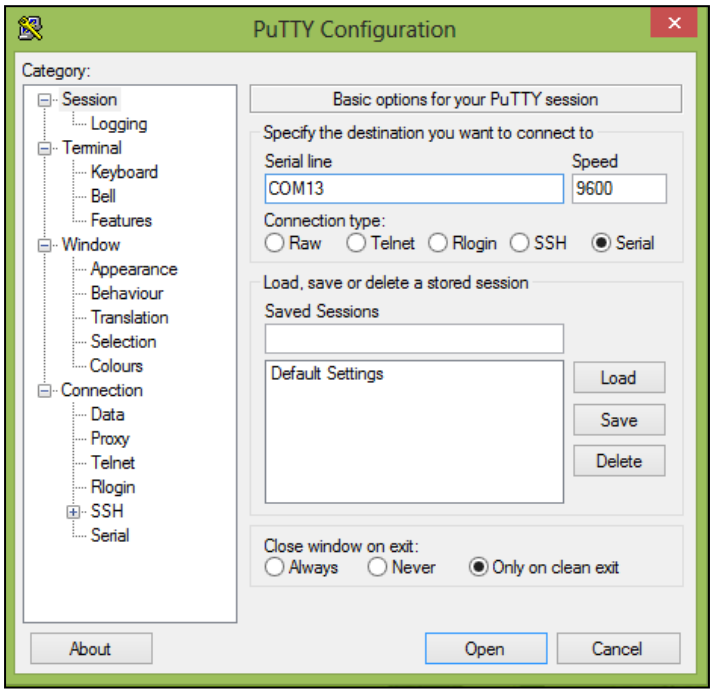


Figura 4.11- Configuración de parámetros

En la siguiente figura se muestra la interfaz de putty, el nombre de usuario es root y no lleva contraseña, en la figura 4.12 se observa lo antes mencionado.

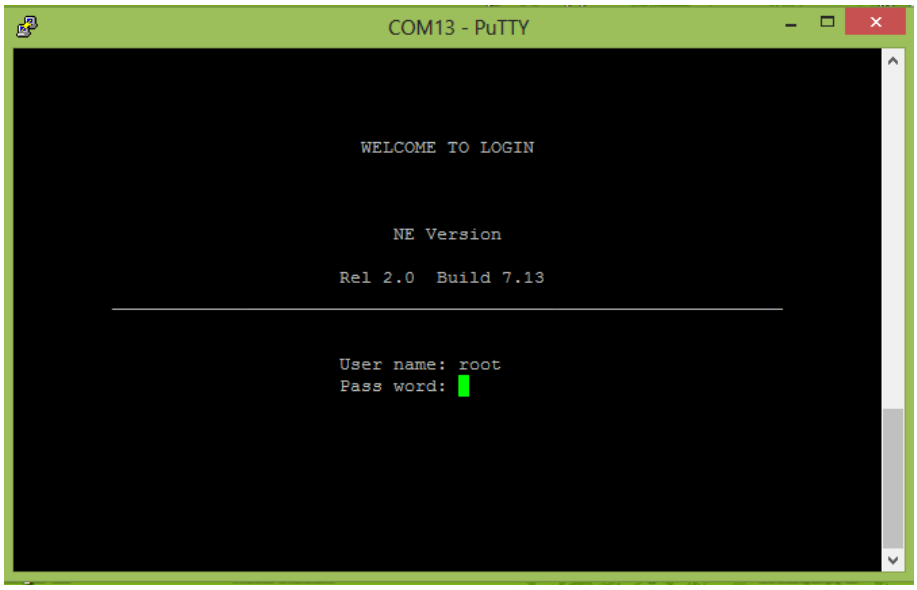


Figura 4.12- Configuración de nombre de usuario.

Seleccionamos la opción (I) Configuración de Direcciones IP, procedemos a configurar el nodo IP y la dirección IP, esto se muestra en la figura 4.15. En la tabla 1 se muestra la direccion IP y nodo IP configurado al HIT 7020.

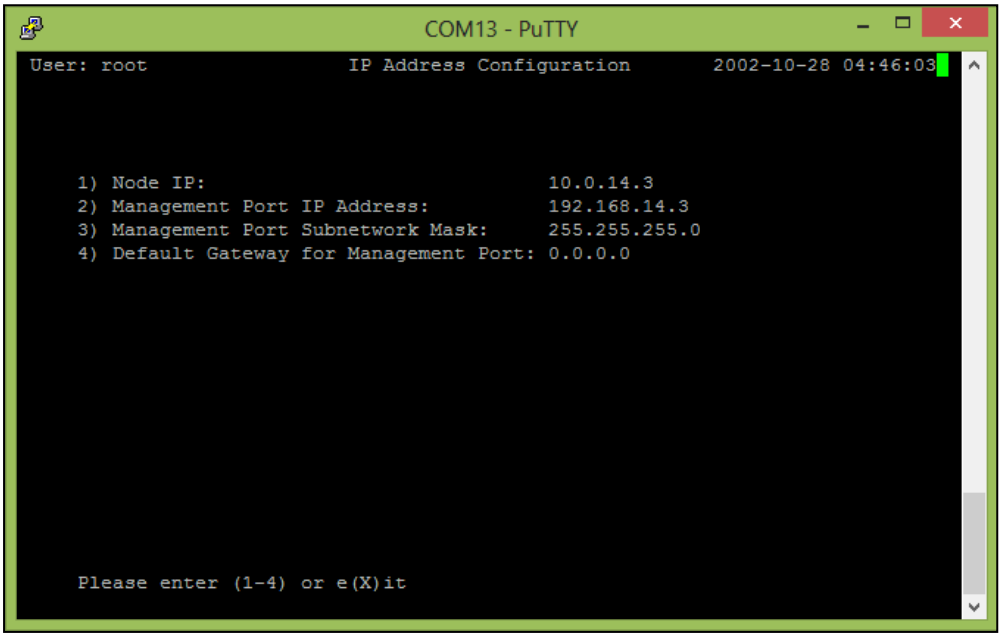


Figura 4.13- Configuración de nodo IP y dirección IP.

Tabla 4.1- Nodo IP y Dirección IP asignada.

Configuración de Equipos HIT 7020			
EQUIPO	NODO IP	DIRECCION IP	MASCARA DE RED
HIT 7020	10.0.14.3	192.168.14.3	255.255.255.0

Al finalizar de configurar la IP y el nodo IP en el HIT 7020, procedemos a configurar nuestra tarjeta de red, siempre en el mismo segmento de red. Nuestra ip será 192.168.14.8. En la figura 4.14 observamos la configuración de nuestra tarjeta de red.

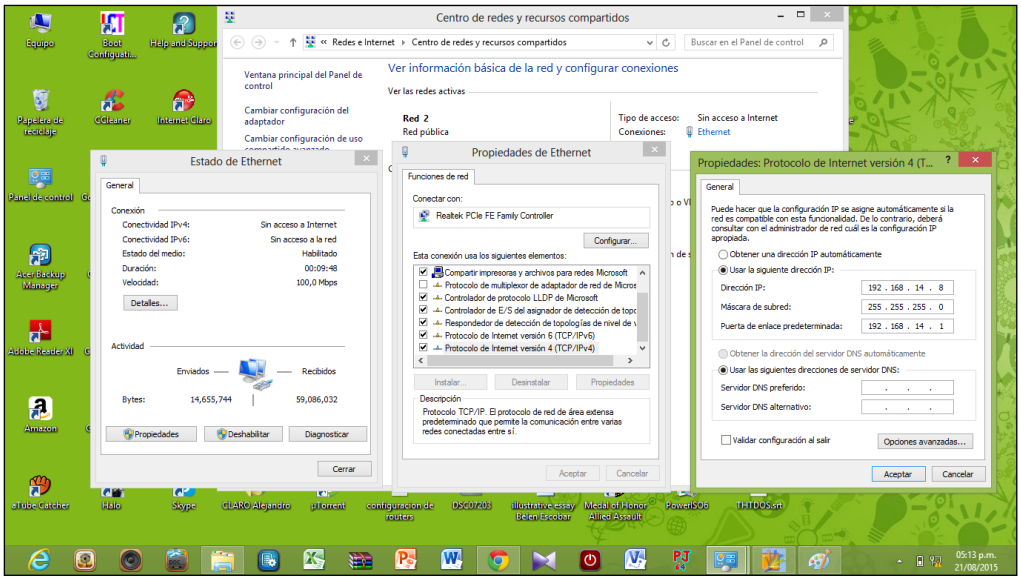


Figura 4.14- Configuración de tarjeta de red en nuestra PC.

Después de haber configurado nuestra tarjeta de red dentro del mismo segmento en el cual se encuentran los equipos HIT 7020, procedemos a abrir el LCT para entrar al equipo HIT 7020,en la figura 17 se observa el icono del LCT Suprass HIT 7020 con la versión 3.2.5.
El tipo de cable que usaremos será cable plano Ethernet, se conectara al puerto MGMT del HIT7020.

Figura 4.15- LCT Suprass HIT7020 versión 3.2.5.

Al ingresar al LCT nos muestra la interfaz del equipo HIT 7020, seguido empezaremos a configurar los puertos DCC de modo y protocolo para la gestión remota, nombre del STM-1. Damos click sobre configuration, nos dirigimos a DCN Managment, abriendo la pestaña de DCC Managment y damos click a como aparece en la figura 4.16.

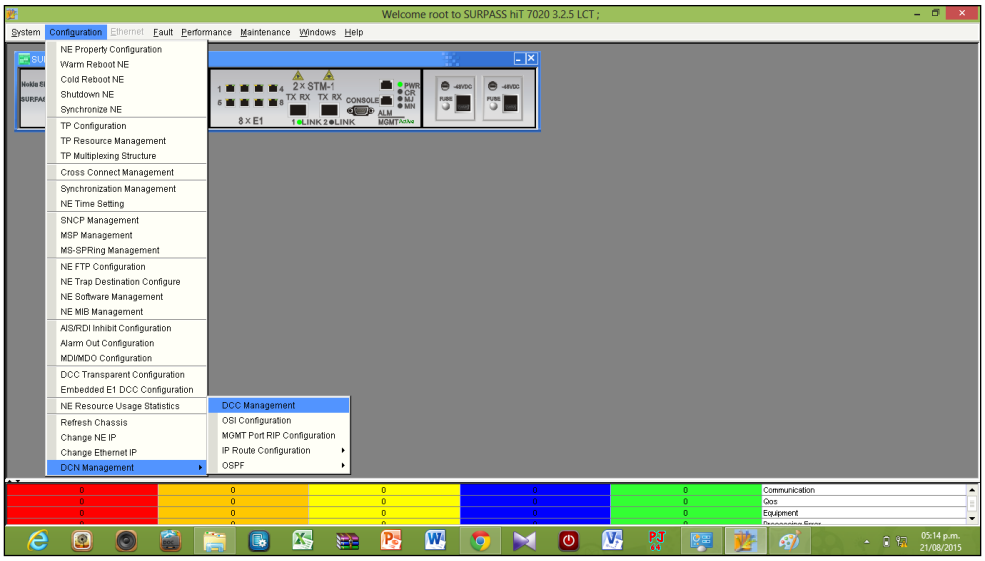


Figura 4.16- Configuración de DCC Managment

En algunas ocasiones los parámetros de DCC Managment, están configurados de manera automática, como lo están en este caso, si algún dado caso el equipo esta nuevo entonces procederemos a realizar dichas configuraciones, figura 4.17 muestra la ventana.

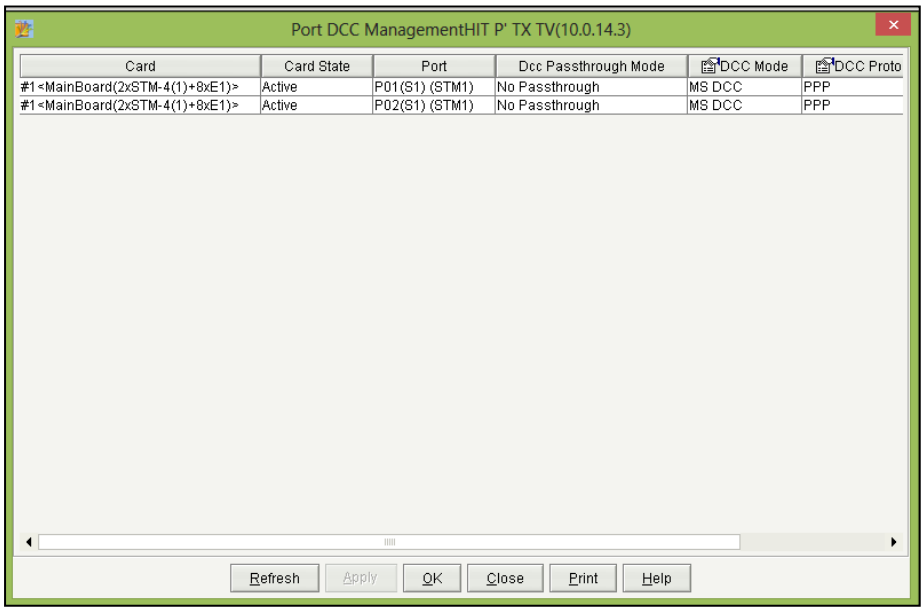


Figura 4.17- Configuración de Modo DCC y Protocolo DCC.

Seguido de eso procederemos a configurar los OSPF General, OSPF áreas y OSPF interfaces. Damos click sobre configuration, seguido de DCN Managment, OSPF y OSPF General. Figura 4.18.

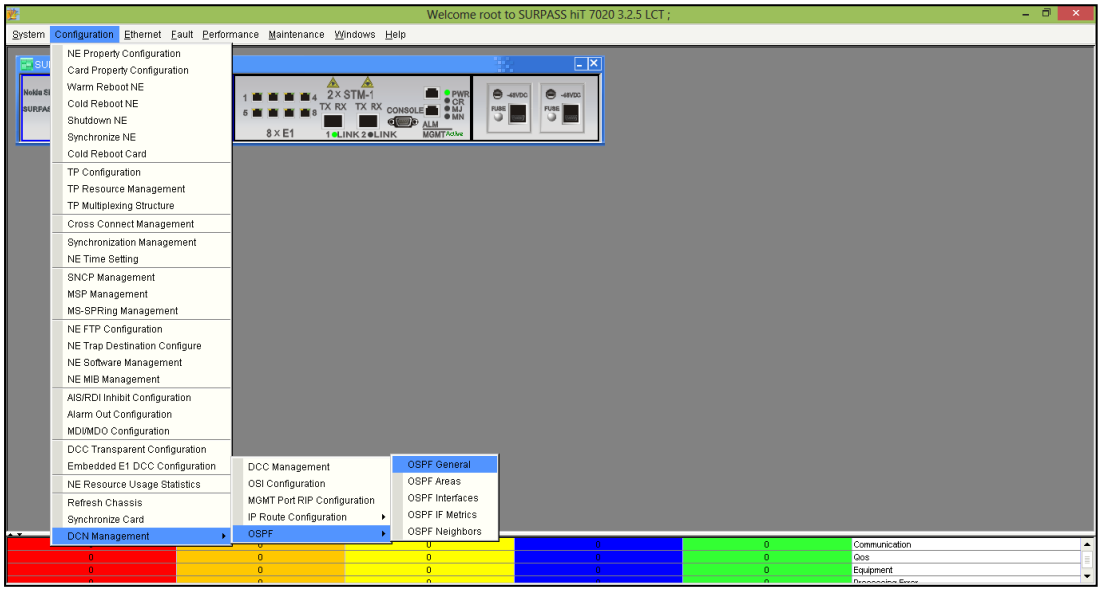


Figura 4.18- Configuración de OSPF.

En OSPF general lo que configuraremos es el router ID, para el HIT 7020 el router ID será la 10.0.14.1. Eso se observa en la figura 4.19.

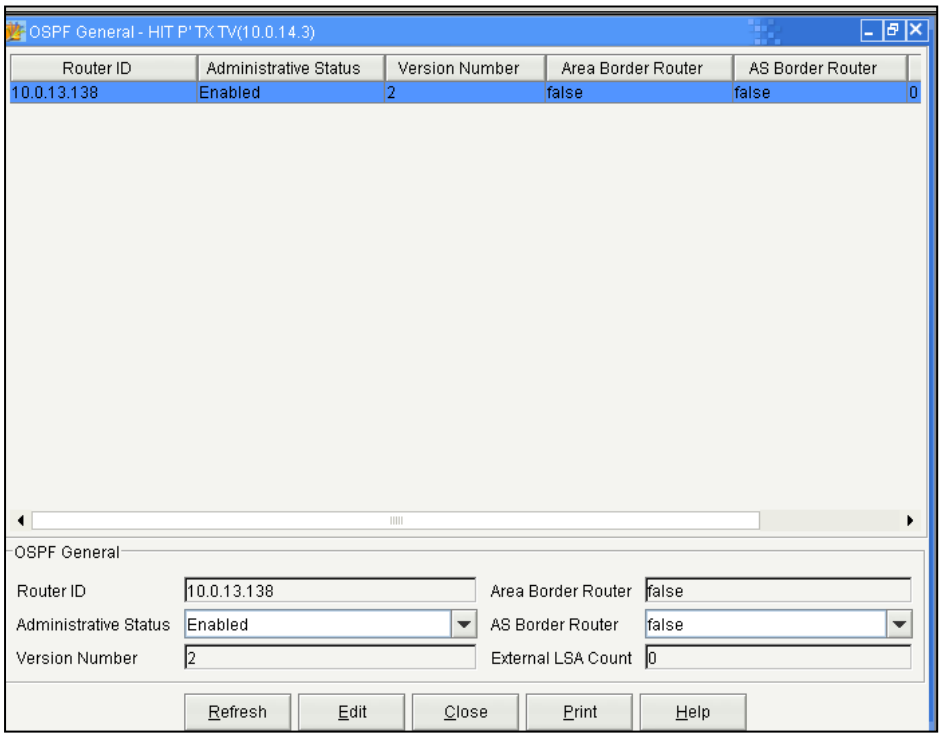


Figura 4.19- Configuración de OSPF General.

Para configurar los OSPF Área damos click sobre configuration, seguido de DCN Managment, OSPF y OSPF Area.

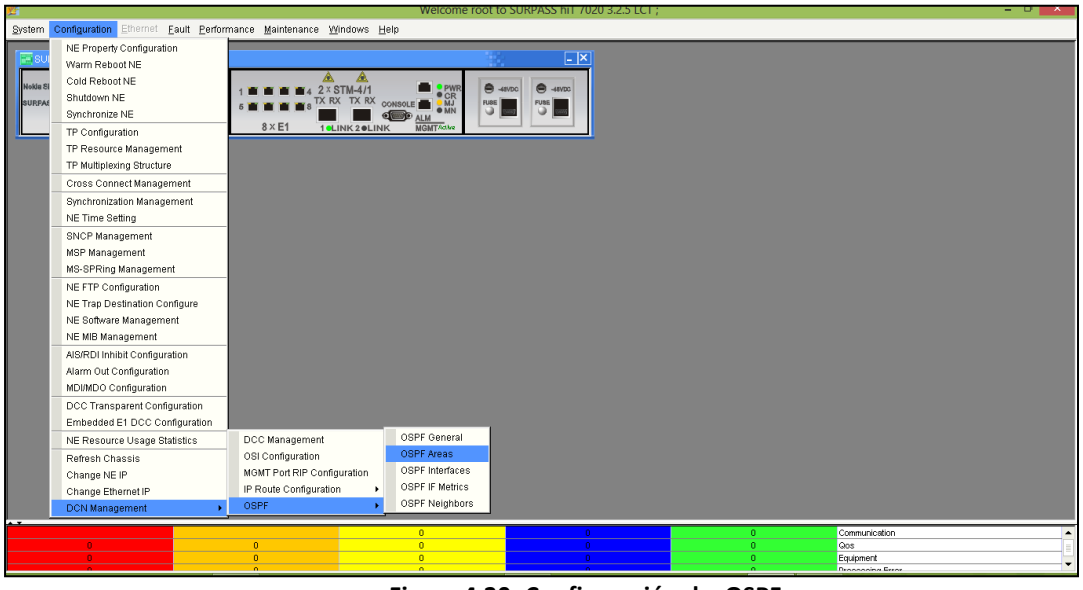


Figura 4.20- Configuración de OSPF.

En OSPF Areas lo que configuraremos será el Area ID, el Area ID será 0.0.14.0. En la figura 4.21 observamos lo anteriormente mencionado.

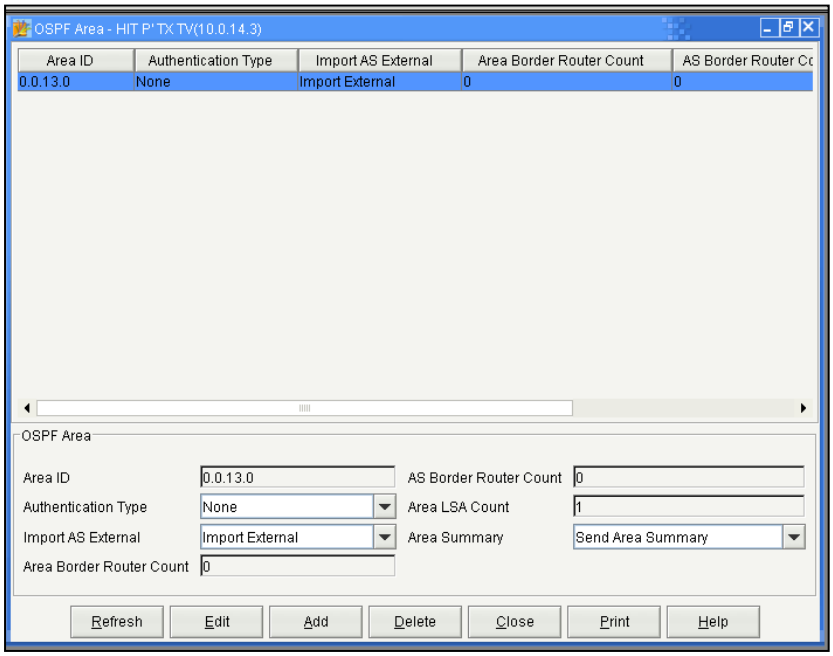


Figura 4.21- Configuración de OSPF Area.

Para configurar los OSPF Interfaces damos click sobre configuration, seguido de DCN Managment, OSPF y OSPF Interfaces.

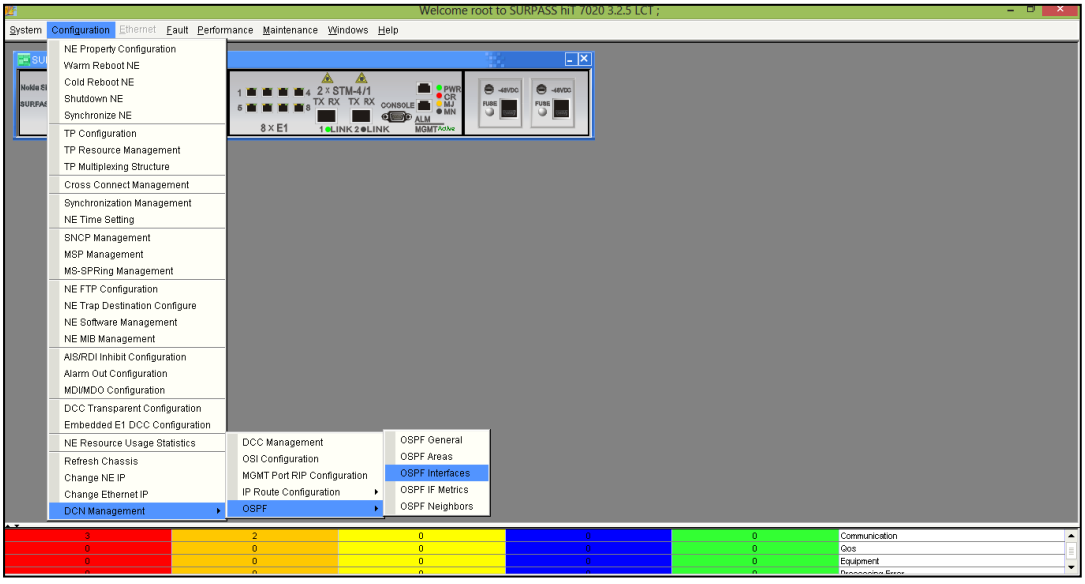


Figura 4.22- Configuración de OSPF.

En OSPF Interfaces lo que tenemos que tener en cuenta es que el Area ID este en la 10.0.14.0, si se encuentra en otra área tendremos que migrar a la área que queremos utilizar, damos click en editar, lo migramos al área a utilizar y le damos ok.Esto lo podemos observar en la figura 4.23.

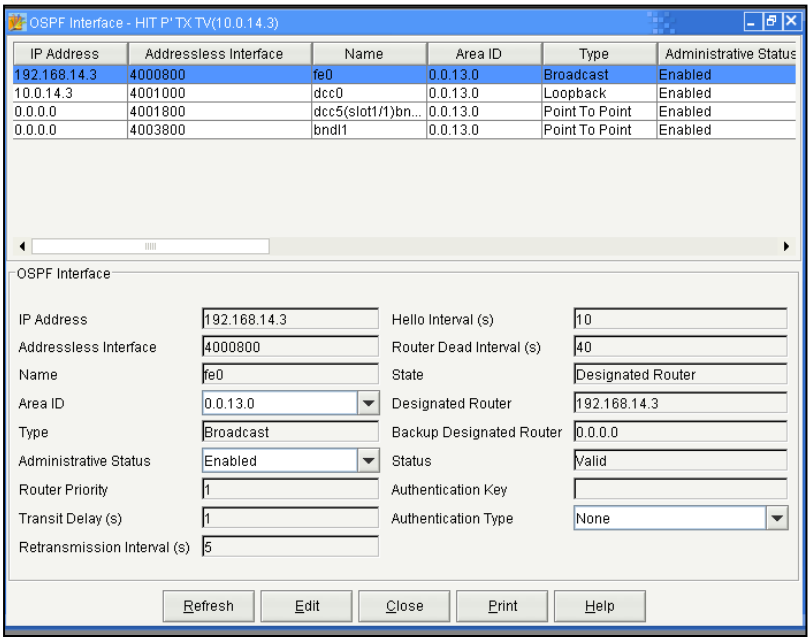


Figura 4.23- Configuración de OSPF Interfaces.

Para habilitar los puertos Fast Ethernet en los equipos HIT 7020, realizaremos lo siguiente, click derecho sobre la tarjeta 4xFE/L2, dar click sobre brigde configuration. Figura 4.24

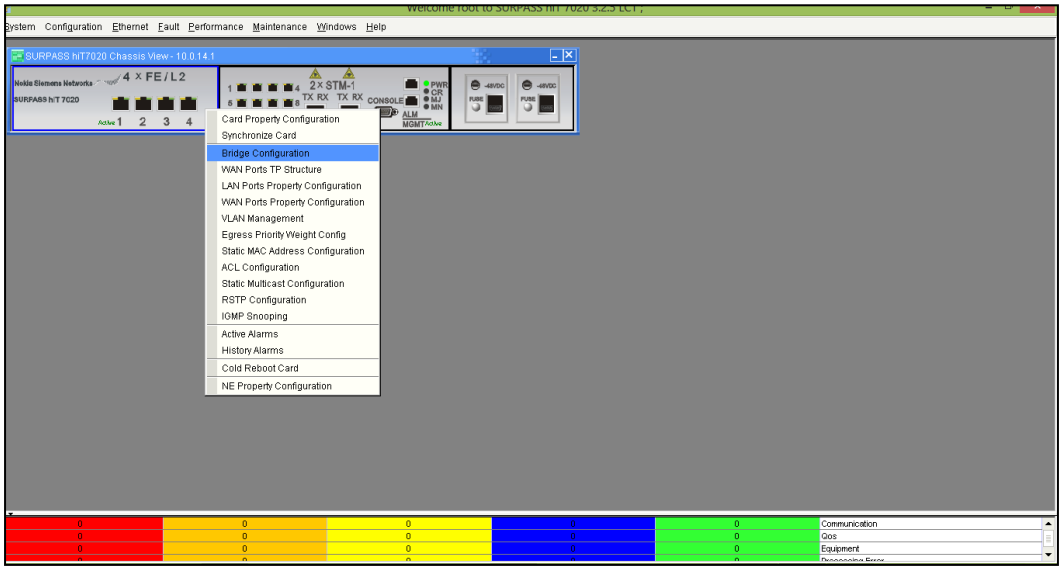


Figura 4.24- Configuración de Puertos FE.

Al darle click en brigde configuration se abre la siguiente ventana que se muestra en la figura 4.25, todo los parámetros quedan igual a excepción del segmento de Vlan,

podemos escoger cualquiera de los 8 segmentos de Vlan disponibles, en nuestro caso utilizaremos el segmento de Vlan # 1, que abarca la (1-511).

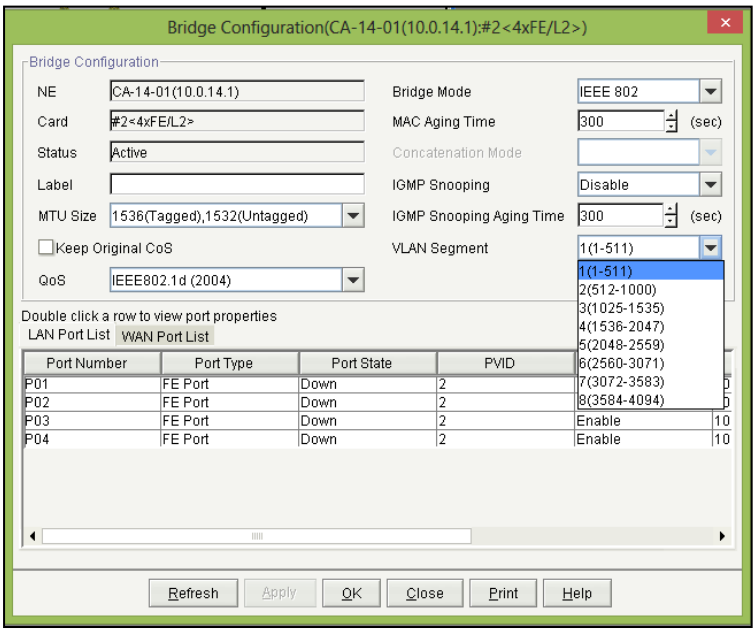


Figura 4.25- Configuración del Brigde Configuration.

El siguiente paso a realizar es configurar los puertos LAN, para ello damos click derecho sobre la tarjeta 4xFE/L2, dar click sobre LAN Ports Property Configuration. Eso se muestra en la figura 4.26.

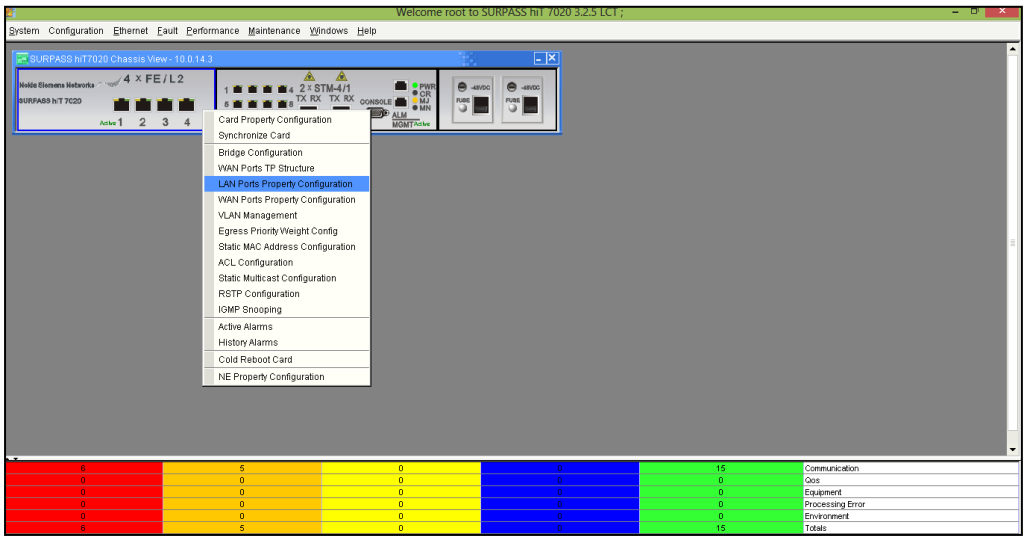


Figura 4.26- Configuración de LAN Ports Property Configuration paso 1.

Al dar click en LAN Ports Property Configuration se nos abre la imagen de la figura 4.27, la configuración que realizaremos será en la pestaña port podemos seleccionar

los 4 puertos FE que posee el HIT 7020, en nuestro caso se seleccionaron los 4 puertos, en la opción Egress Tag Mode lo dejamos configurados como Untag, hay dos tipos de configuraciones, modo Tag que es para que el puerto funcione como modo acceso y modo Untag que es para que el puerto funcione como modo troncal, en nuestra maqueta los 4 puertos FE los configuramos modo Untag. En la opción de PVID asignamos el ID 2 que se encuentra en el segmento de vlan 1 que abarca (1-511), en un entorno real se asignan 2 PVID dentro del segmento de vlan 7 que comprende (3072-3583), las 2 ID son la 3221 que es para litespan voz y la 3222 que es para litespan gestion.

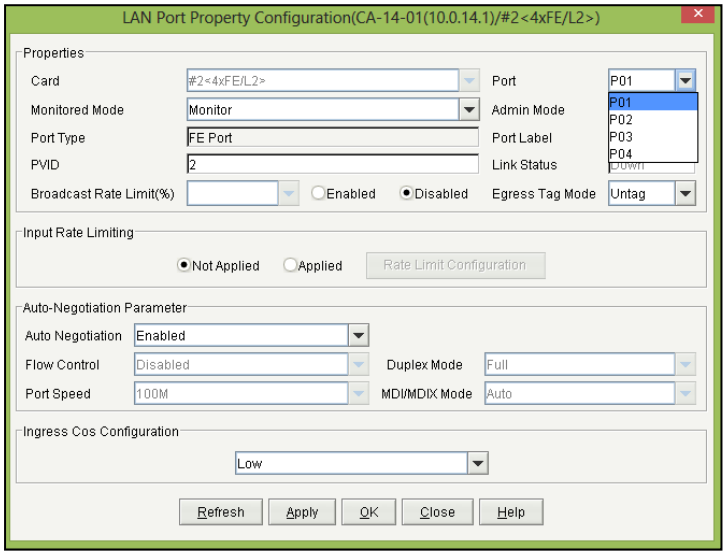


Figura 4.27- Configuración de LAN Ports Property Configuration paso 2.

El siguiente paso a realizar es configurar el ancho de banda a los puertos LAN, para ello damos click derecho sobre la tarjeta 4xFE/L2, dar click sobre WAN Ports Property Configuration. Eso se muestra en la figura 4.28.

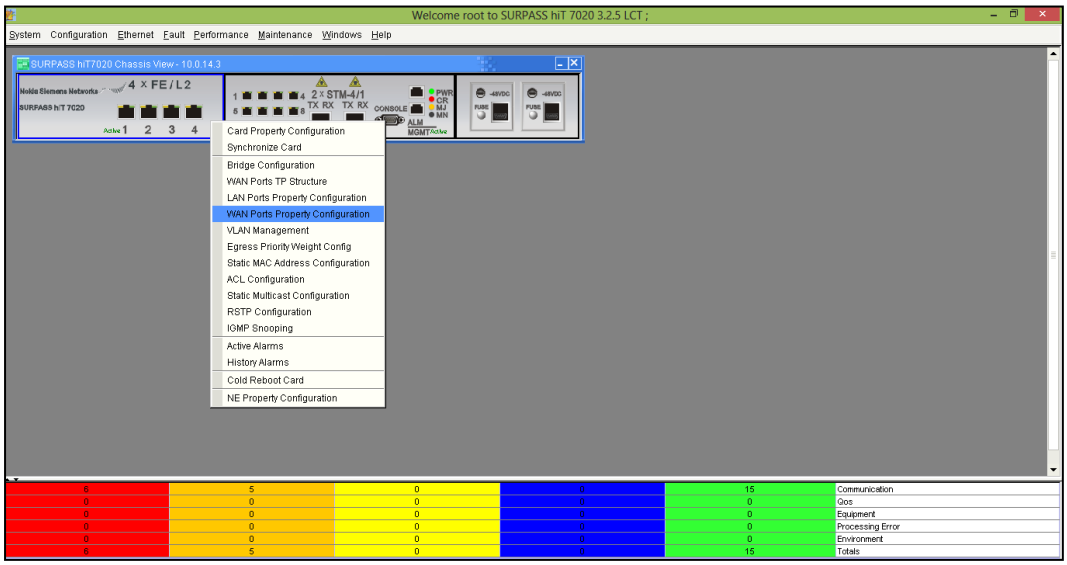


Figura 4.28- Configuración de WAN Ports Property Configuration paso 1 .

Al dar click en WAN Ports Property Configuration se nos abre la imagen de la figura 4.29, para configurar y seleccionar los puertos damos click en ports, seleccionamos LCAS Disable, ponemos en PVID el número de vlan que es la 2, Egress Tag Mode lo dejamos en Untag o modo troncal, Ingress Coss Configuration lo dejamos Low y damos click en Bandwidth Management.

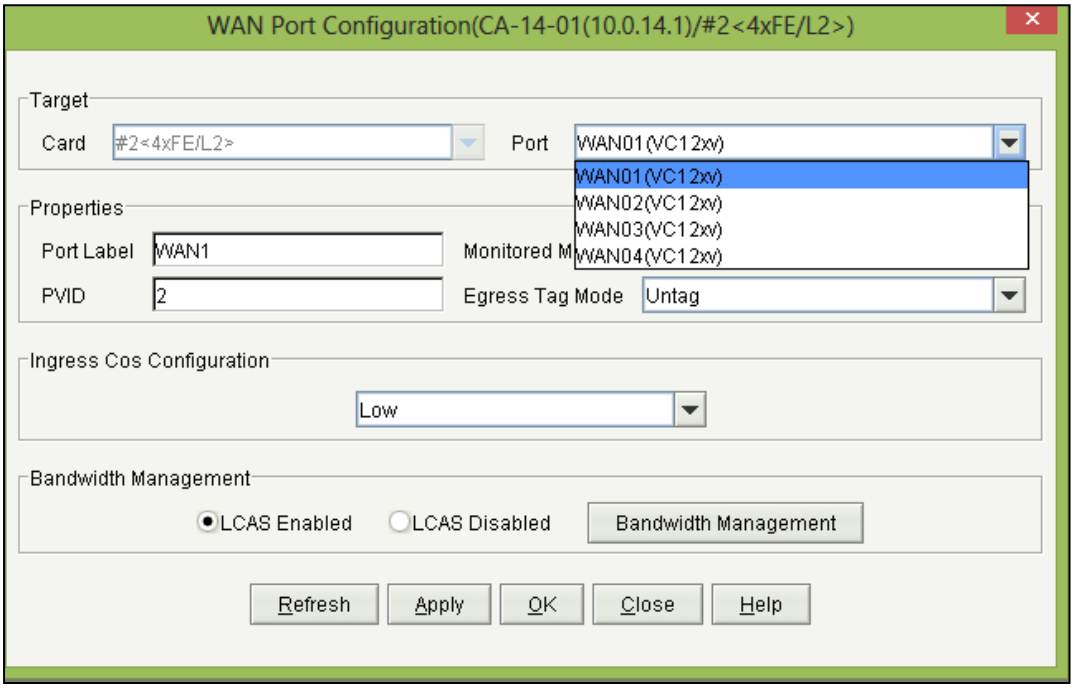


Figura 4.29- Configuración de WAN Ports Property Configuration paso 2.

Al dar click en Bandwidth Management se nos presenta la siguiente ventana, en esta ventana elegimos los VC12 que se van a usar o se elige el ancho de banda que van a tener la WAN, en este caso escogemos 4 VC12. Al escoger los VC12 le damos apply y despues close. Figura 4.30.

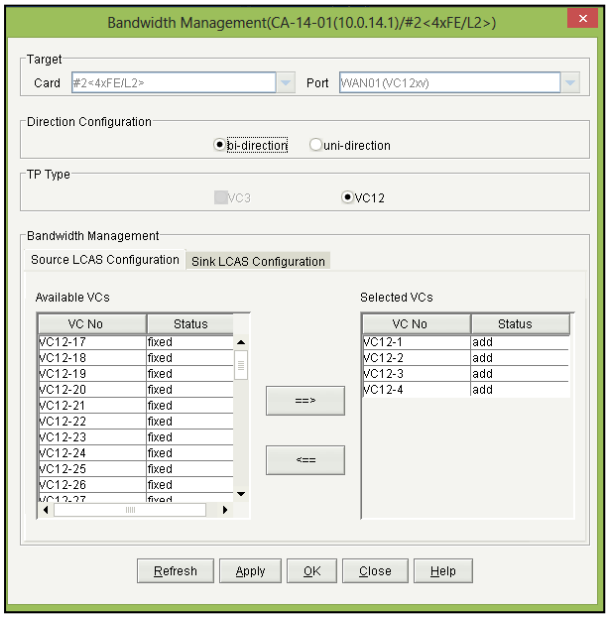


Figura 4.30- Configuración del Ancho de Banda de las WAN.

El último paso para terminar de configurar los puertos FE es la configuración de las Vlan, para ello damos click derecho sobre la tarjeta 4xFE/L2, dar click sobre Vlan Management. Eso se muestra en la figura 4.31.

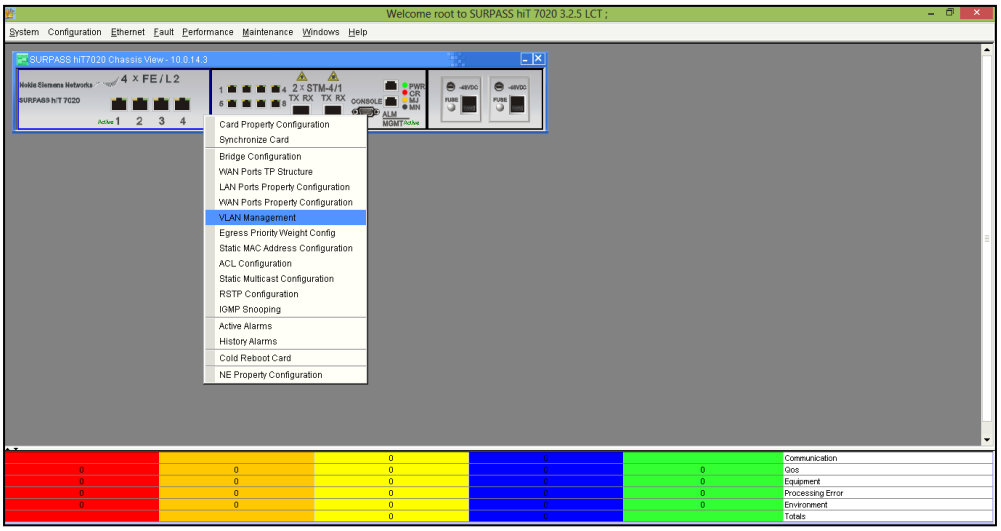


Figura 4.31- Configuración de Vlan.

Al dar click en Vlan Management nos muestra la siguiente ventana, en dicha ventana damos click en Vlan Configuration para asociar las Vlan de los puertos LAN con las WAN, en Vlan ID ponemos la Vlan que estamos usando que es la numero 2 y damos click en port list. Al dra click en port list, aparece en la parte izquierda de la ventana los puertos que estan habilitados, seleccionamos todos los puertos y todas las WAN y le damos apply.Figura 4.32

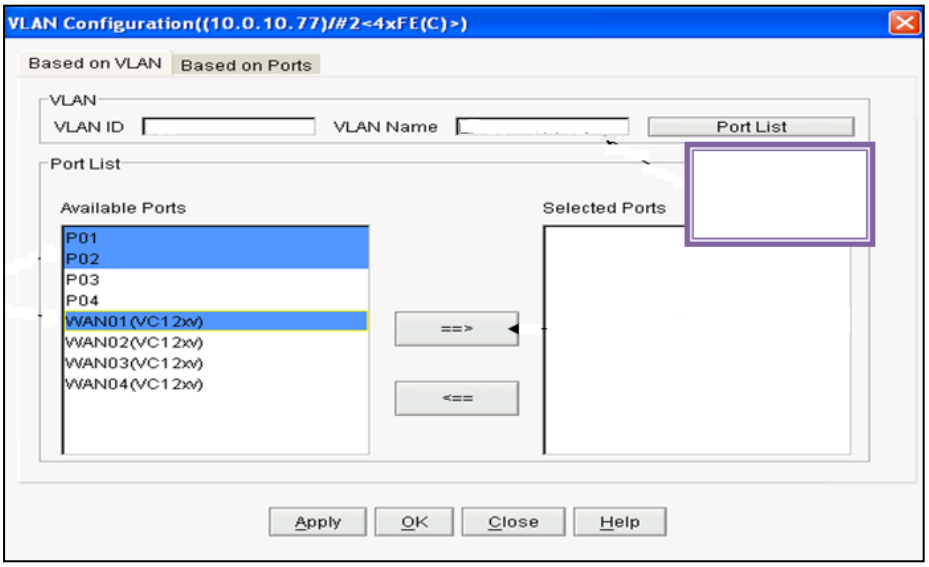


Figura 4.32- Asociación de puertos LAN y WAN.

Al asociar los puerto LAN con las WAN, nos quedara como se muestra en la figura 4.33

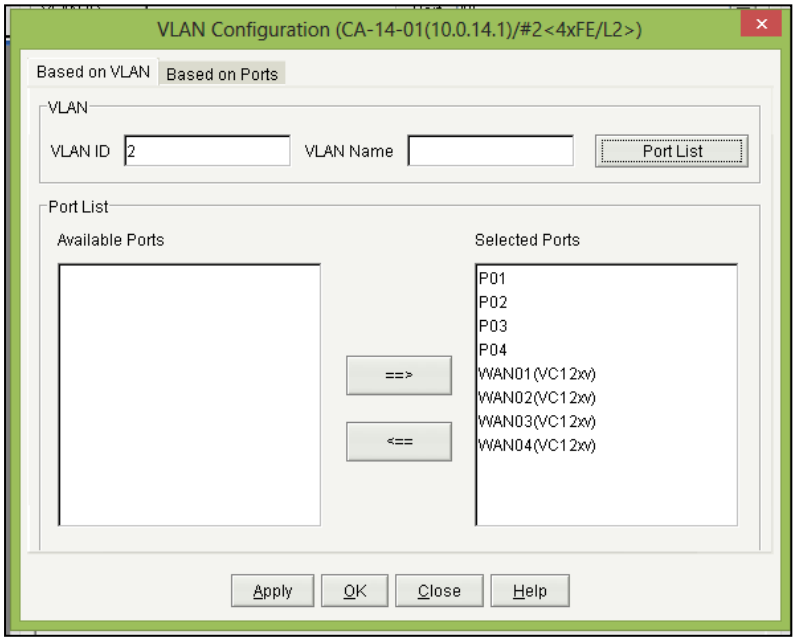


Figura 4.33-Puertos LAN y WAN asociados paso 1.

Al dar click en la opción Close, no aparece una ventana en donde nos muestra que la asociación de puertos LAN y WAN se realizaron de manera exitosa. Ver figura 4.34.

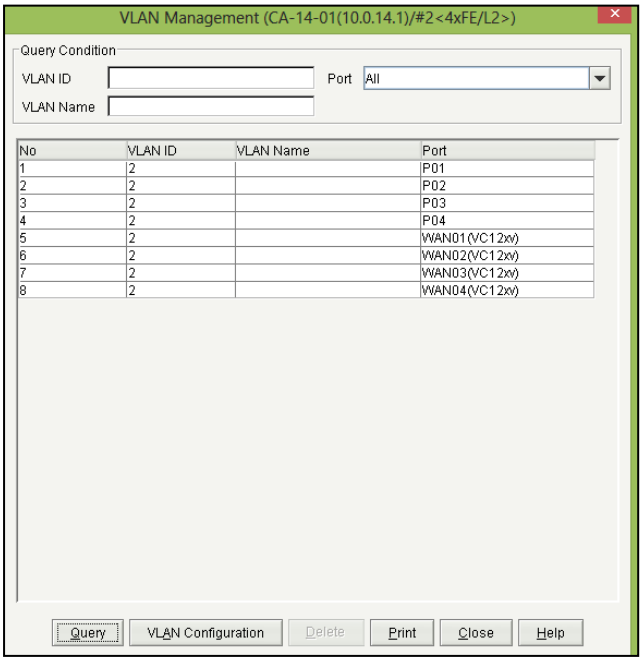


Figura 4.34-Puertos LAN y WAN asociados paso 2.

Al terminar de realizar las configuraciones de los puertos Fast Ethernet, procederemos a realizar las cross-conexiones para que los equipos HIT 7020 y BG20 se puedan comunicar entre sí. Para realizar las cross-conexiones nos dirigimos a la pestaña que dice configuration y damos click en la opción que dice Cross Connect Management. Figura 4.35

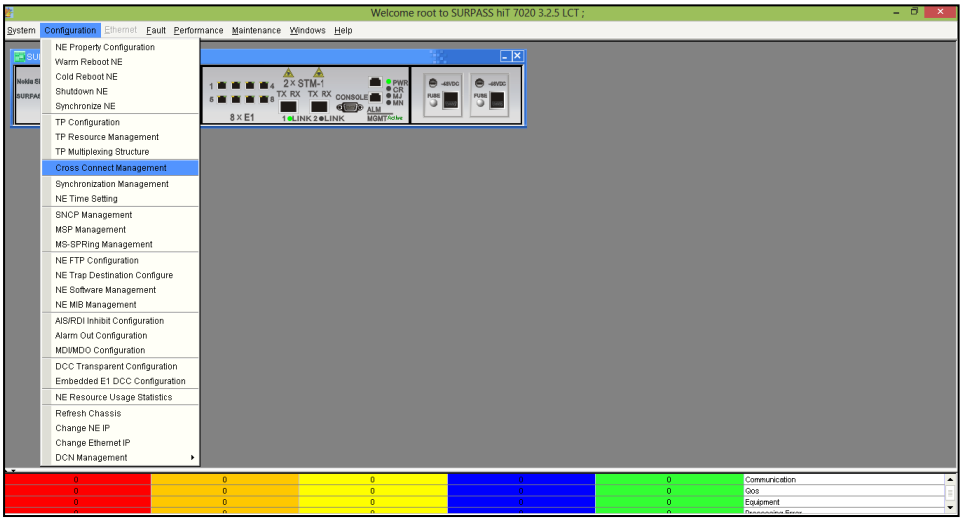


Figura 4.35- Cross Connect Management.

Al dar click en la opción Cross Connect Management, se nos presenta la ventana que se muestra en la figura 4.36, al dar click en Query no nos aparece ninguna cross-conexión ya que no hemos creado ninguna, para crear una cross-conexión damos click en Create a como se muestra en la figura.

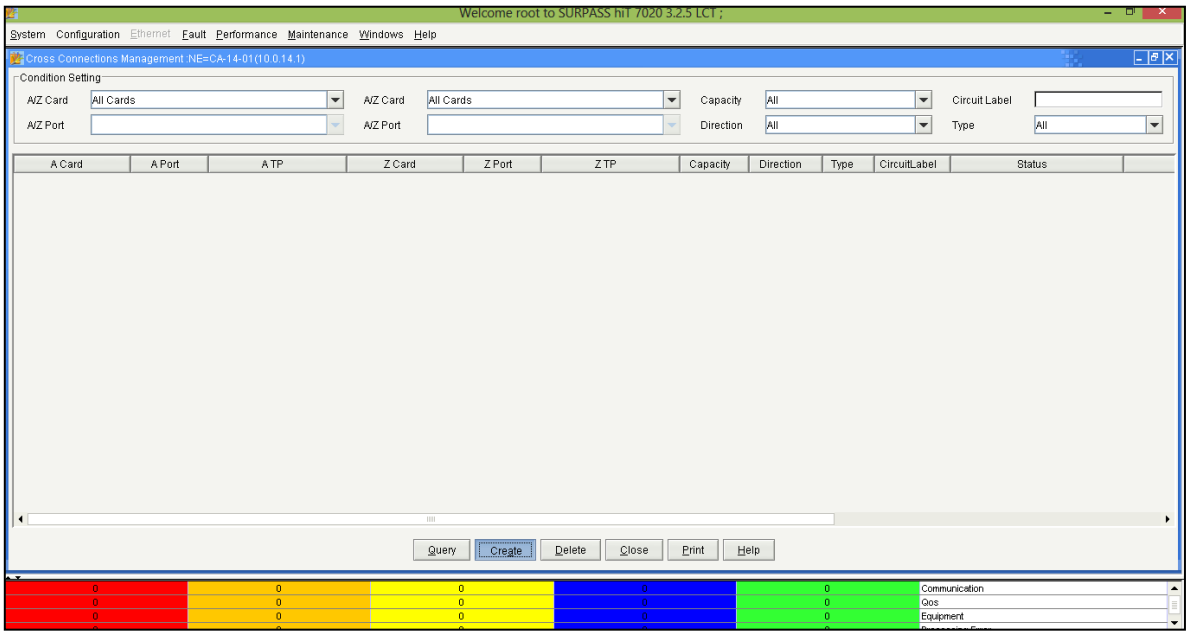


Figura 4.36- Creación de Cross Conexiones paso 1.

Al dar click en la opción Create nos aparece la ventana que se muestra en la figura 4.37, en la opción Capacity nos parecen 3 opciones: VC3, VC4 y VC12, escogemos el VC12, en dirección ponemos la opción bidireccional, para realizar las cross-conexiones escogemos el tipo de tarjeta, para el HIT 7020 elegimos en la tarjeta A 4xFE/L2 y en tarjeta Z escogemos MainBoard (2xSTM-1+8E1) y el puerto óptico 1 o PO1 (S1) y realizamos las cross-conexiones, escogemos los TU12 que vamos a asociar, todos los TU12 tienen que ser idénticos tanto en este equipo como en el BG20.

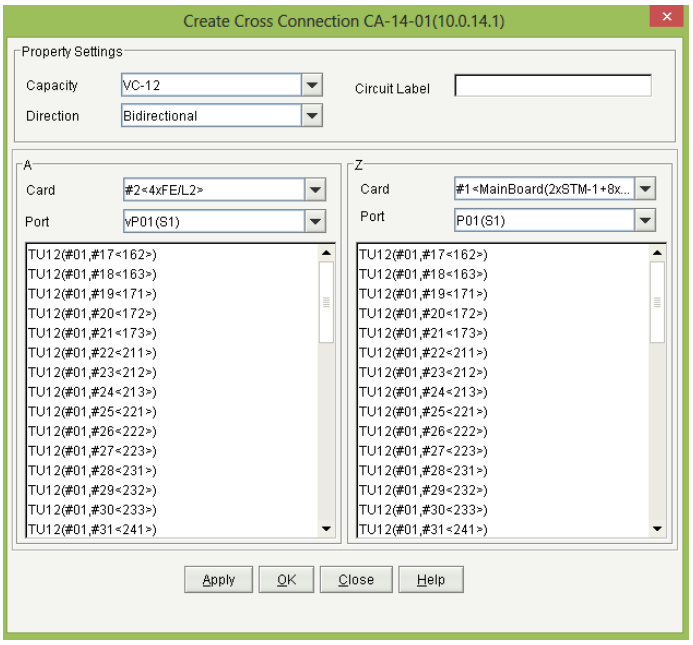


Figura 4.37- Creación de Cross Conexiones paso 2.

Al dar click en close nos aparecen la ventana que se muestra en la figura 4.38.

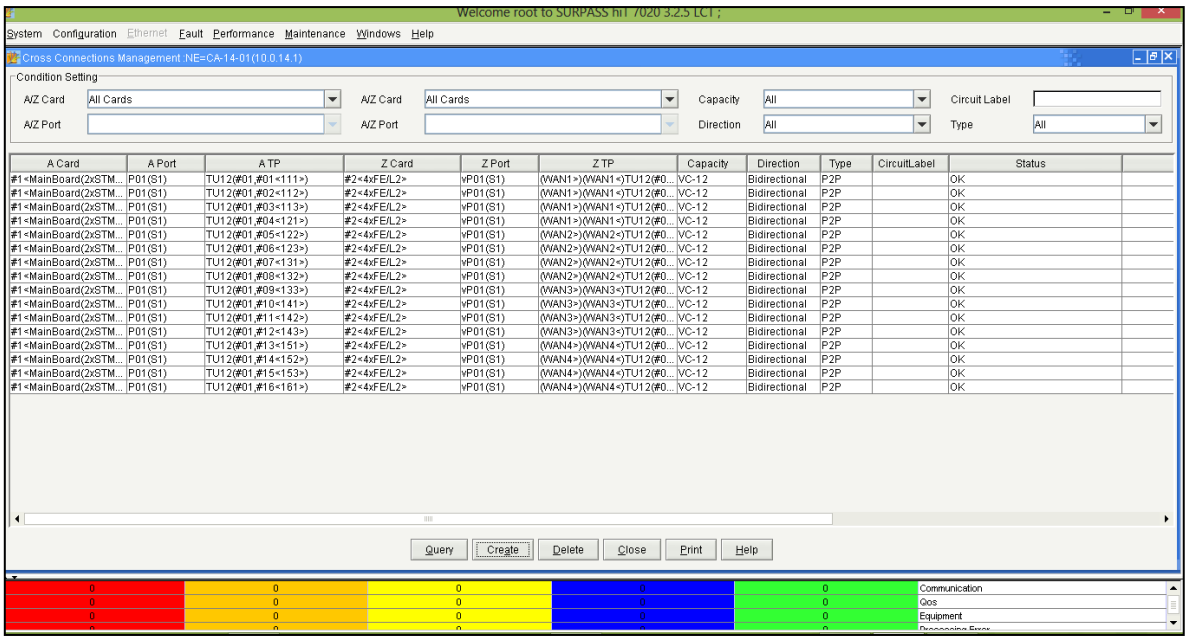


Figura 4.38- Cross Conexiones realizadas en HIT7020.

Al terminar de realizar nuestras cross-conexiones en los 3 HIT7020 tendremos comunicación por Fast Ethernet y por E1s. Lo siguiente es empezar a configurar los equipos CISCO MWR 2941 DC y el equipo CISCO ASR 901.

4.5. Configuración de equipo ECI-BG20.

Para realizar la configuración del equipo ECI BG20 se acceden a dos programas:

- Boot Configuration
- LCT-BGF

Si el equipo es nuevo y no se le conocen las IP o bien si no se le conoce las IP, hacemos uso del primer programa Boot Configuration.

Damos doble click en el icono del programa, al dar doble click nos aparece la siguiente ventana, escogemos la opción BG-20(MXC-20), automáticamente nos aparecen los 2 octetos con 192.100, los 2 últimos octetos lo tomaremos del número serie del equipo, serán los últimos 4 números, en este caso es 4005. Se rellena la dirección IP y queda: 192.100.40.5. Para esto debemos de haber configurado nuestra tarjeta de red dentro del mismo segmento del equipo.

Después de haber puesto la dirección IP, se encenderá el equipo BG20 y se dará un lapso de 5 segundos para poder acceder a él, después de darle un tiempo estimado de 5 segundos le damos click en el botón que dice connect. Figura 4.39

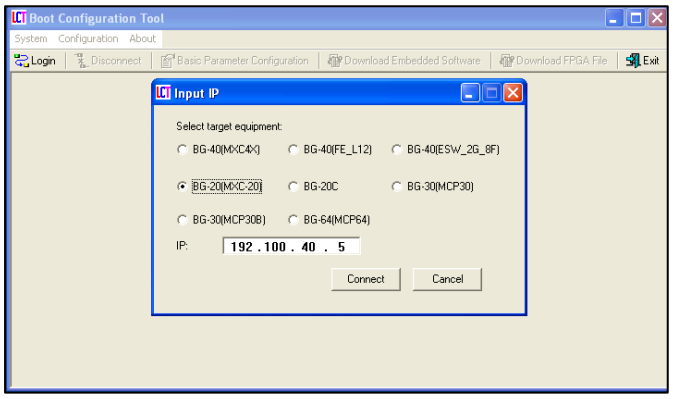


Figura 4.39- Selección de opcionBG-20MXC-20.

Al haber dado click en connect, nos aparece la ventana boot configuration tool, le damos click en la opción que dice Basic Parameter Configuration, nos aparecerá la ventana de la izquierda a como se muestra en la figura 4.39, los valores que se muestran en esa ventana, no es la dirección IP correcta del equipo, para obtener la dirección ip correcta del equipo, damos click en la opción Get y nos aparece la ventana de la derecha. La dirección IP de nuestro equipo es 172.20.29.1 con mascara /24, la cambiamos a 192.168.14.2 y seguidamente le damos apply.

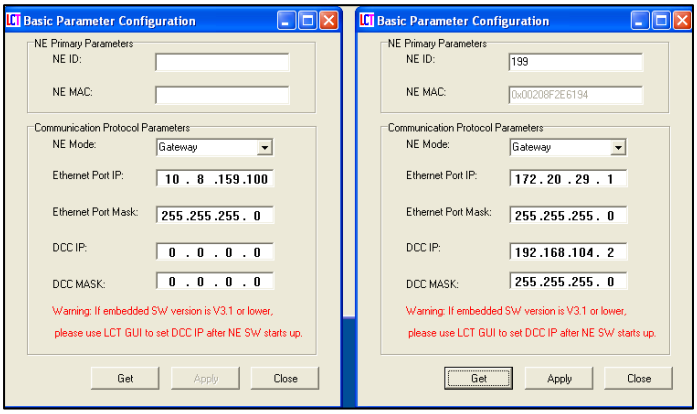


Figura 4.40- Configuración de dirección IP.

Despues de haber conocido la dirección IP de nuestro equipo, procedemos a utilizar el segundo programa. LCT-BGF, nos pedirá IP del equipo que es 192.168.14.2 y la contraseña, la contraseña para el equipo BG20 es: sdh123456, configuramos otra vez nuestra tarjeta de red, damos check en full upload NE data y le damos ok. Figura 4.41

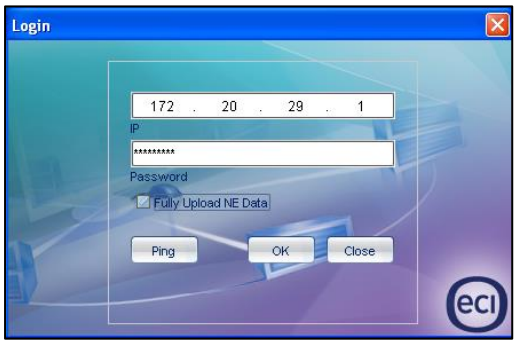


Figura 4.41- Acceso a programa LCT-BGF.

Nos aparecera la interface del equipo, para poder realizar cualquier configuracion nos pondremos sobre el chasis, se puede observar en el menu de la parte izquierda, el chasis dice 199 y sobre el otro menu que se encuentra en la parte superior, eligiremos la pestaña Advance y damos click en la opcion: Request Log in as Master, al dar click en esa opcion, nos dara la capacidad de realizar cualquier cambio en el equipo. Figura 4.41.

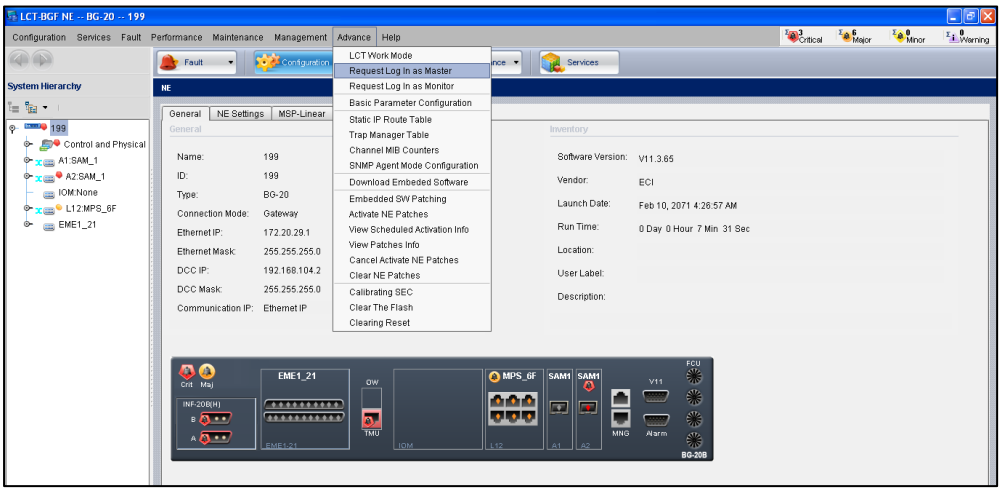


Figura 4.42- Interfaz de equipo BG20.

Para saber con exactitud que tarjetas tiene nuestro equipo, damos click derecho sobre el chasis que aparece en la figura 4.42 y le damos click en la opción Slot Assignment, nos aparece la ventana de la figura 4.43, damos click en Get Logical Card, luego en la opción Get Physical Card, seguido Set As Logical y por ultimo damos click en Apply

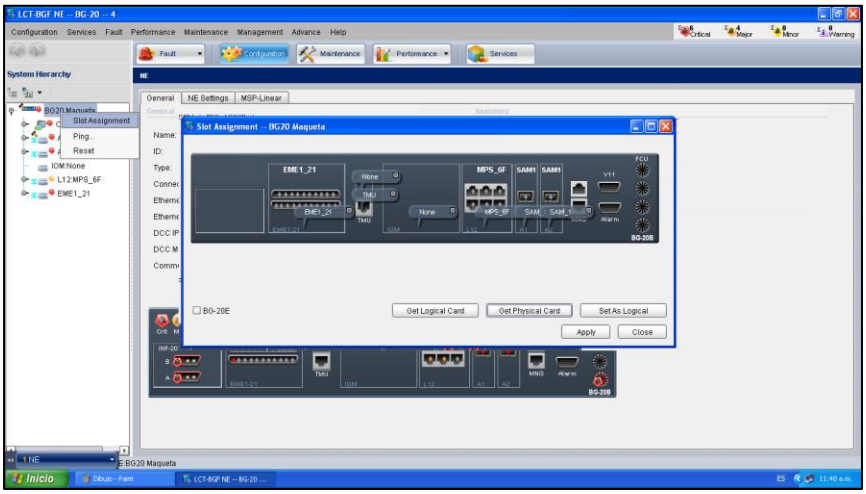


Figura 4.43: Verificación de tarjetas en equipo.

Para poder configurar los puertos ethernet del BG20, realizaremos los siguientes pasos, damos click sobre el menu izquierdo sobre la tarjeta L12MPS_6F, desplegamos dicho menu y damos click sobre el puerto FE-ETY port1, siempre en el menu de arriba en la opcion Configuration. Estando en esa ventana, tomaremos en cuenta lo siguiente:

- ✓ Port Enable: Enable
- ✓ Type: UNI
- ✓ Auto-Negotiation: enable
- ✓ Velocidad de los puertos en: 100 MHz Full y 10 MHz Full

Este mismo paso se realizara para los 6 puertos siguientes, si se desea utilizar todos los puestor fast ethernet. Figura 4.44.

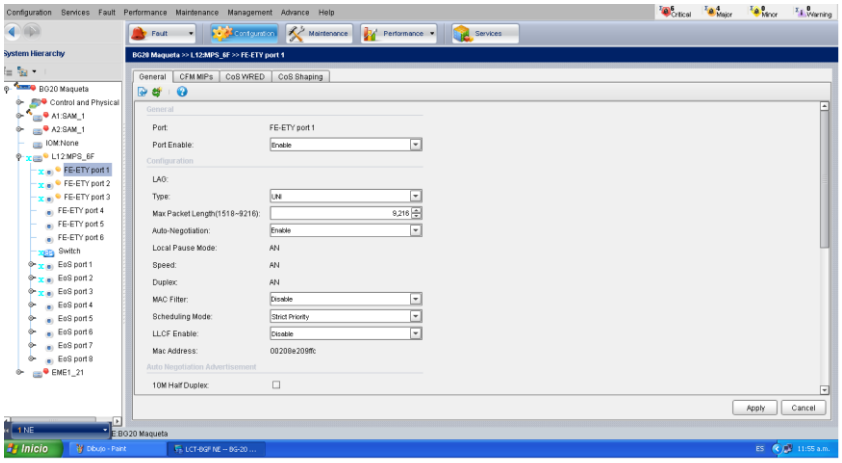


Figura 4.44: Configuración de los FE-ETY.

Para crear las WAN, EoS o asignarle el ancho de banda a los puertos realizaremos los siguientes pasos:
Sobre la tarjeta L12MPS_6F menu izquierdo y en Configuration menu de arriba, nos situamos en la opcion que dice EoS port1, damos click derecho y le damos en la opcion que dira Create VCG, al dar click en esa opcion nos aparecera la ventana que se muestra en la figura 4.45, en la parte izquierda de la figura tenemos los LCAS, en este caso desactivamos los LCAS, esto se da si en otro equipo, ya sea BG20 o HIT 7020 tienen desactivada esta opcion, en la parte derecha de la figura esta la pestaña Traffic tenemos la asignacion del ancho de banda o VC12, tomamos el primer EoS port1 y le damos 6(2Megax6Mega=12Mega). Este EoS port1 luego lo asociaremos con los 6 puertos fast ethernet.

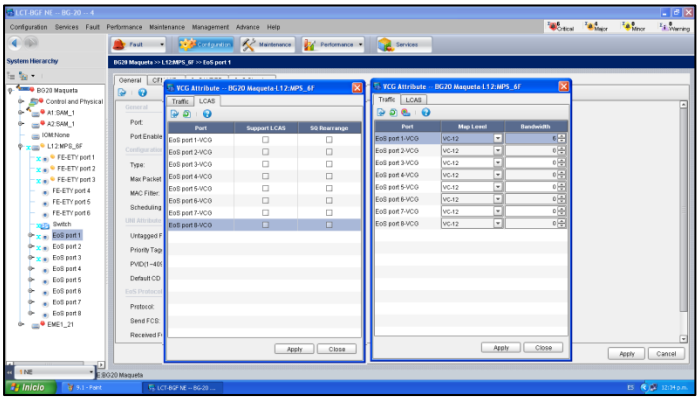


Figura 4.45: Creacion de Wans o EOS.

Para realizar las VLAN o SVI, se realizaran los siguientes pasos:

Siempre sobre el menú izquierdo, damos click en la opción que dice SWITCH y sobre el menú de arriba damos click en SERVICES, al dar click ahí nos aparece la ventana de la figura 4.46, damos click sobre VSI List y damos click en la opción Create VSI.

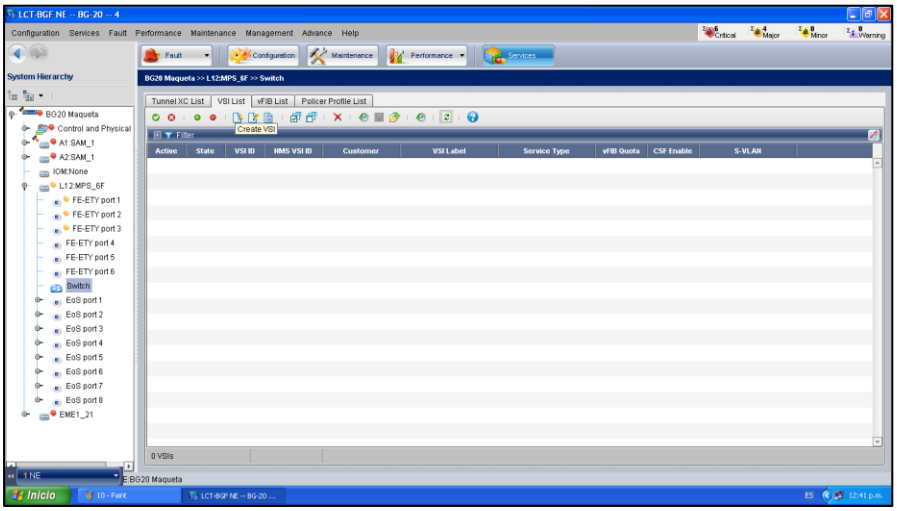


Figura 4.46: Creacion de Vlans o VSI.

Al dar click sobre Create VSI, nos aparecerá la ventana de la figura 10, para configurar las VLAN o VSI se realizaran los siguientes pasos:

- ✓ Service Type: PB MP+MP
- ✓ S-Vlan: 1 (Dependiendo que Vlan se configurara, caso hipotético, en la practica la Vlan a utilizar seria la 3221 para litespan voz y 3222 para gestión)
- ✓ Priority Mapping-UNI Ingress CoS Mapping- Map All Priorities to.
- ✓ vFIB Quot: 250.
- ✓ Se seleccionan los puertos a interactuar junto con el EoS configurado que era el EoS port1, y se crean los policer a como se verá en la figura 4.47.

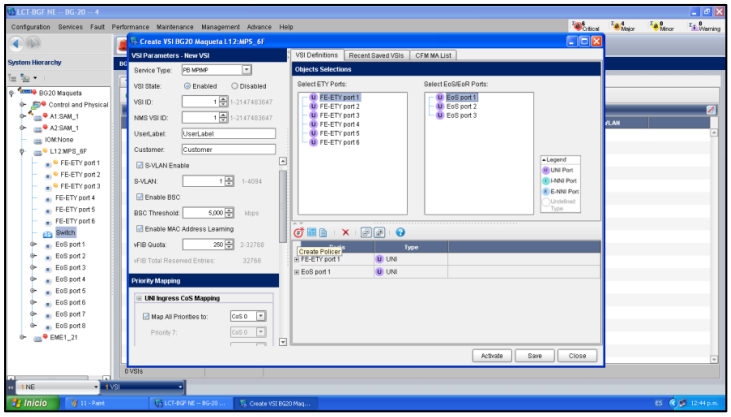


Figura 4.47: Creación de Policer Paso 1.

Sobre la pestaña de la figura 4.49 se dará click en la opción Create Policer, figura 4.48, se crearan 2 policer, el primero para los 6 puertos fast Ethernet y el segundo para el EoS. Se le dara elnombre a nuestro policer, en este caso será policer puertos y policer EoS, en el policer puertos la opción CIR la pondremos en 2000, repartidos los 12Mega de BW entre los 6 puertos y el el policer EoS el CIR será de 12000 que será el total del BW de los 6 puertos.

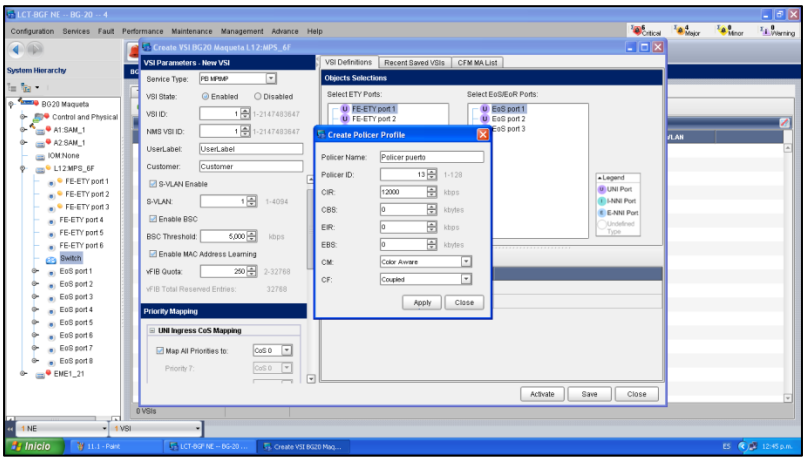


Figura 4.48: Creación de Policer Paso 2.

Al realizar los policer se veran a como se muestra en la figura 4.49. En la parte inferior se ven los 2 policer creados, en el policer FE-ETY port1, configuraremos 3 cosas, la primera sera que el puerto lo pondremos de modo untag o modo acceso, le agregaremos la Vlan que era la 1 y le daremos la opcion de priority & policer Mapping y buscamos elpolicer creado para los puertos, de esta misma manera configuraremos el policer para el EoS, launica diferencia es que no especificaremos la Vlan o C-VIDs.

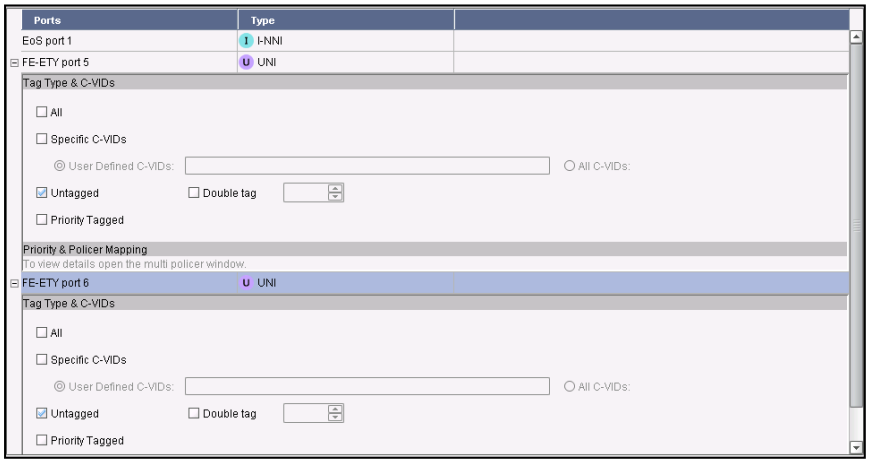


Figura 4.49: Configuración de los Policer.

Después de haber configurado los puertos Ethernet se procederá a efectuar las Cross-Conexiones. Para realizar las cross-conexiones se realizara lo siguiente:
Lo primero que se realizara en crear los VC 4 o contenedores virtuales, sobre el menú izquierdo nos dirigiremos al chasis y sobre el menú de arriba nos dirigiremos a la pestaña Services, estando ahí daremos en la opción que dice Create XC, sobre la opción que dice A1:SAM_1 desplegaremos y nos aparece la opción VC3#1, daremos click derecho y escogemos la segunda opción y damos click en Active, automáticamente nos aparece creado el VC4, para realizar las cross-conexiones en los puertos Ethernet, en la parte izquierda de la figura 13 se divide en 2 partes, la parte izquierda se muestran las tarjetas que usaremos como entrada y en la parte derecha se ven las trajetas que usaremos como salida, nos situamos en la parte izquierda y escogemos la tarjeta óptica o A1:SAM_1, desplegamos y nos aparecen los VC3 y desplegamos y nos aparecerán los VC12, escogemos uno y en la parte derecha de la ventana escogemos la tarjeta L12:MPS_6F, desplegamos y nos aparece los VCG, despegamos y nos aparecerán los VC12, escogemos uno y le damos activar, de esta manera se realizaran las XC, si queremos las XC en los puertos E1s solo nos dirigiremos a la tarjeta de E1s, recordando que los TU12 del HIT 7020 y los del Eci-BG20 deben de coincidir para que exista comunicación. Figura 4.50

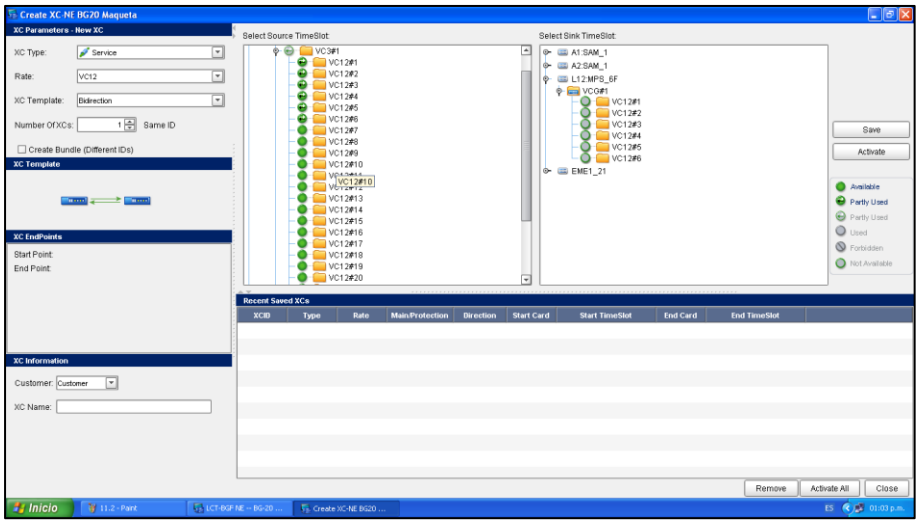


Figura 4.50: Creación de Cross-Conexiones.

4.6. Configuración de CISCO ASR 901.

La configuración de este equipo CISCO es un poco similar a la del equipo MWR. A continuación presentaremos los pasos a seguir.

Para configurar el equipo CISCO ASR 901, utilizaremos el programa Putty anteriormente usado en los equipos HIT7020 y CISCO MWR 2941 DC, nos conectaremos por consola al equipo CISCO y empezaremos a configurarlo. Se seleccionara el puerto COM que coincida con el puerto donde está conectado el conector RJ-45 a DB-9, cable azul de CISCO que utilizaremos para configurar el equipo

Configuración inicial:

Acceso a modos de configuración: Para ir al modo EXEC Privilegiado se introduce el comando "enable".

```
Router>enable
Router#
```

Para ir al modo Configuración Global: introducir "configure terminal" en el modo EXEC privilegiado (Este es un modo de configuración)

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Siempre desde modo de configuración le cambiaremos el nombre a nuestro equipo con el siguiente comando "hostname" seguido del nombre ASR_Maqueta.

```
Router(config)# hostname ASR_Maqueta
ASR_Maqueta(config)#
```

Para activar contraseña en el equipo ASR, siempre en el modo de configuración global ejecutamos el comando "enable secret" y el nombre de la contraseña, nuestra contraseña es cisco. Existen otras opciones de habilitar contraseñas como lo es mediante el comando "enable password".

```
ASR _Maqueta(config)#enable secret cisco
ASR _Maqueta(config)#
```

Para ir al modo de configuración de puertos (desde el modo de configuración global), Se accede con el comando "interface" espacio y el puerto o VLAN a configurar, una vez dentro del modo interface meteríamos los comandos a realizar para ese Puerto o VLAN.

```
ASR _Maqueta(config)#  interface GigabitEthernet0/0
ASR _Maqueta(config-if)#
```

Dentro de la configuración de puertos utilizaremos el comando "no negotiation auto", este comando sirve para que el puerto no pueda asignar una determinada velocidad.

```
ASR _Maqueta (config-if)# no negotiation auto
ASR _Maqueta (config-if)#
```

Utilizaremos el comando "cdp enable" para poder tener información de los demás equipos equipos IP que podrían estar conectados localmente, este protocolo es propietario de CISCO.

```
ASR _Maqueta (config-if)# cdp enable
ASR _Maqueta (config-if)#
```

El comando "service instance" define la instancia de servicio. El número es arbitrario; no tiene nada que ver con las VLAN que se procesarán por este particular, Servicio Instancia La palabra clave " Ethernet " se utiliza siempre, y se ejecuta de esta manera.

```
ASR _Maqueta (config-if)# service instance 1 ethernet
ASR _Maqueta (config-if)#
```

El comando "encapsulation dot1q 1" define la forma en que asignar una etiqueta de entrante a una instancia de servicio, se ejecuta de esta forma.

```
ASR _Maqueta (config-if)# encapsulation dot1q 1
ASR _Maqueta (config-if)#
```

El comando "rewrite ingress tag pop 1 symmetric" realiza la acción de desprenderse de la etiqueta de entrada, antes de ser enviada, en este caso se eliminara la etiqueta 1, este comando es opcional, se ejecuta de la siguiente manera.

```
 ASR _Maqueta (config-if)# rewrite ingress tag pop 1 symmetric
ASR _Maqueta (config-if)#
```

Para finalizar de configurar el puerto utilizamos el comando "bridge-domain" este comando sirve para tener más flexibilidad en los EVCs (Circuitos Virtuales Ethernet). Un dominio Bridge es lo que se piensa tradicionalmente como una Capa 3 SVI. A diferencia de las etiquetas VLAN que están siendo procesados por los EVCs configurados puente - dominios no requerir la VLAN que ser configurado a nivel mundial sobre los recursos de ancho de dispositivos y el uso de la plataforma. Se ejecuta de la siguiente manera.

```
ASR _Maqueta (config-if)#  bridge-domain 1
ASR _Maqueta (config-if)#
```

La configuración del puerto Gigabit Ethernet 0/2 es similar lo único que cambiara será la forma de encapsulación que será de tipo untag o de acceso. A continuación se muestra la configuración del puerto.

```
ASR _Maqueta(config)# GigabitEthernet0/2
ASR _Maqueta (config-if)# no negotiation auto
ASR _Maqueta (config-if)# service instance 2 ethernet
ASR _Maqueta (config-if)# encapsulation untagged
ASR _Maqueta (config-if)#  bridge-domain 2
ASR _Maqueta (config-if)#  exit
```

A continuación presentaremos el Scrip del equipo CISCO ASR 901, como es una maqueta a nivel de laboratorio solo habilitamos 2 puertos del equipo, el puerto Gigabit Ethernet 0/0 y el puerto Gigabit Ethernet 0/2. Esto se muestra en la figura 4.51.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname ASR_Maqueta
ASR_Maqueta(config)#enable secret cisco
!
ASR_Maqueta(config)# interface GigabitEthernet0/0
ASR_Maqueta (config-if)#no negotiation auto
ASR_Maqueta (config-if)# cdp enable
ASR_Maqueta (config-if)# service instance 1 ethernet
ASR_Maqueta (config-if)# encapsulation dot1q 1
ASR_Maqueta (config-if)#rewrite ingress tag pop 1 symmetric
ASR _Maqueta (config-if)#  bridge-domain 1
ASR_Maqueta (config-if)#exit
!
interface GigabitEthernet0/1
 no negotiation auto
!
ASR_Maqueta # configure terminal
ASR_Maqueta (config)# interface GigabitEthernet0/2
ASR_Maqueta (config-if)# no negotiation auto
ASR_Maqueta (config-if)#service instance 2 ethernet
ASR_Maqueta (config-if)#encapsulation untagged
ASR_Maqueta (config-if)#bridge-domain 2
ASR_Maqueta (config)# exit
```

Figura 4.51-Scrip de configuración de CISCO ASR 901.

Al terminar de configurar el equipo HIT7020, ECI-BG20 y CISCO ASR 901, se realizaron las 2 pruebas logrando resultados satisfactorios, prueba de E1s entre multiplexores y ping extendido entre extremos de la maqueta a continuación se presenta en la imagen 4.52 el ping satisfactorio de una de las computadoras portátiles de extremo a extremo de la maqueta y en la figura 4.53 se presenta el resultado de ok de la prueba de E1s.

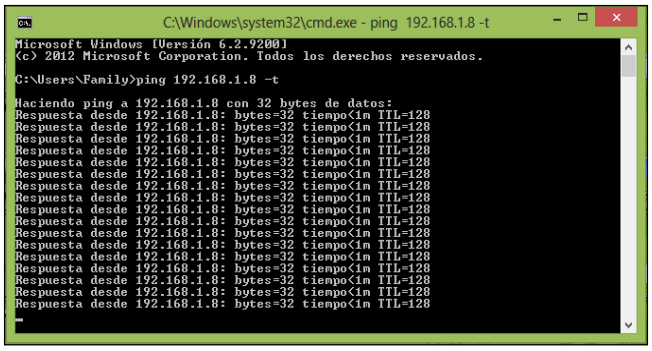


Figura 4.52-Ping realizado de una pc a otra pc conectada a los extremos de la maqueta.

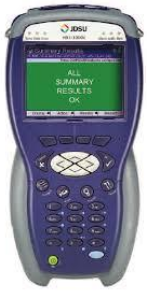


Figura 4.53 Prueba de E1s en multiplexores

CAPÍTULO IV.

5. Resultado y Discusión.

5.1. Descripción del Capítulo

En esta parte se hará una recopilación de la forma en la cual los equipos multiplexores SDH y equipo IP fueron conectados físicamente, se describirá los tipos de prueba que se realizaron al terminar de configurar la maqueta a escala de laboratorio, se determinara el tipo de configuración más adecuada para transportar paquetes de datos en una red de transporte mixta y se abordara que ventajas y desventajas presenta una red al implementar ambas tecnologías.

5.2. Conexión Física de Equipos Multiplexores Surpass HIT-7020, Eci BG-20 y Equipo CISCO

Antes de empezar a realizar la conexión de los equipos de baja jerarquía lo que se realizo fue la posición de cada equipo. En la figura 4.5 del capítulo III de esta tesis monográfica se observa la posición en la que están los equipos que componen dicha maqueta a escala de laboratorio, primero posicionamos el equipo SURPASS HIT-7020, luego se puso al equipo Eci BG-20 y como extremo se dejó al equipo CISCO, decidimos posicionar de esta manera a los equipos por comodidad al configurar, pero se pudo haber posicionado de cualquier manera. (Ver Figura 4.5 capitulo III)

Después de haber posicionado los equipos procedimos a conectarlos físicamente, la conexión en los equipos multiplexores con tecnología SDH se realizó mediante patchcord de fibra óptica de 5 metros con conectores LC a ambos lados de la fibra, dicha fibra va conectada a los puertos ópticos del equipo HIT 7020 y Eci BG-20, en dichos puertos ópticos pusimos transceptores SFP (small form-factor pluggable transceptor), con capacidad STM-1 con alcance de 15 km, se encuentra dentro de la ventana de los 1310 nm, en la parte de recepción de los SFP se colocó un atenuador de 5dB para evitar que los transceptores se dañen debido a la corta distancia entre los equipos.

La conexión de los equipos con tecnología SDH al equipo CISCO fue mediante cable Ethernet plano. El equipo CISCO posee entradas para SFP, en este caso no serán utilizadas ya que no poseemos transceptores para equipos CISCO.

5.3. Resultado de las pruebas realizadas en la maqueta.

Al terminar de realizar las conexiones físicas en los equipos procedimos a la configuración lógica de la maqueta, dicha configuración se puede observar en el capítulo III de esta tesis monográfica, ya configurada la maqueta efectuamos las pruebas de conexión entre los equipos, realizamos 2 tipos de prueba con el fin de demostrar la compatibilidad de ambas tecnologías y la posible interoperabilidad de las tecnología LTE, 2G y 3G dentro de la misma red de transporte, estas pruebas normalmente son las que se realizan en los sitios donde se encuentran instalados estos equipos. La primer prueba consistía en hacer conexión de E1s entre el Suprass HIT7020 y BG20, en dicha prueba se utilizó un conector RJ-45 que lo utilizamos como bucle, para que el conector RJ-45 sirviera como bucle utilizamos los pines 1-4 y 2-5, el ping 1-2 es transmisión y ping 4-5 es recepción, esto dependerá de la fabricación del equipo; al otro extremos usamos un equipo ACTERNA HST-3000C para cerrar el bucle de E1s , este equipo se conectó al HIT 7020 mediante un cable Ethernet cruzado. Esta prueba se realizó solamente en equipos con tecnología SDH ya que el equipo CISCO no posee puertos para E1s.

La segunda prueba que se realizo fue verificar la conexión Ethernet de los equipos HIT7020, BG20 y CISCO, se configuraron 2 pc dentro del mismo segmento de red y se hizo un ping extendido entre las computadoras portátiles.

5.4. Retos en la configuración realizada en la maqueta.

Al realizar las configuraciones lógicas en los equipos HIT 7020, ECI BG20 y CISCO ASR 901 se tuvo pequeños inconvenientes al interconectar dichas tecnologías. Para solucionar ese problema el puerto Ethernet número 1 del BG20 se configuro en modo troncal al igual que el puerto GigaBit Ethernet del ASR 901 y en el puerto donde se conectarían los servicios o en este caso la PC se tenía que configurar en modo Acceso. Con este pequeño inconveniente se llegó a la conclusión que la única forma de configuración lógica para interconectar estas dos tecnologías es de esta manera.

Dentro de la red de transporte existen 3 tipos de configuraciones físicas o topologías de red, topología lineal que se utilizó en esta tesis, topología de malla y topología en anillo. Las configuraciones realizadas en esta maqueta funcionan en cualquier topología.

Se decidió utilizar la topología línea en esta tesis debido a su sencillez de instalación y su valor económico, una topología lineal es más económica que cualquiera de las dos topologías anteriormente mencionadas (topología de anillo y topología en malla).

La única restricción en la topología lineal es relacionada con el aspecto físico y de tráfico (máxima longitud del anillo y número de dispositivos). Además, los fallos se

pueden aislar de forma sencilla. Generalmente, en un anillo hay una señal en circulación continuamente.

5.5. Ventajas y Desventajas en la Implementación de ambas tecnologías tecnología SDH y tecnología IP.

En el capítulo II de esta tesis monográfica se efectuó un análisis de manera individual de las ventajas y desventajas que tenían estas tecnologías (SDH-IP), en esta sección haremos un pequeño análisis de estas tecnologías pero de manera conjunta.

Ventajas

SDH sobre IP puede proporcionar un mejor servicio teniendo en cuenta que la velocidad de los modernos equipos IP, usando MPLS es posible enviar los datagramas IP a SDH eliminando el overhead de ATM.

El SDH forma un enlace punto a punto entre los enrutadores IP por lo que utiliza el protocolo PPP[30] lo cual proporciona encapsulamiento y transferencia de paquetes desde múltiples capas de red sobre un mismo enlace físico, establecimiento, configuración y monitoreo de la conexión del nivel del enlace, determina y configura los protocolos de nivel de red, y no existe encabezado ATM.

Desventajas

Aunque la tecnología SDH sobre IP es viable su aplicación es reducida al envío de datos de alta capacidad, ya que SDH solo puede operar en el modo de punto a punto y esto causa que no existan circuitos virtuales, no existan ingeniería de tráfico y la ruta del trafico sea manejada por el IP.

---

30 Protocolo Punto a Punto es un protocolo de nivel de enlace de datos, estandarizado en el documento Request For Comments *1661 (RFC 1661). Comúnmente usado para establecer una conexión directa entre dos nodos de una red de computadoras.*

6. Conclusión.

Con el incremento de equipos móviles, la demanda de mayor ancho de banda para transmitir más cantidad de tráfico de datos, calidad de servicio y el auge de LTE (Long Term Evolution) etc., se necesita una tecnología de transporte que solucione estas nuevas exigencias por parte de los usuarios en la red, es por esta razón que se han venido implementando estrategias y soluciones para tratar de encontrar una tecnología que soporte estas exigencias.

Por esta razón este proyecto de tesis monográfica tiene como objetivo principal Implementar a escala de laboratorio una red de transporte mixta basada en tecnología SDH (Synchronous Digital Hierarchy) y tecnología IP (Internet Protocol) utilizando equipos de baja jerarquía.

En esta tesis se demostró la configuración necesaria para que ambas tecnologías puedan trabajar en conjunto dentro de una red de transporte, ya que realizar cambios bruscos en una red que nació con tecnología SDH generaría una gran inversión para las empresas de telecomunicaciones, migrar de manera pausada la red de transporte a FULL IP sería lo más ideal.

Se realizaron dos tipos de pruebas de conexión entre equipos que haría un ingeniero de campo en un entorno real, la primera prueba fue probar los puertos E1s de los multiplexores y la segunda prueba fue realizar un ping extendido en los extremos de la maqueta con dos computadoras portátiles.

Hablamos sobre las ventajas y desventajas de usar tecnología mixta SDH-IP dentro de la red de transporte, llegando a la conclusión que la mayor ventaja es usar la red ya existente (SDH) para integrar la tecnología IP y la peor desventaja es la limitante del ancho de banda por parte de la tecnología SDH.

Esta tesis monográfica se limitó a configurar los equipos de transporte para que existieran conexiones entre ellos. Existen otras configuraciones para brindar servicios, pero se requiere de otros equipos para poder interconectarlos.

6. Recomendaciones.

Para llevar a cabo una evolución de la red a All IP se tendría que utilizar servicios carrier Ethernet como tecnología de transporte de capa 2. Se utilizarían principalmente radioenlaces Ethernet.

Dado los niveles de inversión de recursos económicos y humanos que supone el despliegue y mantenimiento de una red extensa, el proceso de migración tiene que hacerse de forma gradual y progresiva, optimizando el uso que se hace de los equipos y espectros ya disponibles. Como dato orientativo se podría decir que realizar esta transformación en redes del tamaño de Nicaragua, podría constar un operativo de varios años (2-4 años) y varios miles de millones de dólares. En lo que se refiere a recursos humanos, será necesario el trabajo de numerosos ingenieros de transmisión, técnicos de O&M instaladores, instaladores, implantadores, subcontratas, así como personal encargado de elaborar presupuestos, informes de gastos, estadísticas etc.

Con esto en mente se puede considerar la migración a ALL IP de la siguiente manera:

Desplegar una red troncal MPLS para reemplazar a la infraestructura ATM. El tráfico de los nodos B ATM debe migrarse en ese momento hacia la nueva red MPLS, lo que se hara mediante pseudowire (PWE3) de nivel 2.

Durante el proceso de migración, las estaciones GSM TDM pueden introducirse en la red MPLS (que atravesaran de forma transparente mediante PWE) o bien pueden conservar sus rutas a través de la red SDH hasta llegar a las BSCs.

El siguiente paso sería comenzar el despliegue de la red Ethernet sustituyendo a PDH. Como criterio de partida puede empezarse por sustituir los enlaces entre equipos MPLS que agregan el tráfico de muchos nodos b.

A la hora de diseñar radioenlaces Ethernet se le asigna un canal de un cierto ancho de banda que determinara la capacidad de los mismos.

Cuando sea viable se tratara de llegar con fibra óptica a los equipos IP y a equipos que permitan fibra al nodo. Esto es habitual en las ciudades y núcleos urbanos que disponen de fibra óptica instalada en múltiples puntos.

Los nodos Full-IP una vez configurada disponen de la misma capacidad en downlink y uplink, siendo esta mayor que la obtenida mediante trafico TDM: máximo 8xE1s y hasta 100 Mbps en IP.

7. Bibliografía.

[1] http://www.ecologistasenaccion.org/article2157.html

[2] http://www.diffen.com/difference/Capex_vs_Opex

[3] *Las telecomunicaciones de la nueva generación*

[4] *http://www.itu.int/*

[5] *http://www.monografias.com/*

[6] *Oportunidades de negocio en el sector de las Tecnologías de Información y Comunicaciones Un estudio del sector TIC, preparado para Danida, por la Federación Danesa de Pequeñas y Medianas Empresas en colaboración con Ricardo Castillo Arguello.*

[7] *Tecnologías de la información y la comunicación en NicaraguaTecnologías de la información y la comunicación en Nicaragua*

[8] *http://www.gobenic.gob.ni/eventos/interoperabilidad/presentaciones/fibraoptica%20Enatrel.ppt http://www-entel.upc.es/rvidal/jitel01.pdf*

[10] http://www.academia.edu/6150230/Presente_y_Futuro_de_las_comunicaciones_%C3%B3pticas_en_Colombia_abril_2012

[11] *Evolución de las redes de transporte hacia la integración de servicios.*

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

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

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

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

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

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

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

[19] *Las Telecomunicaciones de Nueva generación, Telefonica,Direccion General de Desarrollo del Negocio.*

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

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

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

[23] *McBride, R. D. Awduche et al. "Requirements for Traffic Engineering over MPLS".*

ANEXOS.

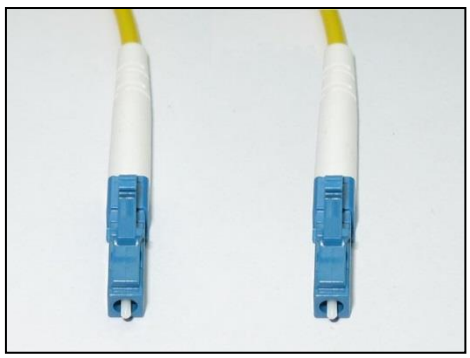
ANEXO A.

(Equipos con Tecnología SDH E IP)

Idu de Radio Minilink

Equipo ACTERNA HST 300c
Realiza pruebas de trama ethernet y de E1s

Equipo HIT 7070, Alta Jerarquia



Pachcord de fibra LC- para STM-N

Shelter Huawie para equipos IP

BTS LTE

Protector de Linea para Cable Ethernet

Radio Ipasolink 200

ANEXO B.

(Características y Configuración de CISCO MWR 2941 DC)

CISCO MWR 2941

El Cisco MWR 2941 es una plataforma de acceso a la sede celular específicamente diseñado para optimización, agregado, y el transporte de la red de radiofrecuencia (RAN). Permite a los operadores de servicios inalámbricos a reducir sus gastos de manera significativa.

El Cisco MWR 2941 es una tecnología rentable para desplegar nuevas tecnologías de radio como Sistema universal de telecomunicaciones móviles (UMTS) / High Speed Packet Access (HSPA) / Long Term Evolution (LTE) y WiMAX redes de voz y datos ; es capaz de generar ingresos a partir de la nueva sede celular IP basado en servicios; y facilitar el rápido despliegue de los servicios móviles de próxima generación.

El Cisco MWR 2941 ayuda a habilitar una variedad de soluciones RAN extendiendo la conectividad IP para Sistema Global para Comunicaciones Móviles (GSM) / Servicio General Packet Radio (GPRS) / Velocidades de Datos Mejoradas para la Evolución de GSM (EDGE) estaciones de transceptor base (BTS) , UMTS / HSPA / LTE Nodos B , Code Division Multiple Access (CDMA) / CDMA - 2000 / EVDO BTS , WiMAX BTS. Transporta de manera eficiente datos y tráfico de señalización sobre IP utilizando circuitos T1 / E1 tradicionales, incluyendo línea arrendadas, microondas y satélite, así como las redes de backhaul alternativas, incluyendo portadoras Ethernet , DSL y WiMAX . También es compatible con los estándares basados en Internet Engineering Task Force (IETF) Protocolos de Internet más de la red de transportes RAN. , incluidos los referidos a las de tercera generación.

4.3.2.3.1 Características.

- Descripción General del Hardware.

✓ BackPlane TDM.
✓ Distribución de reloj común a través del chasis.
✓ Panel Frontal de Acceso eIndicadores deLED.
✓ 16 Puertos Integrados RJ- 45 T1/E1.
✓ Cuatro puertos integrado RJ – 45 con capacidad de 100 / 1000BASE –T.
✓ Dos Puertos SFP Small Form Factor con capacidad 1000BASE - X.
✓ Puertos Auxiliares integrados de 115.2 Kbps.
✓ Construido para Capa 2 de GigaBit Ethernet y soporta el cambio de tráfico de línea.
✓ 512 MB de DRAM y 128 MB de memoria flash externa.
✓ Posee 2 fuentes de alimentación DC y se alimenta a (±) 20 o 60 V DC.

- Descripción general del software

El software para el Cisco MWR 2941 está adaptado para transporte IP RAN e incluye varios Cisco IOS Software, características desarrolladas específicamente para este tipo de aplicaciones. Estas características incluyen Recuperación Adaptable de Reloj, IEEE 1588-

2008, el UIT-T Synchronous Ethernet, ATM y TDM IETF.

El software que implementa el equipo Cisco MWR 2941 es el Pseudowire Emulation (PWE), es el que define el transporte de servicio en la capa 2 a través de una red MPLS, pseudowires han estado en existencia por casi una década, principalmente en el núcleo y el borde de la red, típicamente el transporte de ATM y Frame Relay tráfico sobre una red IP portadora.

Para la utilización de Pseudowire Emulation se recomiendan tres criterios, el tipo de servicio, el ancho de banda y que tipo de tecnología que se usara. En el tipo de servicio a ofrecer se basa en E1/T1 o 64 E1/T1, el ancho de banda es limitado y solo se puede utilizar en entornos donde pueda soportar la carga como por ejemplo DSL, esto se debe a que pseudowire de tipo TDM es más simple y eficiente sin mucha sobrecarga y transportando paquetes más pequeños, si la portadora llevaría una mezcla de servicios y se intentaría reducir el número de tecnologías a usar TDMoIP es la pseudowire mas capaz de transportar todo tipo de servicio TDM. En la figura 1 podemos ver el Cisco MWR 2941 y en la figura 2 observamos la ubicación de Cisco MWR 2941 en una red.

Figura 1: Cisco MWR 2941

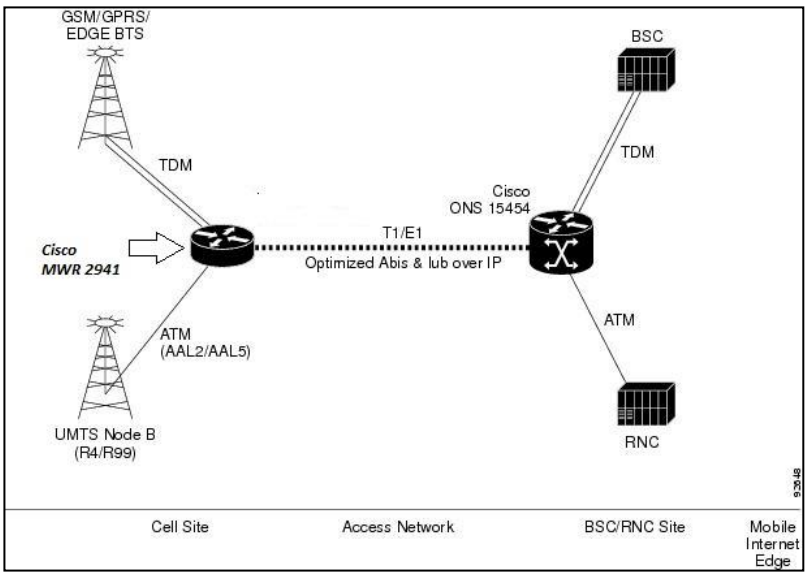


Figura 2: Uso Cisco MWR 2941

Configuración de CISCO MWR 2941 DC.

Para configurar el equipo CISCO MWR 2941 DC, utilizaremos el programa Putty anteriormente usado en los equipos HIT7020, nos conectaremos por consola al equipo CISCO y empezaremos a configurarlo. Se seleccionara el puerto COM que coincida con el puerto donde está conectado el conector RJ-45 a DB-9, cable azul de CISCO que utilizaremos para configurar el equipo

Configuración inicial:

Acceso a modos de configuración: Para ir al modo EXEC Privilegiado se introduce el comando "enable".

```
Router>enable
Router#
```

Para ir al modo Configuración Global: introducir "configure terminal" en el modo EXEC privilegiado (Este es un modo de configuración)

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Siempre desde modo de configuración le cambiaremos el nombre a nuestro equipo con el siguiente comando "hostname" seguido del nombre MWR_Maqueta.

```
Router(config)# hostname MWR_Maqueta
MWR_Maqueta(config)#
```

Para activar contraseña en el equipo MWR, siempre en el modo de configuración global ejecutamos el comando "enable secret" y el nombre de la contraseña, nuestra contraseña es cisco. Existen otras opciones de habilitar contraseñas como lo es mediante el comando "enable password".

```
MWR_Maqueta(config)#enable secret cisco
MWR_Maqueta(config)#
```

Para ir al modo de configuración de puertos (desde el modo de configuración global), Se accede con el comando "interface" espacio y el puerto o VLAN a configurar, una vez dentro del modo interface meteríamos los comandos a realizar para ese Puerto o VLAN.

```
MWR_Maqueta(config)# GigabitEthernet0/2
MWR_Maqueta(config-if)#
```

Para configurar un puerto troncal sin filtro o sin asignar una vlan en específico para dejar pasar las vlan de la 1-4094 que posee el MWR se realiza con el comando "switchport mode trunk". Esa configuración se hace para manejar el tráfico de diferentes Vlans, esto se utiliza para interconectar diferentes equipos, como lo es el caso de esta maqueta.

```
MWR_Maqueta (config-if)#switchport mode trunk
```

Para configurar el tipo de velocidad y operación del puerto se ejecutan los siguientes comandos "speed" y la velocidad a la cual se dejara el puerto, esta puede ser auto/1000/100 en nuestro caso la dejaremos en 100 y el comando "duplex" y la manera en que dejaremos el puerto, puede ser auto/half/full, en nuestro caso se dejó full.

```
MWR_Maqueta (config-if)# speed 100
MWR_Maqueta (config-if)# duplex full
```

A continuación para encender la interface configurada se ejecuta el comando "no shutdown" y el comando "exit" para salir del modo de configuración de puerto.

```
MWR_Maqueta (config-if)# no shutdown
MWR_Maqueta (config-if)#exit
```

Esta misma configuración se le realizara al puerto Gigabit Ethernet 0/3 del MWR, y se presenta a continuación.

```
MWR_Maqueta(config)# GigabitEthernet0/3
MWR_Maqueta (config-if)#switchport mode trunk
MWR_Maqueta (config-if)# speed 100
MWR_Maqueta (config-if)# duplex full
MWR_Maqueta (config-if)# no shutdown
MWR_Maqueta (config-if)#exit
```

Para los puertos Gigabits Ethernet 0/4 y Gigabits Ethernet 0/5 se realizara la misma configuración que los 2 puertos anteriormente citados, con la única diferencia que los puertos Gigabits Ethernet 0/4 y Gigabits Ethernet 0/5 se configuraran para modo acceso con el comando "switchport mode access", esto se debe a que no se espera recibir tráfico que haga referencia a alguna Vlan, ya que estos puertos van a conectarse a dispositivos finales normales, en este caso una pc. A continuación veremos los comandos que se ejecutan en cada puerto.

```
MWR_Maqueta # configure terminal
MWR_Maqueta (config)# interface gigabitethernet 0/4
MWR_Maqueta (config-if)#switchport mode access
MWR_Maqueta (config-if)#speed 100
MWR_Maqueta (config-if)#duplex full
MWR_Maqueta (config-if)# no shutdown
MWR_Maqueta (config)# exit
!
!
MWR_Maqueta # configure terminal
MWR_Maqueta (config)# interface gigabitethernet 0/5
MWR_Maqueta (config-if)#switchport mode access
MWR_Maqueta (config-if)#speed 100
MWR_Maqueta (config-if)#duplex full
MWR_Maqueta (config-if)# no shutdown
MWR_Maqueta (config)# exit
```

En la siguiente imagen presentamos el scrip completo para el equipo CISCO MWR 2941 DC. Figura 3

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# hostname MWR_Maqueta
MWR_Maqueta(config)#enable secret cisco
!
MWR_Maqueta(config)# GigabitEthernet0/2
MWR_Maqueta (config-if)#switchport mode trunk
MWR_Maqueta (config-if)# speed 100
MWR_Maqueta (config-if)# duplex full
MWR_Maqueta (config-if)# no shutdown
MWR_Maqueta (config-if)#exit
!
MWR_Maqueta(config)# GigabitEthernet0/3
MWR_Maqueta (config-if)#switchport mode trunk
MWR_Maqueta (config-if)# speed 100
MWR_Maqueta (config-if)# duplex full
MWR_Maqueta (config-if)# no shutdown
MWR_Maqueta (config-if)#exit
!
MWR_Maqueta # configure terminal
MWR_Maqueta (config)# interface gigabitethernet 0/4
MWR_Maqueta (config-if)#switchport mode access
MWR_Maqueta (config-if)#speed 100
MWR_Maqueta (config-if)#duplex full
MWR_Maqueta (config-if)# no shutdown
MWR_Maqueta (config)# exit
!
MWR_Maqueta # configure terminal
MWR_Maqueta (config)# interface gigabitethernet 0/5
MWR_Maqueta (config-if)#switchport mode access
MWR_Maqueta (config-if)#speed 100
MWR_Maqueta (config-if)#duplex full
MWR_Maqueta (config-if)# no shutdown
MWR_Maqueta (config)# exit
```

Figura 3-Scrip de configuración de CISCO MWR 2941 DC.