UNIVERSIDAD POLITECNICA SALESIANA

SEDE CUENCA

FACULTAD DE INGENIERÍAS

CARRERA DE INGENIERÍA ELECTRÓNICA

Tesis previa a la obtención del Título de Ingeniero Electrónico

"ESTUDIO DE MIGRACIÓN DE LA RED PDH DE LA III ZONA MILITAR A UNA RED METRO ETHERNET BASADA EN TECNOLOGÍA IP/MPLS"

AUTORES:

Manuel Salvador Pomaquiza Urgiles

Edwin Faustino Mora Mejía

DIRECTOR:

Ingeniero Jhonatan Coronel

Cuenca, 04 Febrero de 2012

DEDICATORIA

Dedico este proyecto de tesis a Dios y a mis padres. A Dios porque ha estado conmigo en cada paso que doy, cuidándome y dándome fortaleza para continuar, a mis padres, Honorio y Rosa quienes a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en todo momento, depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en mi inteligencia y capacidad. Es por ellos que soy lo que soy ahora. Los amo con toda mi vida.

A mis hermanos Lilian, Freddy y Carlos, los cuales han sido pieza fundamental en mi formación primero como persona y luego como profesional, dándome el ejemplo de perseverancia, constancia y honradez. El cariño y el amor que me han entregado durante todos los años de mi vida se ven reflejados hoy con este logro tan importante para mí.

Manuel Salvador

DEDICATORIA

La concepción de este proyecto está dedicada a mis padres, Fausto y Blanca, pilares fundamentales en mi vida. Sin ellos, jamás hubiese podido conseguir lo que hasta ahora. Su tenacidad y lucha insaciable han hecho de ellos el gran ejemplo a seguir y destacar, no solo para mí, sino para mis hermanos y familia en general. También dedico este proyecto a mi novia, mi inspiración, Belén. Ella representó un gran soporte sentimental en mis momentos de decline y cansancio. A ellos este proyecto, que sin ellos, no hubiese podido ser.

.

Edwin Faustino

AGRADECIMIENTO

Este proyecto es el resultado del esfuerzo conjunto de todos los que colaboraron con ideas, propuestas y soluciones. Por esto agradecemos a nuestro director de tesis, Ing. Jhonatan Coronel. Un agradecimiento general a los docentes de la Universidad Politécnica Salesiana y a sus aportes de información muy valiosa. Un agradecimiento al Ing. Patricio Álvarez el cual fue el mentalizador del tema de tesis, su visión profesional hizo que se desarrolle este tema que creemos servirá para que la institución en la cual ejecutamos el mismo, tome la alternativa más adecuada en cuanto a la implementación a corto plazo. Un agradecimiento especial y muy grato al Ingeniero Fabián Carvajal Jefe del Departamento de Troncalizado de la III Zona Militar quien nos brindó todas las facilidades para realizar el estudio, guiándonos de principio a fin en el desarrollo del trabajo.

Manuel Salvador y Edwin Faustino

DECLARACIÓN DE AUTORÍA

Nosotros, Manuel Salvador Pomaquiza Urgiles y Edwin Faustino Mora Mejía, alumnos de la Universidad Politécnica Salesiana, Facultad de Ingenierías de la Carrera de Ingeniería Electrónica, libres y voluntariamente DECLARAMOS que el presente proyecto ha sido elaborado en su totalidad por nuestras personas, asumiendo la responsabilidad de la autoría. El presente documento ha sido preparado como requerimiento del título de ingeniero Electrónico.

Cuenca, 04 de Febrero del 2012

---------- ----------

Manuel Salvador Pomaquiza Urgiles Edwin Faustino Mora Mejía

CERTIFICACIÓN

Yo, Jhonatan Coronel, docente de la Universidad Politécnica Salesiana, Facultad de Ingenierías de la Carrera de Ingeniería Electrónica, libre y voluntariamente CERTIFICO que el presente proyecto ha sido dirigido en su totalidad por mi persona. El presente documento ha sido preparado como requerimiento del Título de ingeniero Electrónico.

Cuenca, 04 de Febrero del 2012

Jhonatan Coronel

INTRODUCCIÓN

En la Actualidad las Instituciones Privadas (Operadoras) y Estatales poseen redes de transporte de datos a través de Radio Enlaces, como CNT, Claro, Telefónica y este caso puntual las Fuerzas Militares Terrestres, estos sistemas de Transmisión fueron montados ya hace varios años, la Red Militar fue implementada hace 10 años y por su funcionamiento continuo presenta ya inestabilidad de operación, caídas de servicio, etc.

El objetivo de este estudio en primera instancia, es proponer una Actualización (Migración) de la Tecnología de Red Militar, para reemplazar el sistema anterior ya deteriorado y obsoleto, por uno con mayor capacidad y con tecnología Actual. Luego elaborar un nuevo diseño de Red, el cual pueda garantizar una plataforma que soporte las aplicaciones y beneficios de MPLS (Multiprotocol Label Switching), esto con la visión de implementar una convergencia de servicios (voz, datos y video), sobre la misma red.

En el capitulo 1 y 2 se presenta un análisis de las Tecnologías de Transporte y Acceso, se repasan conceptos y características principales de cada uno de los vertiginosos avances que ha tenido las Telecomunicaciones como tal a través de los años. Se presenta un capitulo completo detallado a cerca de la topología de Red a diseñar (Metro Ethernet) y a cerca de la Tecnología a implementar sobre esta Red (MPLS).

En el siguiente capítulo se presenta el diseño de la Red MetroEthernet propuesto, con todas las características geográficas, funcionales e ingenieriles de sus puntos de conexión. Se hace un análisis y cálculo del tráfico a cursar por la red, según los requerimientos de ancho de banda de cada servicio a implementar. Por último se realiza el establecimiento y dimensionamiento de la Red según las aplicaciones MPLS (VRFs) que se pueden generar en la plataforma diseñada, todo esto según los servicios de exclusividad de tráfico a incluir en la misma.

ÍNDICE

CAPITULO 1

ESTUDIO DE LAS DIFERENTES TECNOLOGÍAS EXISTENTES

1.1. ESTUDIO COMPARATIVO ENTRE LAS PRINCIPALES TECNOLOGÍAS DE TRANSPORTE Y ACCESO.

1.1.1. INTRODUCCIÓN

Las Telecomunicaciones hacen posible el intercambio de información entre estaciones diferentes de una empresa o institución, ya sea esta comunicación a escala nacional como internacional, integrando (convergencia) varios servicios en una misma red, especialmente diseñada para cubrir sus necesidades, todo esto acorde y paralelo al avance de la tecnología.

En telecomunicaciones se distingue una infraestructura de transporte y otra de acceso, sobre las que se montan los distintos servicios que se ofrecen, ha sido una evolución notable de las redes de transporte y acceso a través de los años, vamos a estudiar cómo ha ido escalando la tecnología en este aspecto. La convergencia de servicios (voz, datos, video, etc.) utilizando un mismo canal digital de comunicación ha sido la meta desde el principio, y a partir de esto se ha ido desarrollando las diferentes arquitecturas y diseños de red. Es de mucha importancia estudiar estas tecnologías, analizar sus características y asociarlas después en una síntesis comparativa enfocada a los servicios que ofrecen. Este proyecto se sostiene específicamente en el resultado del crecimiento evolutivo de las arquitecturas de transporte de información que han dado lugar a comunicaciones con conexiones de muy altas prestaciones y con velocidades mucho mayores.

1.1.2. TECNOLOGÍAS DE TRANSPORTE MÁS USADAS

Las Empresas que poseen sus redes propias actualmente se encuentran obligadas a evolucionar y actualizar las mismas, para suplir todas sus necesidades tecnológicas y

brindar el soporte adecuado para sus aplicaciones existentes y futuras, proporcionando convergencia y Calidad de Servicio (QoS), acorde a las exigencias actuales.

1.1.2.1. PDH (JERARQUÍA DIGITAL PLESIÓCRONA)[1]

PDH, es una tecnología usada en telecomunicaciones nativamente para telefonía que permite enviar varios canales telefónicos sobre un mismo medio ya sea este coaxial, de radio o microondas, usando técnicas de multiplexación por división de tiempo. Se llama *plesiocrono* porque cada nivel de multiplexación, es independiente de los demás niveles, los cuales pueden funcionar nominalmente a la misma velocidad (bit rate), pero tienen cierta variación con respecto a la velocidad nominal, es decir que van a tener un margen de tolerancia.

La tecnología PDH está basada en canales de 64 Kbps. A medida que se incrementa el nivel de multiplexación, también se van incrementando el número de canales en el medio físico, al existir estas variaciones en el número de canales, la formación de la estructura de la trama y su duración, va a ir cambiando en los distintos niveles.

En cada nivel de multiplexación, a una trama que transporta un canal de voz se le adiciona la información de control, razón por la cual si un nivel superior transporta cierto número de canales, este número de canales va a ser un múltiplo de un número de canales que se pueda transportar en un nivel inferior.

Existen tres jerarquías PDH:
La europea descrita en la norma G.732 de la UIT-T.
La norteamericana y la japonesa descritas en la norma G.733 de la UIT-T.

[1] "*Jerarquía Digital Plesiocrona*
http://es.wikipedia.org/wiki/Jerarqu%C3%ADa_Digital_Plesi%C3%B3crona

1.1.2.1.1. JERARQUÍA EUROPEA (E1)

El primer nivel jerárquico, o la velocidad básica de transferencia están basadas en un flujo de 2048 Kbps conocido también como E1, al tratarse de señales de voz, esta se muestrea a una frecuencia de 8 Khz es decir una muestra cada 125 μs, cada muestra se codifica con 8 bits con lo que se obtiene un régimen binario de 64 kbps, con esto se obtiene 30 canales de voz, y otros 2 canales utilizados para señalización y control. En la Figura 1.1 se muestra la trama descrita.

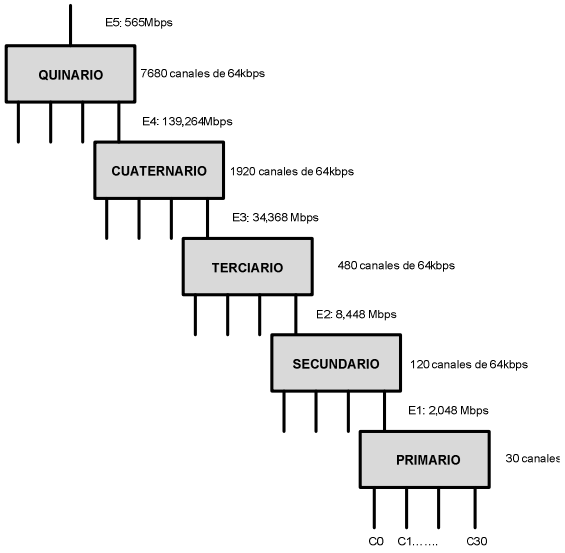

Figura 1.1 Jerarquía Europea (E1)

La velocidad de flujo está expuesta a cierta variación con respecto a su velocidad nominal, ya que no son síncronas sino *plesiòcronas*, al tener una tasa de transferencia de 2,048 Mbps, esta tiene un margen de tolerancia de ±50 ppm (partes por millón), y cada flujo de transferencia tiene su respectiva tolerancia.

Nombre	Velocidad	Tolerancia	Nª Canales
E1	2,048 Mbps	±50 ppm	30
E2	8,448 Mbps	±30 ppm	120
E3	34,368 Mbps	±20 ppm	480
E4	139,264Mbps	±15 ppm	1920

Tabla 1.1. Jerarquía Digital Plesiocrona (PDH) [2]

Si se necesita transportar múltiples flujos de datos o E1s, a estos hay que combinarlos y multiplexarlos en grupos de cuatro, además se añade otros bits, para que en el momento de la demultiplexacion se identifique que bits pertenecen a cada flujo de datos, estos bits adicionales tienen el nombre de *bits de justificación* o de *relleno,* la función de estos bits es también igualar las velocidades, ya que los flujos no están trabajando a la misma velocidad, siendo estos bits de compensación.

1.1.2.1.2 JERARQUÍA NORTEAMERICANA Y JAPONESA

En la jerarquía norteamericana, las agrupaciones se realizan primero 24 canales a una velocidad de 1,544 Mbps, luego a medida que va subiendo el orden, sus valores van cambiando como se muestra a continuación, el siguiente orden x4 a una velocidad de 6,312 Mbps, luego x7 a una velocidad de 44,736 Mbps y x6 a 274,176 Mbps. Para la jerarquía japonesa, se puede partir de la velocidad de 6,312 Mbps y continuando de acuerdo al orden se tiene x5 32,064Mbps y luego x3 a 97,728Mbps.

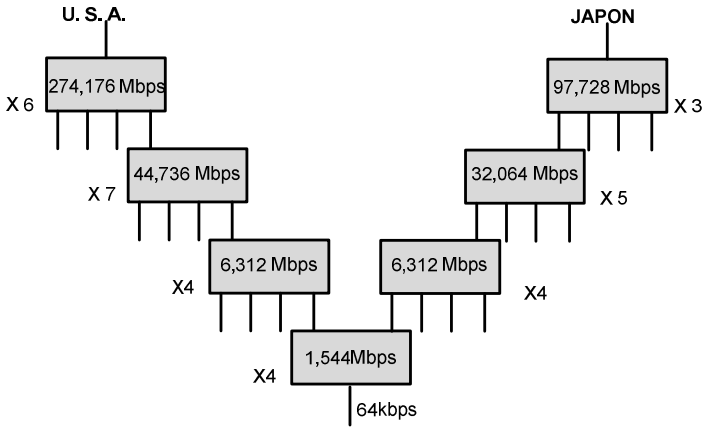

Figura 1.2. Jerarquía americana y japonesa

1.1.2.1.3 JERARQUÍAS DE MULTIPLEXACIÓN

En la Tabla 1.2 se muestran los distintos niveles de multiplexación PDH utilizados en Norteamérica (Estados Unidos y Canadá), Europa y Japón.

	Norteamérica			Europa			Japón		
	Canales	Mbps	Denominación	Canales	Mbps	Denominación	Canales	Mbps	Denominación
1	24	1,544	T1	30	2,048	E1	24	1,544	J1
2	96	6,312	T2	120	8,448	E2	96	6,312	J2
3	672	44,736	T3	480	34,368	E3	480	32,064	J3
4	4032	274,176	T4	1920	139,264	E4	1440	97,728	J4

Tabla 1.2. Jerarquías de Multiplexación (PDH)

Los flujos de datos que llegan a los multiplexores se les suele llamar tributarios, afluentes o cargas del múltiplex de orden superior.

1.1.2.1.4 TRAMA E2 [2]

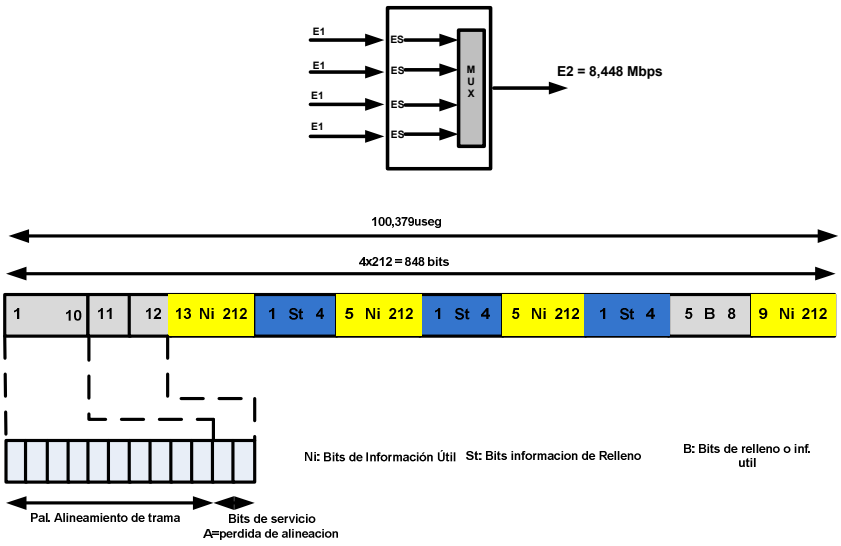

Figura 1.3 Trama E2

Como se trata de un sistema que no es síncrono, la lectura se realiza a una velocidad mayor a la velocidad de escritura, razón por la que se coloca el bit de relleno para que las velocidades se igualen, y por cada sistema tributario solamente se posee un bit de relleno.

[2] Ing. Edgar Ochoa, Material de estudio de la asignatura "*Comunicaciones III*"

Cuando tenemos los bits de relleno llamado St activados en 111, entonces el bit que podría ser de relleno o información útil no contiene información, pero en el caso en que los bits St se encuentren en 000, el bit que podría ser de relleno en este caso contiene información útil. En PDH la multiplexación se realiza bit a bit, ya que la justificación a bytes implica más problemática y cada etapa de multiplexación tiene su propia referencia de temporización, lo que produce inconvenientes en el momento de la demultiplexacion Plesiócrona, ya que no es posible extraer un tributario concreto sin demultiplexar completamente la señal.

1.1.2.2 SDH (JERARQUÍA DIGITAL SÍNCRONA) [3]

SDH, es un conjunto jerárquico de estructuras de transporte digitales síncronos, normalizadas para el transporte, por redes de transmisión físicas de cabidas útiles correctamente adaptadas. En este caso las técnicas de multiplexación y demultiplexacion son simplificadas.

SDH es un estándar internacional para redes de telecomunicaciones de alta capacidad. La multiplexación se realiza de manera sincrónica byte a byte, con diferentes tipos de justificación, presentando una estructura de trama idéntica, proporciona completa centralización de todas las funciones de administración y control de la red.

Modulo de Transporte Síncrono (STM): Es la estructura de información utilizada para soportar conexiones de capa de sección en la SDH. Consta de campos de cabida útil de información y de tara de sección (SOH) organizados en una estructura de trama de bloque que se repite cada 125 µs.

[3] "*Jerarquía Digital Síncrona*" http://es.wikipedia.org/wiki/Jerarqu%C3%ADa_digital_s%C3%ADncrona

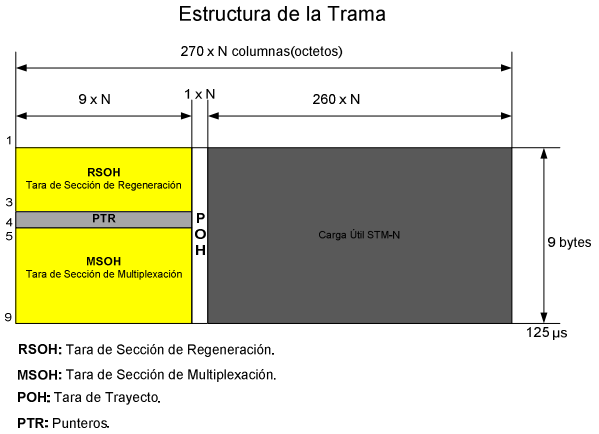

Figura 1.4 Estructura de la Trama.

La información está adaptada para su transmisión por el medio elegido a una velocidad que se sincroniza con la red. El STM básico se define a 155,52 Mbps. Se denomina STM-1. Los STM de mayor capacidad se constituyen a velocidades equivalentes a N veces la velocidad básica. Se han definido capacidades de STM para N=4, N=16 y N=64. Todas las señales tributarias, de cualquier jerarquía y origen, deben poder acomodarse a la estructura sincrónica del STM-1 que se pueden resumir en la Figura 1.5.

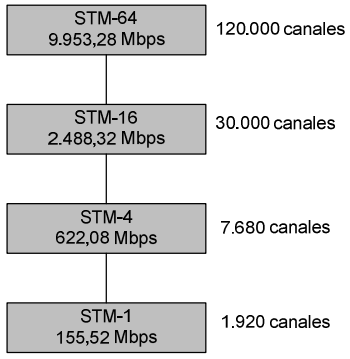

Figura 1.5 Modulo de Transporte Síncrono

Contenedor (C): Es la estructura de información que forma la cabida útil de información síncrona de red para un contenedor virtual. Para cada uno de los contenedores virtuales definidos existe el correspondiente contenedor.

Contenedor Virtual (VC): Es la estructura de información utilizada para soportar conexiones de capa de trayecto en la SDH. Consta de campos de información de cabida útil de información y de la tara de trayecto (POH) organizados en una estructura de trama de bloque que se repite cada 125 o 500 µs.

Puntero (PTR): Indicador cuyo valor define el desplazamiento de la trama de un contenedor virtual con respecto a la referencia de trama de la entidad de transporte sobre lo que es soportado.

Concatenación: Procedimiento en una multiplicidad de contenedores virtuales que se asocian unos a otros de modo que su capacidad combinada puede utilizarse como un contenedor sencillo en el que se mantiene la integridad de la secuencia de bits.

Unidad Administrativa (AU): Es la estructura de información que proporciona la adaptación entre la capa de trayecto de orden superior y la capa de sección de multiplexación. Consta de una cabida útil de información (el contenedor virtual de orden superior) y un puntero de unidad administrativa que señala el desplazamiento del comienzo de la trama de cabida útil con relación al comienzo de la trama de la sección de multiplexación.

Unidad Afluente: Es una estructura de información que proporciona la adaptación entre la capa de trayecto de orden inferior y la capa de trayecto de orden superior. Consta de una cabida útil de información (el contendor virtual de orden inferior) y un puntero de unidad afluente que señala el desplazamiento del comienzo de la trama de cabida útil con relación al comienzo de la trama del contenedor virtual de orden superior.

Tara de Sección (SOH): la información de SOH se añade a la cabida útil de información para crear un STM-N.

Incluye información de alineación de trama de bloques e información para el mantenimiento y la supervisión de la calidad de funcionamiento y otras funciones operacionales.

La información de SOH se clasifica además en tara de sección de regeneración (RSOH), que se termina en funciones de regeneración y tara de sección de multiplexación (MSOH), que pasa transparentemente a través de los regeneradores y se termina donde los AUG son ensamblados y desensamblados.

Las filas 1 a 3 de la SOH se designan como RSOH mientras que las filas 5 a 9 se designan de modo que sean la MSOH.

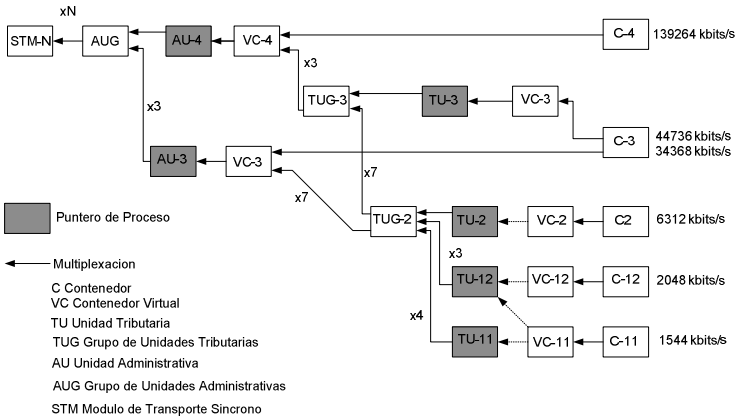

Figura 1.6 Jerarquía Digital Síncrona

- STM-1 = 8000*(270octeto s*9filas*8bits)= 155 Mbps
- STM-4 = 4*8000*(270octetos*9filas*8bits)= 622Mbps
- STM-16 = 16*8000*(270octetos*9filas*8bits)= 2.5Gbps
- STM-64 = 64*8000*(270octetos*9filas*8bits)= 10Gbps
- STM-256 = 256*8000*(270octetos*9filas*8bits)= 40Gbps

1.1.2.3 TDM (MULTIPLEXACIÓN POR DIVISIÓN DE TIEMPO) [4]

TDM, es una de las técnicas más utilizadas actualmente en los sistemas de transmisión digitales, donde el ancho de banda total del medio de transmisión se asigna a cada canal durante un intervalo del tiempo total. Se adapta bien a las señales binarias que consisten en impulsos que representan un dígito binario 1 o 0. Estos impulsos pueden ser de muy corta duración y sin embargo, son capaces de transportar la información deseada; por tanto, muchos de ellos pueden comprimirse en el tiempo disponible de un canal digital. La señal original puede ser una onda analógica que es convertida a un formato digital para su transmisión, como las señales de voz de una red telefónica, o puede estar ya en forma digital, como los de un equipo de datos o un computador.

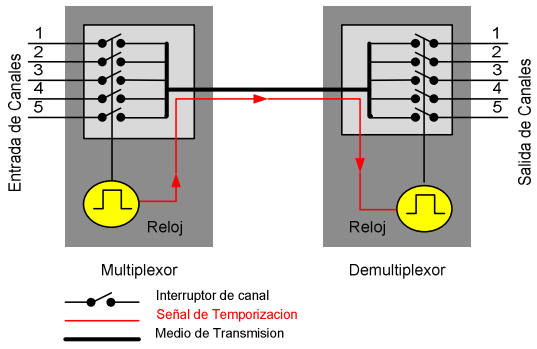

Figura 1.7 Multiplexación por división de Tiempo

"En el extremo emisor de este esquema, se tiene entradas de varios canales que llegan a los interruptores de canal, los mismos que se cierran de forma secuencial, según los pulsos de reloj, de manera que cada canal se conecta al medio de transmisión durante un intervalo de tiempo determinado por la duración de los impulsos de reloj.

En el extremo receptor, se tiene el demultiplexor que realiza la función inversa, es decir, conecta el medio de transmisión, secuencialmente, con la salida de cada uno de los canales mediante interruptores controlados por señales de su reloj.

---

[4] "Multiplexación por División de Tiempo"
http://es.wikipedia.org/wiki/Acceso_m%C3%BAltiple_por_divisi%C3%B3n_de_tiempo

Las señales de reloj de multiplexor y demultiplexor están sincronizadas mediante señales que se transmiten por el mismo medio o por otro." [4]

Esta técnica también conocida como PCM (Pulse Code Modulation), consiste en digitalizar una señal analógica proporcionando en nuestro medio una capacidad de 64 Kbps, como resultado de la toma de muestras cada 125 μs , regidas por el ancho de banda teórico requerido para una señal vocal que es de 4 KHz, en nuestro medio el verdadero ancho de banda asignado a una señal vocal es de 3100 Hz, pues el rango abarca desde los 300 Hz hasta los 3400 Hz; luego las muestras tomadas se cuantifican y codifican mediante la Ley A de cuantificación que se usa en la región.

1.1.2.4 RDSI-ISDN (RED DIGITAL DE SERVICIOS INTEGRADOS) [5]

RDSI, esta tecnología se la puede definir como una evolución de las redes actuales, que presta conexiones extremo a extremo a nivel digital y es capaz de ofertar una amplia gama de servicios, utilizando la misma infraestructura para servicios que nativamente requerían interfaces distintas como (télex, voz, conmutación de circuitos, conmutación de paquetes, etc.).

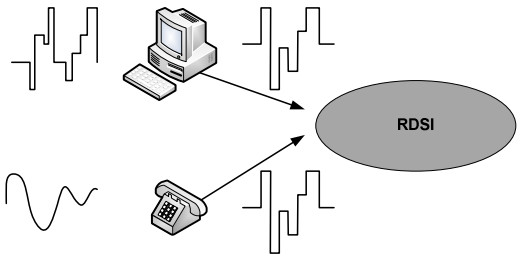

Figura 1.8. Integración Señales en RDSI

RDSI se basa en la transmisión digital, integrando las señales analógicas mediante la conversión Analógico - Digital, ofreciendo una capacidad básica de comunicación de 64

[4] "Multiplexación por División de Tiempo" http://es.wikipedia.org/wiki/Acceso_m%C3%BAltiple_por_divisi%C3%B3n_de_tiempo

[5] "ISDN: *Red digital de servicios integrados*" http://www.frm.utn.edu.ar/comunicaciones/isdn.html

Kbps. En el caso de un teléfono convencional, se efectúa la conversión Analógico Digital y en el caso de equipos digitales como un computador, se transforma el código original a otro más adecuado para ser transportado.

1.1.2.4.1 ESTRUCTURA DE LA RDSI

RDSI como se dijo anteriormente tiene la capacidad de llegar a los terminales de los abonados con una tasa de 64 kbps, dividiendo a los canales en grupos a los que se les denomina canal B y canal D.

Los denominados canal B tienen una tasa de 64kbps, mientras que el D puede tener una tasa de 16kbps o 64kbps, esto dependerá del tipo de acceso, si es un acceso básico (2B+D) o si es un acceso primario (30B+D), la multiplexación de estos canales se la realiza en el tiempo.

ACCESO BÁSICO (BRI)

BRI (Basic Rate Interface), este tipo de acceso consta de 2 canales B full-dúplex de 64 kbps y un canal D full-dúplex de 16 kbps. Durante la división en tramas, la sincronización, y la adición de otros bits, se obtiene una velocidad total a 192 kbps.

2B+D+señalización+framing

ACCESO PRIMARIO (PRI)

PRI (Primary Rate Interface), este tipo de acceso esta designado para usuarios que requieren mayores capacidades, ya sea para PBX (Private Branch Exchange), como no en todos los países se usa la misma jerarquía de transmisión, no es posible tener una velocidad de datos única.

Como en determinados países utilizan una velocidad de transmisión estándar de 1,544Mbps, esta estructura tiene 23 canales B y un canal D de 64Kbps.

23 B(64)+D(64)+señalización+framing(8) en total 1,544 Mbps

En los países que utilizan la velocidad de transmisión estándar de 2,048Mbps, se tiene 30 canales B y un canal D de 64Kbps.

30 B(64)+D(64)+señalización+framing(64) en total 2,048 Mbps

Con el propósito de integrarse con redes no digitalizadas tiene diferentes modos de interconexión, ya que soporta la conmutación de paquetes, mientras que su versión anterior solo soportaba la conmutación de circuitos.

1.1.2.4.2 ARQUITECTURA DE PROTOCOLOS

Para la señalización de la RDSI y el usuario, se tiene la estructura del modelo OSI, la cual consta de tres niveles:

- Capa física
- Capa de enlace, o data link layer (DLL)
- Capa de red, o network layer (el protocolo RDSI)

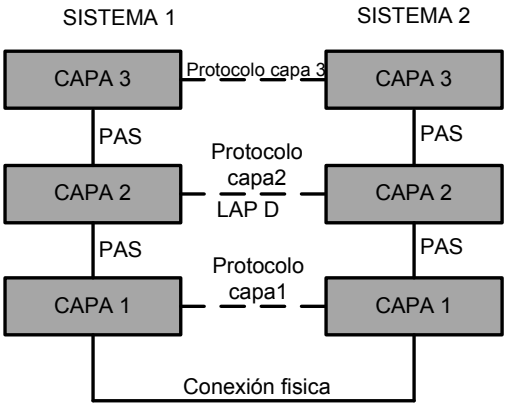

Figura 1.9. Arquitectura de Protocolos RDSI

La transferencia es a través del canal D.

“La capa 1, se encuentran todos los parámetros eléctricos de la señal en la interfaz (tensión, impedancias), la estructura de la trama y su temporización, la activación y desactivación de los terminales y el control del acceso de los terminales conectados en paralelo al bus del interfaz.

La capa 2 (LAP D), define los procedimientos de transferencia de las tramas, la provisión de una o más conexiones de enlace de datos sobre un mismo canal D, la detección y el control de errores de la transmisión y el control de flujo de la transferencia de tramas.

La transmisión en el canal D se la realiza en forma de tramas LAPD, aquí se consideran tres aplicaciones: señalización de control, conmutación de paquetes, y telemetría.

La capa 3 establece los procedimientos de encaminamiento y retransmisión, establece las conexiones con la red, realiza la transferencia de información del usuario y realiza también control de flujo. Por medio de los procedimientos de capa 3 se pueden realizar conexiones por conmutación de circuitos, de paquetes, transferir información de

señalización usuario-usuario transparentemente a través de la red y solicitar de ésta facilidades o servicios suplementarios." [6]

1.1.2.4.3. CARACTERISTICAS DE LA RDSI

Velocidad: Esta tecnología ofrece múltiples canales digitales que pueden operar paralelamente a través de la misma conexión telefónica entre central y usuario; la tecnología digital está en la central del proveedor y en los equipos del usuario.

Este esquema permite una transferencia de datos más veloz de hasta 128 Kbps sin comprimir, con un servicio de acceso básico, y empleando un protocolo de agregación de canales, tomando en cuenta que el tiempo necesario para establecer una comunicación en RDSI es cerca de la mitad del tiempo empleado con una línea con señal analógica.

Conexión de múltiples dispositivos: Es posible combinar diferentes fuentes de datos digitales y hacer que la información llegue al destino correcto, debido a que la línea es digital, es fácil controlar el ruido y las interferencias producidos al combinar las señales.

Señalización: La llamada se establece enviando un paquete especial de datos a través de un canal independiente de los canales para datos. Este método de llamada se engloba dentro de una serie de opciones de control conocidas como señalización, y permite establecer la llamada en un par de segundos, informando al destinatario del tipo de conexión (voz o datos) y desde que número se ha llamado.

Servicios: Esta tecnología no se limita a ofrecer comunicaciones de voz, sino que ofrece otros muchos servicios, como transmisión de datos informáticos (servicios portadores), videoconferencia, conexión a Internet, opciones como llamada en espera, identidad del origen, conmutación de circuitos y conmutación de paquetes.

---

[6] "ISDN: *Red digital de servicios integrados*" http://personales.mundivia.es/jtoledo/angel/SE.HTM

1.1.2.5 X.25 [7]

X.25, es un estándar UIT-T para redes de área amplia de conmutación de paquetes. Es una conexión punto a punto entre el terminal de usuario DTE (Data Terminal Equipment) y el equipo de comunicación DCE (Data Circuit Terminating Equipment) que es el nodo de acceso a la red. Establece mecanismos de direccionamiento entre usuarios, negociación de características de comunicación, técnicas de recuperación de errores. Los servicios públicos de conmutación de paquetes admiten numerosos tipos de estaciones de distintos fabricantes. Por lo tanto, es de la mayor importancia definir la interfaz entre el equipo del usuario final y la red.

"X.25 trabaja sobre servicios basados en circuitos virtuales (VC). Un circuito virtual o canal lógico es aquel en el cual el usuario percibe la existencia de un circuito físico dedicado exclusivamente al ordenador o equipo que el maneja, cuando en realidad ese circuito físico "dedicado" lo comparten muchos usuarios. Mediante diversas técnicas de multiplexado estadístico, se entrelazan paquetes de distintos usuarios dentro de un mismo canal." [8]

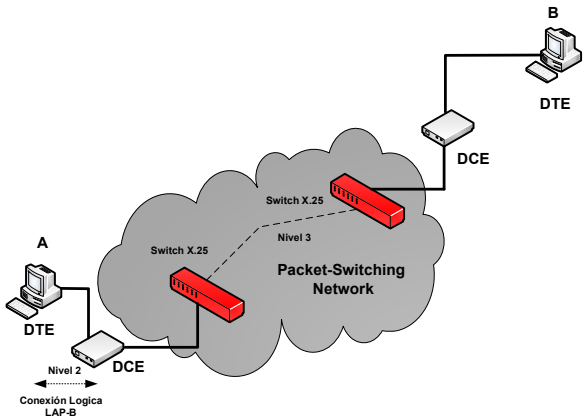

Figura 1.10. X.25

X.25 Soporta SVC (Switched Virtual Circuit) que es dinámicamente establecido y PVC (Permanent Virtual Circuit) que se da solamente cuando se contrata. Los paquetes de control de llamadas son transportados en el mismo circuito virtual de paquetes de datos.

---

[7] "*Norma X.25*" http://es.wikipedia.org/wiki/Norma_X.25

[8] "*Redes X.25*" http://www.angelfire.com/wi/ociosonet/5.html

Cuando el tráfico es continuo se usa PVC y en este caso no se envía la dirección de destino. Cuando el trafico no es continuo se usa SVC y aquí si se envía la dirección de destino. X.25 usa tres capas del modelo OSI; Capa Física, Enlace de Datos y Capa de Red. El Multiplexado de circuitos virtuales se da en Capa 3, el control de errores en capa 2 y el control de flujo en capa 2 y 3.

X.25 maneja velocidades bajas de 9,6 kbps a 64 kbps, se usa mayormente en cajeros automáticos y no es apropiado para redes digitales modernas con alta confiabilidad.

1.1.2.6 FRAME RELAY [9]

Frame Relay, es una tecnología para redes de área amplia (WAN) que requiere el mínimo procesamiento de los nodos de conmutación. Es un protocolo de transmisión de paquetes de datos en ráfagas de alta velocidad a través de una red digital fragmentados en unidades de transmisión llamadas Frame.

Es un servicio orientado a conexión, sus conexiones virtuales pueden ser del tipo permanente, (PVC, Permanent Virtual Circuit) o conmutadas (SVC, Switched Virtual Circuit), puesto que no tiene mecanismos para la corrección de errores o el control de flujo, permite una asignación dinámica del ancho de banda basada en los principios de la concentración y multiplexación estadística empleada en la tecnología X.25, así, se ha pasado de los 64 kbps de las redes de conmutación de paquetes X.25 originales, a una velocidad de 2 Mbps llegando incluso a los 34 Mbps.

[9] "*Tecnología Frame Relay*" http://www.monografias.com/trabajos11/frame/frame.shtml

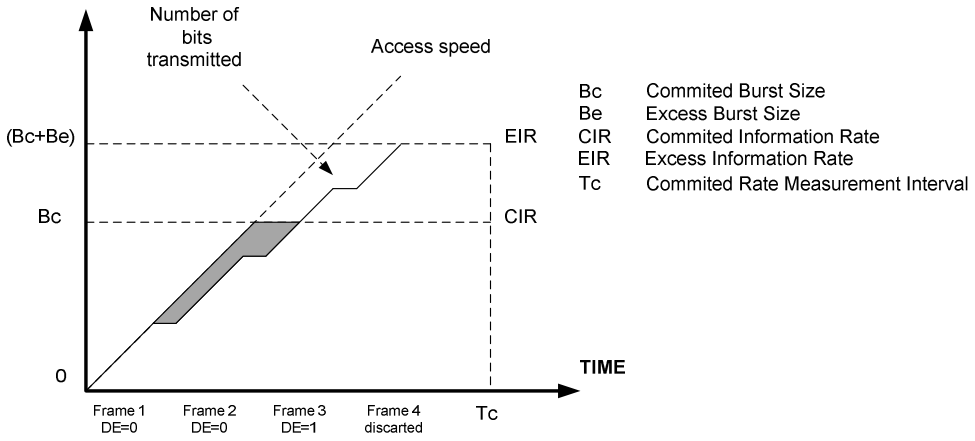

Figura 1.11. Frame Relay

Al contratar un servicio Frame Relay, contratamos un ancho de banda determinado en un tiempo determinado. A este ancho de banda se le conoce como CIR (*Commited Information Rate*). Esta velocidad, surge de la división de Bc (*Committed Burst*), entre Tc (el intervalo de tiempo). No obstante, una de las características de Frame Relay es su capacidad para adaptarse a las necesidades de las aplicaciones, pudiendo usar una mayor velocidad de la contratada en momentos puntuales, adaptándose muy bien al tráfico en ráfagas. Aunque la media de tráfico en el intervalo Tc no deberá superar la cantidad estipulada Bc.

Estos Bc bits, serán enviados de forma transparente. No obstante, cabe la posibilidad de transmitir por encima del CIR contratado, mediante los Be (*Excess Burst*). Estos datos que superan lo contratado, serán enviados en modo *best-effort*, activándose el bit DE de estas tramas, con lo que serán las primeras en ser descartadas en caso de congestión en algún nodo.

Esta tecnología solo utiliza las dos primeras capas del modelo de referencia OSI (Open System Interconnection) y además liberando a la capa enlace de todas las funciones de control de flujo y recuperación de errores, las cuales pasan a ser responsabilidad de los equipos terminales. Con ello, las demoras se reducen al mínimo en cada conmutador, que ya no necesita efectuar esas funciones en cada trama antes de reenviarla, y se elimina el tráfico adicional que generaban los mecanismos de corrección de errores.

1.1.2.7 ATM (MODO DE TRANSFERENCIA ASÍNCRONO) [10]

ATM, es una arquitectura de red que utiliza pequeñas celdas de tamaño fijo 53bytes, de esta manera las celdas no tienen segmentos específicos de tiempo para la alineación del paquete, la celda contiene todo tipo de información en campos pequeños de 48 bytes, los 5 bytes restantes contienen la información del header, el cual es interpretado por la red para mover las celdas.

El modo de Transferencia Asíncrono (ATM) es una tecnología orientada a conexión, si dos nodos desean empezar una transmisión, primero deben tener establecido un canal mediante el protocolo de llamada o señalización, cada celda ATM contiene información que sirve para reconocer la conexión a la que pertenecen.

ATM soporta diferentes tipos de transmisiones como pueden ser voz, datos y video (red multimedia), estas pueden estar mezcladas en la misma transmisión, teniendo los rangos de velocidad para transmitir desde 155Mbps hasta 2,5Gbps, no se reserva posiciones de una celda para transmitir algún tipo de información específica, por esta razón la velocidad de transmisión se la puede dirigir a un usuario, una red o un grupo de trabajo.
Los dispositivos llamados switchs son los encargados en establecer la comunicación en las redes ATM, si se desea formar redes mas grandes se puede conectar varios switchs en cascada.

1.1.2.7.1 CANALES Y TRAYECTOS VIRTUALES

Se trata de conexiones lógicas que sirven para establecer comunicación entre los clientes de la red, entre estas tenemos:

[10] "ATM: *Modo de Transferencia Asíncrona*"
http://es.wikipedia.org/wiki/Asynchronous_Transfer_Mode

Figura 1.12. Canales y Trayectos Virtuales.

VCC (Virtual Channel Connection) o canal virtual, es una conexión básica entre dos elementos de la red ATM, esta conexión se la puede realizar entre usuario – usuario, usuario – red, y entre red – red.

VPC (Virtual Path Connection) o trayectoria virtual, es un conjunto de VCCs que viajan dentro del mismo trayecto virtual, con las ventajas de tener menor procesamiento y tiempo de establecimiento de la conexión, además mejorando la confiabilidad y performance de la red.PS (Physical Section) o sección física, se encarga de conectar y mantener continuidad entre los elementos de la red, debe conservar en óptimas condiciones las señales eléctricas y ópticas, para que estas no resulten afectadas por el ruido, atenuaciones y distorsiones.

1.1.2.7.2 CELDA Y CAMPOS DE LA CELDA ATM

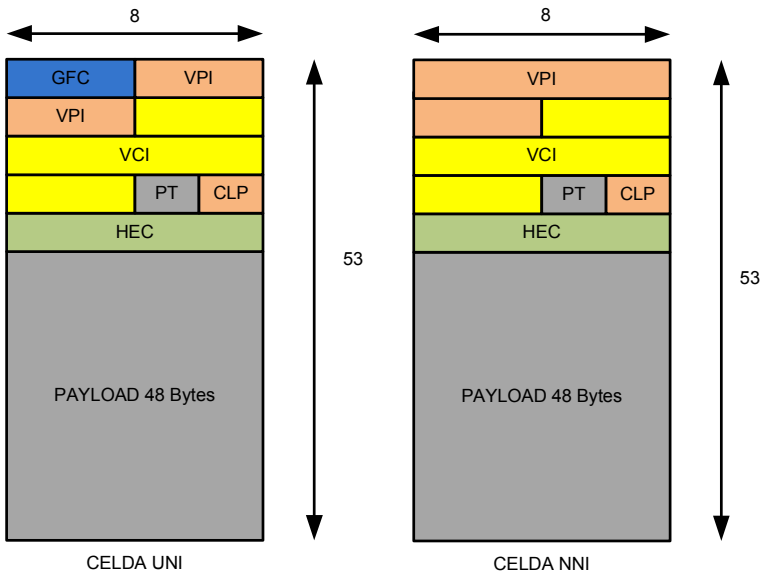

Figura 1.13. Campos de la Celda ATM

ATM maneja dos tipos de interfaces, la UNI(user network interface) o interface usuario red, esta asocia un switch público o privado con un dispositivo de usuario, y la NNI (network network interface) o interface de red a red, asocia la conexión entre switchs.

Control de Flujo o GFC (Generic Flow Control), está formado de 4 bits, en un principio este campo fue destinado para labores de gestión de tráfico (no se usa en la práctica), las celdas NNI lo utilizan para extender el campo VPI a 12 bit, como el mostrado en la figura anterior, este campo es usado solamente en la interface UNI (usuario-red).

Identificador de Ruta Virtual o VPI (Virtual Path Identifier campo de 8 bits) conjuntamente con el Identificador de Circuito Virtual (VCI virtual Channel Identifier campo de 16bits), son usados para identificar la ruta de destino de la celda.
Tipo de información de usuario o PT (Payload type campo de 3 bits) este campo sirve para distinguir la información de usuario de gestión de red.

Prioridad o CLP (Cell Loss Priority campo de 1 bit), nos dice el nivel de prioridad de una celda, con este campo en “0” indica alta prioridad, y este campo en “1” indica baja prioridad.

Corrección de error de cabecera o HEC (Header Error Correction campo de 8 bits), permite detectar múltiples errores y corregir errores simples en el header, en el caso de voz y video no hay control, y cuando se trata de datos, el control es "end to end" en protocolo superior.

1.1.2.7.3 TRANSMISIÓN DE CELDAS ATM [11]

La transmisión en ATM se la realiza en la interfaz física basada en SDH/SONET, se puede transmitir a distintas velocidades:
25,6 Mbps, 51,84 Mbps: STM-0/STS-1, 155,52 Mbps: STM-1 y a 622,08Mbps STM-4.
SONET (Synchronous Optical Network) es un estándar para el transporte en redes de fibra óptica, en ATM dependiendo de la aplicación se requerirá de servicios de la red, por ejemplo servicio sensible al retardo de la voz y video.

Dentro de lo que se refiere a la gestión de tráfico, en ATM el trafico de la voz y video se la realiza a través de un flujo continuo de celdas, se pretende que el retardo a través de la red no sea variable, y sea lo más pequeño posible.

ATM está diseñado para manejar los siguientes tipos de tráfico:

"Clase A - Constant Bit Rate (CBR), orientado a conexión, tráfico síncrono (Ej. voz o video sin compresión).

Clase B - Variable Bit Traffic (VBR), orientado a conexión, tráfico síncrono (voz y video comprimidos).

Clase C - Variable Bit Rate, orientado a conexión, tráfico asíncrono (X.25, Frame Relay, etc).

Clase D - Información de paquete sin conexión (tráfico LAN, SMDS, etc)." [11]

---

11 "*Redes ATM*" http://www.angelfire.com/wi/ociosonet/29.html

1.1.2.7.4 ENCAMINAMIENTO

En ATM gracias a las trayectorias virtuales VP y los canales virtuales, la llegada de las celdas es de forma ordenada, debido a que es un servicio orientado a conexión.
Al establecer una comunicación con QoS, se debe buscar la trayectoria que seguirán todas las celdas, esta trayectoria se mantiene durante toda la comunicación, en caso de que falle un nodo, la comunicación se verá afectada, en toda la sesión y durante la conexión también se deberá garantizar la calidad de servicio.

En ATM tenemos dos formas de crear una conexión vía circuito virtual VC: SVC Switched Virtual Channel (Canal virtual Conmutado) y PVC Permanent Virtual Channel (Canal Virtual Permanente).

PVC es creado por medio del Network manager (NM), para tener acceso al servicio o acceso al equipo terminal, PVC se mantiene siempre hasta que es liberado por el NM, esto es parecido a una línea dedicada o permanente.

SVC el canal virtual se crea para la comunicación entre partes, solo después de que la red ha solicitado la llamada, al finalizar la misma la señalización libera el SVC.
Para las funciones de gestión del tráfico, ATM ha estandarizado un conjunto de funciones, para obtener mayor eficiencia, la red tiene definido 3 niveles: Nivel físico, Nivel ATM, Nivel de adaptación.

Nivel Físico, hace referencia a los medios de transmisión, en ATM se puede transmitir con fibra óptica a 155Mbps, o también nuevas interfaces capaces de trabajar a 622Mbps.
Nivel ATM, es el nivel en donde se realiza el multiplexado y conmutación de paquetes, para el encaminamiento de las celdas se basa en los campos VCI (virtual circuit identifiers) y VPI (virtual path identifiers) que son los que definen las trayectorias.

1.1.2.7.5 CATEGORÍAS DE SERVICIOS ATM

Dentro de las categoría de servicio ATM se definen las siguientes: CBR, VBR, UBR, ABR.

CBR (Constant Bit Rate) proporciona una conexión de un ancho de banda dedicado, está diseñado para aplicación en “real time”, requiere retardos y jitter de retrasos pequeños y predecibles.

VBR (Variable Bit Rate) para aplicaciones con trafico a ráfagas, se caracteriza por las tasa máxima que se quiere transmitir PCR (Peak Cell Rate) y la tasa media o sostenida SCR (Sustained Cell Rate), dentro de este tenemos dos categorías; rt-VBR (Real Time Variable Bit Rate) para aplicaciones que tiene requerimientos estrictos de retraso por ejemplo voz o video comprimido; y nrt-VBR(Non real time Variable Bit Rate) para aplicaciones que tienen requerimientos críticos de tiempo de respuesta, ejemplo transacciones bancarias.

UBR (Unspecified Bit Rate) comparte el ancho de banda que el resto de servicios no utiliza, ya que puede existir capacidad disponible en la red debido a que, la red no dedica todos los recursos a trafico CBR y VBR (trafico de naturaleza “bursty”). UBR es usado para aplicaciones que puedan tolerar la perdida de celdas y retardos variables, se provee de “Best Effort Service”.

ABR (Available Bit Rate) aquí todos los usuarios comparten en la gestión de tráfico, cualquier capacidad adicional se comparte entre todas las fuentes ABR. Las aplicaciones especifican el PCR (Peak Cell Rate) y el MCR (Minimum Cell Rate), de esta manera toda aplicación ABR por lo menos debe recibir su MCR, durante la transmisión se evita la perdida de celdas.

1.1.2.7.6 ATM ADAPTATION LAYER (AAL)

Es un mecanismo de la tecnología ATM para el soporte de protocolos de transferencia de información que no son basados en ATM, tales como TCP/IP o el modelo OSI, se

encarga también de servicios como: segmentación, temporización, errores de transmisión, celdas perdidas, celdas mal insertadas y control de flujo.

Los protocolos AAL divide sus funciones en tareas como: la subcapa de convergencia (CS-Convergence Sublayer) para el soporte de aplicaciones especificas y la subcapa de ensamblado y segmentación (SAR-Segmentation and Reassembly Sublayer) la que se encarga de empaquetar y desempaquetar la información que se obtiene de CS. Se han diseñado diferentes protocolos para diferentes arquitecturas.

AAL tipo 1 soporta CBR(Constant Bit Rate), síncrono, orientado a conexión.

AAL tipo 2 soporta rt-VBR(real time variable bit rate).

AAL tipo 3/4 soporta nrt-VBR(non real time variable bit rate)

AAL tipo 5 es similar a AAL 3/4.

1.1.2.8. TCP(PROTOCOLO DE CONTROL DE TRANSMISIÓN)/IP (PROTOCOLO DE INTERNET) [12]

TCP / IP, es un conjunto de protocolos, que permiten la transmisión de datos entre redes de computadoras, incluso entre computadoras con diferentes sistemas operativos como Windows, Mac, etc. Se basa en la noción de dirección IP, cada equipo de la red, va a tener una dirección IP para poder enrutar los paquetes de datos.

Este protocolo está dividido en diversos módulos en donde cada uno cumple una función específica, en un orden específico, por eso se habla de modelo de capas, es decir al transportar datos por la red, estos deberán atravesar diferentes niveles de protocolos.

En cada capa de red se realiza un procesamiento de los datos o paquetes, y antes de enviarlos a la siguiente capa a estos se les agrega un encabezado.

[12] Miguel Alejandro Soto “Protocolo *TCP/IP*” http://usuarios.multimania.es/janjo/janjo1.html

TCP/IP es muy similar al modelo OSI (modelo de 7 capas y sirve para la Interconexión de sistemas abiertos) para estandarizar las comunicaciones entre equipos de una red.

1.1.2.8.1 COMPARACIÓN ENTRE EL MODELO OSI Y LA ARQUITECTURA TCP/IP

TCP/IP fue influenciado por el modelo OSI a utilizar capas, las capas se encuentran jerarquizadas, cada una tiene diferentes funciones y servicios que dependerá del tipo de red, la misión de las capas es proveer servicios a sus capas superiores, cada capa se ocupa únicamente de su nivel inmediato inferior, a quien solicita los servicios, y del nivel inmediato superior al que le devuelve los resultados, de esta manera tenemos las siguientes capas para el modelo TCP/IP:

Capa de enlace (capa 1): es la capa de acceso al medio, es similar a la capa física y de enlace de datos del modelo OSI (capa1 y capa2 respectivamente).

Capa de red (capa 2): es la capa de internet similar a la capa de red del modelo OSI (capa 3).

Capa de transporte (capa 3): Es quien envía o recibe los datos, y es similar a la capa de transporte del modelo OSI (capa 4).

Capa de aplicación (capa 4): La capa de aplicación es el conjunto de aplicaciones que hacen uso de las tres capas anteriores, es similar a las capas del modelo OSI: capa de sesión o capa 5, capa de presentación o capa 6, y capa de aplicación o capa 7, se incluyen protocolos destinados a proporcionar servicios, tales como correo electrónico (SMTP), transferencia de ficheros (FTP), y protocolos HTTP (Hypertext Transfer Protocol), etc.

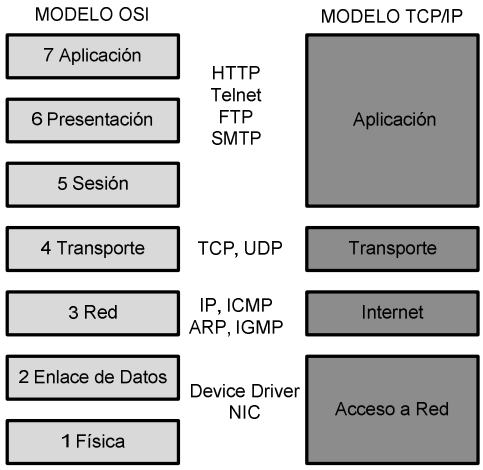

Figura. 1.14. Comparación entre los modelos OSI y TCP/IP

http://erikrz.wordpress.com/2010/09/02/tcpip-vs-osi/

El conjunto de protocolos TCP/IP están asociados a distintas capas y la combinación de las capas de la red y sus protocolos asociados se denominan Pila de Protocolos, donde una capa representa un encapsulamiento de una función, a diferencia del Modelo OSI, donde se trata a las capas como grupos funcionales bastante reducidos asociando al menos un protocolo con cada capa.

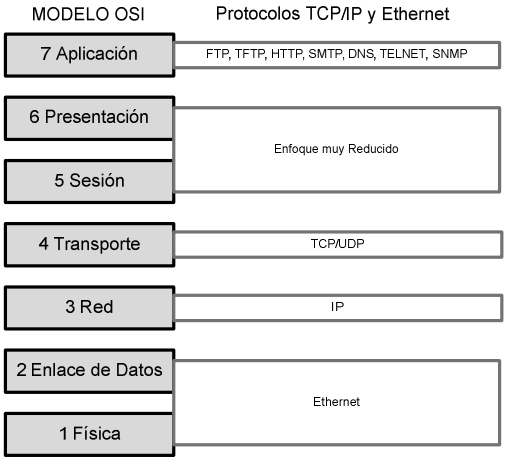

Figura. 1.15. Comparación entre los modelos OSI y TCP/IP

1.1.2.8.2 FUNCIONALIDAD DE CADA UNA DE LAS CAPAS DE LA ARQUITECTURA TCP/IP

Capa de enlace

A través de esta capa es posible acceder a la red física, consta de recursos y especificaciones necesarias para llevar a cabo la transmisión dentro de la red, aquí se manejan los conceptos de enrutamiento, sincronización, formato de datos, conversión de señales y la detección de errores a su llegada.

Capa de red

En esta capa se encuentran definidos los datagramas, permitiendo el enrutamiento de los mismos, además administra las nociones de direcciones IP, en esta capa se manejan los siguientes protocolos: IP(internet protocol), ARP(Address Resolution *Protocol*), ICMP(Internet Control Message *Protocol), RARP (*Reverse Address Resolution Protocol), y el IGMP(Internet Group Management Protocol).

Capa de transporte

En las capas anteriores se definió diferentes protocolos que permiten enviar la información entre equipos, esta capa se encarga de que las aplicaciones que se ejecutan en equipos remotos logren la comunicación, estas aplicaciones dependen del equipo, sistema operativo, ya que pueden ser un proceso o una aplicación razón por la cual no es fácil de identificarlas, por eso se ha creado un sistema de numeración para asociar a cada aplicación llamado puerto.

Para permitir el intercambio de datos entre dos aplicaciones que no dependen del tipo de red, se tiene dos protocolos denominamos: TCP y UDP.

TCP(Transmission Control Protocol), es un protocolo orientado a conexión y también ofrece la detección de errores.

UDP(User Datagram Protocol) es un protocolo no orientado a conexión, la detección de errores se le considera ya obsoleta.

La capa de aplicación

En esta capa se encuentra las aplicaciones a través de las cuales es posible comunicarse con capas inferiores, a través de los protocolos TCP o UDP, las aplicaciones también sirven para facilitar la interfaz usuario sistema operativo, entre las diferentes aplicaciones podemos tener: administración de archivos, conexión a red, utilidades de internet, etc.

1.1.3. TECNOLOGÍAS DE ACCESO A LA RED [13]

1.1.3.1. TECNOLOGÍA xDSL (DIGITAL SUBSCRIBER LINE)

DSL, proporciona un ancho de banda capaz de soportar diferentes aplicaciones, a través de líneas telefónicas es posible un acceso rápido a internet, es posible también acceso remoto a redes LAN(Local Área Network) y sistemas de VPNs(Virtual private network).

xDSL se encuentra integrado por varias tecnologías que tienen la capacidad de brindar gran ancho de banda sobre redes de cobre, sin la necesidad de amplificadores, ni repetidores, entre la conexión del cliente y el nodo de red, su acceso es punto a punto, de esta manera es posible un flujo de alta velocidad sobre el bucle de abonado, tanto de forma simétrica como asimétrica.

Tipo de DSL	Simétrico/ Asimétrico	Distancia De la línea (m)	Velocidad Descendente (Mbps)	Velocidad Ascendente (Mbps)
IDSL	Simétrico	5400	0,128	0,128
SDSL	Simétrico	3000	1,544	1,544
HDSL (2 pares)	Simétrico	3600	2,048	2,048
SHDSL	Simétrico (1 par)	1800	2,312	2,312

[13] "*Tecnologías en las Redes de Acceso*" http://www.monografias.com/trabajos13/tecnacc/tecnacc.shtml

	Simétrico (2 par)	1800	4,624	4,624
ADSL G. lite	Asimétrico	5400	1,5	0,512
ADSL	Asimétrico	3600	8	0,928
VDSL	Asimétrico	300	52	6
	Simétrico	300	26	26
	Asimétrico	1000	26	3
	Simétrico	1000	13	13

Tabla 1.3. Tecnologías xDSL en Red de Acceso

Siempre y cuando los pares de cobre cumplan los requerimientos en cuanto a la calidad del circuito y la distancia, xDSL puede ofrecer servicios de banda ancha a sus usuarios, similares a los servicios brindados por las redes inalámbricas, convirtiendo en este caso las líneas analógicas convencionales en líneas digitales de alta velocidad.

1.1.3.1.1 CLASIFICACIÓN DE TECNOLOGÍAS XDSL [14]

Existen varias tecnologías xDSL, cada una viene diseñada para cumplir finalidades especificas, algunas formas xDSL son propias, a otras se las usa como estándar, y otras son modelos teóricos, entre los varios tipos de xDSL tenemos: ADSL, RADSL, ASDL G LITE O UDSL, VDSL, HDSL, HDSL2 o SHDSL, SDSL, MDSL, IDSL o ISDN-BA.

ADSL (Asymmetric Digital Subscriber Line o Linea de Abonados Digital Asimétrica)

A través de un modem, es posible utilizar las líneas o pares de cobre, como líneas de alta velocidad, facilitando el acceso a internet, redes corporativas y aplicaciones multimedia, videoconferencia, VoIP, juegos online, etc. Los módems ADSL operan en un margen de frecuencias que va desde los 24 KHz hasta los 1104 KHz, aproximadamente. Esto hace

[14] "*Tecnología DSL*" http://www.monografias.com/trabajos5/tecdsl/tecdsl.shtml

que el ADSL pueda coexistir en un mismo lazo de abonado con el servicio telefónico, pues no se solapan sus intervalos de frecuencia.

RADSL(Rate-Adaptive DSL o DSL con Tasa Adaptable)

Funciona con los mismos márgenes de ADSL, pero la parte importante en RADSL, es que la velocidad de acceso se puede ajustar a las condiciones de la línea (longitud) de manera dinámica, teniendo así el rango para downstream de 640kbps a 2.2Mbps, y para upstream de 272kbps a 1,088Mbps.

ADSL G.LITE o UDSL (Línea de Abonados Digital Pequeña)

ADSL G.LITE o UDS.: G.Lite es también conocido como DSL Lite, splitterless ADSL (sin filtro voz/datos), y ADSL Universal. Hasta la llegada del estándar, el UAWG (Universal ADSL Work Group, Grupo de trabajo de ADSL) llamaba a la tecnología G.Lite, Universal ADSL. En junio de 1999, G.992.2 fue adoptado por la ITU como el estándar que recogía esta tecnología. Desgraciadamente para los consumidores, G.Lite es más lento que ADSL, ofreciendo velocidades de 1,5 Mbps (downstream) y de 512 Kbps (upstream).

VDSL (Very high rate DSL o Línea de Abonados Digital de Tasa Muy Alta)

Mucho más rápido que xDSL, puede alcanzar velocidades de 13 a 52 Mbps entre la central y el abonado y de 1,5 a 2,6 Mbps en sentido contrario, es ideal para proveer señales de TV HD. La máxima distancia que puede haber entre los dos módems VDSL (Very High Speed Digital Sbuscriber Line) no puede superar los 1.371 metros. VDSL está destinado a proveer el enlace final entre una red de fibra óptica y las premisas pues permite la transmisión de datos en un cierto estilo, sobre algún medio físico que es independiente de VDSL, teniendo como posibilidad el utilizar la infraestructura existente de cableado local.

HDSL(High-bit-rate DSL)

Este tipo de tecnología es simétrica, puede llegar a alcanzar una velocidad de 2,048Mbps full dúplex, usando dos pares de cobre, la distancia de 3600 metros es similar a la de ADSL, generalmente se implementa en grandes empresas, donde se necesita transportar gran cantidad de información a velocidades muy grandes.

HDSL tiene el acceso a última milla para redes de transporte digital para RDI, redes satelitales a costos razonables.

HDSL2 o SHDSL (High Bit-rate DSL 2)

Se diseño para el transporte de señales T1 (1,544Mbps) sobre el par de cobre, utiliza OPTIS(overlapped phase Trellis-code interlocked spectrum), puede brindar 2,048Mbps igual que HDSL, pero con la ventaja de usar un simple par de cobre.

SDSL (Symmetric Digital Subscriber Line)

Es muy similar a la tecnología HDSL, ya que soporta transmisiones simétricas, pero con dos particularidades:

Utiliza un solo par de cobre y tiene un alcance máximo de 3.048 metros. Esta tecnología provee el mismo ancho de banda en ambas direcciones, tanto para subir como para bajar datos, teniendo el mismo rendimiento de calidad. SDSL brinda velocidades de transmisión entre un rango de T1/E1, de hasta 1,5 Mbps, y a una distancia máxima de 3.700 m a 5.500 desde la oficina central, a través de un único par de cables. Este tipo de conexión es ideal para las empresas pequeñas y medianas que necesitan un medio eficaz para subir y bajar archivos a la Web.

MDSL

Para transmisiones simétricas, soporta cambios operacionales en la tasa del transceiver, en su versión CAP, puede soportar 64/128kbps, y una tasa de 2Mbps para una distancia de 4,5Km.

IDSL o ISDN-BA (ISDN Digital Subscriber Line)

Opera a bajas velocidades, su implementación se la realiza sobre las líneas ISDN (Integrated Service Digital Network), manejando velocidades de 128kbps o 144kbps, emplea técnicas de cancelación de eco, permitiendo así transmitir a una tasa de 160Kbps full dúplex.

1.2 IP (PROTOCOLO DE INTERNET) [15]

IP, es un protocolo no orientado a conexión, es usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados. Los datos en una red basada en IP se envían en bloques conocidos como paquetes o datagramas. IP hace posible la comunicación con equipos que no se había comunicado antes. El Protocolo de Internet provee un servicio de datagramas no confiable, es decir, hará el mejor esfuerzo en el envió (*best effort*) pero garantizando poco.

IP no dispone de ningún sistema para determinar si un paquete puede o no alcanzar su destino y únicamente proporciona seguridad (mediante checksums) de sus cabeceras y no de los datos transmitidos. Al no garantizar la recepción del paquete, éste podría llegar dañado, desordenado con respecto a otros paquetes, duplicado o simplemente no llegar.

Si los datagramas superan el tamaño máximo, estos podrán ser divididos en paquetes más pequeños, y reensamblados luego cuando sea necesario. Estos fragmentos podrán ir cada uno por un camino diferente dependiendo de cómo estén de congestionadas las rutas en cada momento.

Las cabeceras **IP** contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los conmutadores de paquetes (switches) y los enrutadores (routers) para decidir el tramo de red por el que reenviarán los paquetes

[15] "*Protocolo de Internet*" http://es.wikipedia.org/wiki/Internet_Protocol

El protocolo IP tiene tres aspectos muy importantes:

- Define la unidad básica para la transferencia de datos en una interred, especificando el formato exacto de un Datagrama IP.
- Realiza las funciones de enrutamiento.
- Define las reglas para que los Host y Routers procesen paquetes, los descarten o generen mensajes de error.

1.2.1 EL DATAGRAMA IP

El esquema de envío de **IP** es similar al que se emplea en la capa Acceso a red, donde se envían tramas formadas por un Encabezado y los Datos incluyéndose en el Encabezado la dirección física del origen y del destino. En el caso de IP se envían Datagramas, estos también incluyen un Encabezado y Datos, pero las direcciones empleadas son Direcciones IP.

Figura. 1.16. Estructura del Datagrama IP

1.2.1.1 FORMATO DEL DATAGRAMA IP [16]

Los Datagramas **IP** en su versión 4 (IPv4), están formados por palabras de 32 bits, cada Datagrama tiene un mínimo (y tamaño más frecuente) de cinco palabras y un máximo de quince.

[16] "*Cabecera IP*" http://es.wikipedia.org/wiki/Cabecera_IP

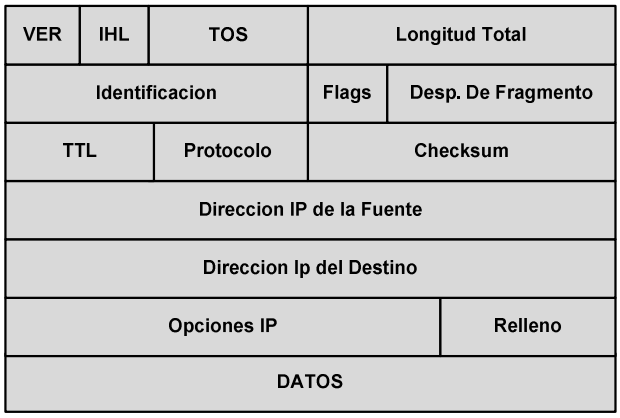

Figura. 1.17. Estructura de la cabecera IP más el campo de datos

Como se puede notar, la cabecera IP se constituye por 13 campos y la sección de Datos o información de Aplicación, a continuación se detalla la función de cada campo.

Ver (Versión): (4 bits) Este campo nos indica la versión de IP que se emplea para construir el Datagrama. Se requiere para que quien lo reciba lo interprete correctamente. Siempre vale lo mismo (0100).

IHL (Internet Header Length): (4 bits) Muestra el tamaño de la cabecera en cantidad de palabras de 32 bits. Su valor mínimo es de 5 para una cabecera correcta, y el máximo de 15.

TOS (Type of Service): (8 bits) La gran mayoría de los Host y Routers ignoran este campo, que indica la manera como debe ser manejado el paquete, definiendo la confiabilidad, prioridad, retardos y parámetros de envío. Su estructura es:

Figura. 1.18. Estructura del campo TOS

Los 5 bits de menos peso son independientes e indican características del servicio:

Bit 0: sin uso, debe permanecer en 0.

Bit 1: 1 costo mínimo, 0 costo normal.

Bit 2: 1 máxima fiabilidad, 0 fiabilidad normal.

Bit 3: 1 máximo rendimiento, 0 rendimiento normal.

Bit 4: 1 mínimo retardo, 0 retardo normal.

Los 3 bits restantes están relacionados con la precedencia de los mensajes:

000: De rutina.

001: Prioritario.

010: Inmediato.

011: Relámpago.

100: Invalidación relámpago.

101: Procesando llamada crítica y de emergencia.

110: Control de trabajo de Internet.

111: Control de red.

La prioridad (0 = Normal, 7 = Control de red) permite implementar algoritmos de control de congestión más eficientes. Los tipos D, T y R solicitan un tipo de transporte dado: D = Procesamiento con retardos cortos, T = Alto Desempeño y R= Alta confiabilidad. Nótese que estos bits son solo "sugerencias", no es obligatorio para la red cumplirlo.

Longitud Total (Total Length): (16 bits) Es el tamaño total, en octetos, del datagrama, incluyendo el tamaño de la cabecera y el de los datos. El tamaño máximo de los datagramas usados normalmente es de 576 octetos (64 de cabeceras y 512 de datos). Una máquina no debería enviar datagramas mayores a no ser que tenga la certeza de que van a ser aceptados por la máquina destino.

En caso de fragmentación este campo contendrá el tamaño del fragmento, no el del datagrama original.

Identificación (Identification): (16 bits) Identifica al Datagrama, permite implementar números de secuencias y reconocer los diferentes fragmentos de un mismo Datagrama, pues todos ellos comparten este número, es decir, que debido a la fragmentación, se crea la necesidad de la identificación de cada fragmento para así reconocer cada Datagrama enviado. El valor asignado en este campo debe ir en formato de red.

Bandera (Flags): (3 bits) Se utiliza sólo para especificar valores relativos a la fragmentación de paquetes:

bit **0**: Reservado; debe ser 0
bit **1**: **0** = Divisible, **1** = No Divisible (DF)
bit **2**: **0** = Último Fragmento, **1** = Fragmento Intermedio (le siguen más fragmentos) (MF)

La indicación de que un paquete es indivisible debe ser tenida en cuenta bajo cualquier circunstancia. Si el paquete necesitara ser fragmentado, no se enviará.

Fragmentos de compensación (Frag Offset): (13 bits) Campo denominado Fragmentos de compensación, nos indica donde fue fragmentado el Datagrama, medido en unidades de 8 bytes.

Tiempo de Vida TTL (Time To Live): (8 bits) Indica el máximo número de enrutadores que un paquete puede atravesar. Cada vez que algún nodo procesa este paquete disminuye su valor en 1 como mínimo, una unidad. Cuando llegue a ser 0, el paquete será descartado.

Protocolo (Protocol): (8 bits) Especifica qué protocolo de alto nivel se empleó para construir el mensaje transportado en el campo datos del Datagrama IP.

Suma de comprobación de cabecera (Checksum): (16 bits) Se recalcula cada vez que algún nodo cambia alguno de sus campos (por ejemplo, el Tiempo de Vida). El método de cálculo intencionadamente simple consiste en sumar cada palabra de 16 bits de la

cabecera (considerando valor 0 para el campo de suma de control de cabecera), si es necesario repetir el proceso con el resultado hasta obtener un valor inferior a 16 bits, y hacer el complemento a 1 del valor resultante.

Direcciones IP de la fuente y del destino (Source and destination IP Address): (16 bits/cada campo) Campo que nos sirve para indicar la dirección origen y destino del paquete.

Opciones IP (IP Options): (Opcional) Utilizado para funciones de administración solicitadas por el emisor.

Campo de relleno (Padding): este campo es de relleno, pues sólo con ceros se asegura que el final del Header sea de 32 bits.

Datos (Data): (variable) En este campo están los datos a transportarse, deben ser múltiplos de 8 bits, pudiendo tener como tamaño máximo 65535 bytes incluida la cabecera.

1.2.2 DIRECCIONAMIENTO IP

Para que se comuniquen dos sistemas, deben identificarse y ubicarse entre sí. En la figura 1.19 se puede observar un ejemplo de agrupación de direcciones, en donde se tiene el grupo A y B para identificar la red y la secuencia numérica de host individuales.

La combinación de letra (dirección de red) y el número (dirección de host) forman una dirección única para cada dispositivo del Grupo (red). Un computador puede estar conectado a más de una red. En este caso, se le debe asignar al sistema más de una dirección. Cada dirección identificará la conexión del computador a una red diferente. No se suele decir que un dispositivo tiene una dirección sino que cada uno de los puntos de conexión (o interfaces) de dicho dispositivo tiene una dirección en una red. Esto permite que otros computadores localicen el dispositivo en una determinada red.

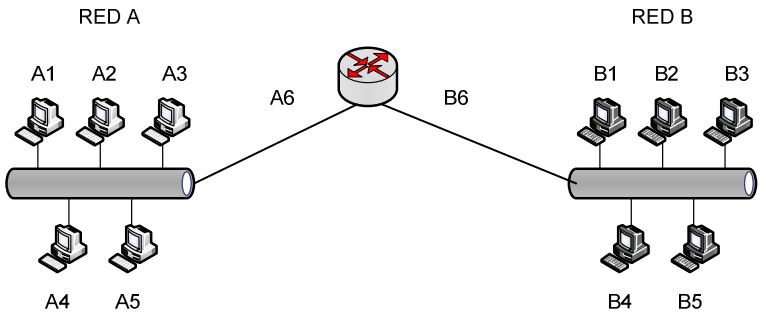

Figura. 1.19. Ejemplo de agrupamiento de direcciones

Cada computador conectado a una red TCP/IP debe recibir un identificador exclusivo o una dirección IP. Esta dirección, que opera en la Capa 3, permite que un computador localice otro computador en la red. Todos los computadores también cuentan con una dirección física exclusiva, conocida como dirección MAC (Media Access Control Address). Estas son asignadas por el fabricante de la tarjeta de interfaz de la red. Las direcciones MAC operan en la Capa 2 del modelo OSI.

1.2.2.1. DIRECCIONES IPv4 [17]

Las direcciones IPv4 se expresan por un número binario de 32 bits permitiendo un espacio de direcciones posibles de 4.294.967.296 (2^{32}). Las *direcciones IP* se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto está comprendido en el rango de 0 a 255.

En la expresión de direcciones IPv4 en decimal se separa cada octeto por un carácter único ".". Cada uno de estos octetos puede estar comprendido entre 0 y 255, salvo algunas excepciones. Los ceros iníciales, si los hubiera, se pueden obviar.

En 1981 el direccionamiento IP fue revisado y se introdujo la arquitectura de clases .En esta arquitectura hay tres clases de direcciones IP: clase A, clase B y clase C.

[17] "*Dirección IP*" http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP

- En una red de **clase A**, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{24} - 2 (se excluyen la dirección reservada para broadcast (últimos octetos en 255) y de red (últimos octetos en 0), es decir, 16 777 214 hosts.

- En una red de **clase B**, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es 2^{16} - 2, o 65 534 hosts.

- En una red de **clase C**, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los hosts, de modo que la cantidad máxima de hosts es 2^{8} - 2, ó 254 hosts.

Clase	**Rango**	**# de Redes**	**# de Host Por Red**	**Mascara de Red**	**Broadcast ID**
A	0.0.0.0-127.255.255.255	128	16777214	255.0.0.0	x.255.255.255
B	128.0.0.0-191.255.255.255	16384	65534	255.255.0.0	x.x.255.255
C	192.0.0.0-223.255.255.255	2097150	254	255.255.255.0	x.x.x.255
(D)	224.0.0.0-239.255.255.255	Histórico			
(E)	240.0.0.0-255.255.255.255	Histórico			

Tabla 1.4. Clases de direcciones IP.

- La dirección 0.0.0.0 es reservada para identificación local.
- La dirección que tiene los bits de host iguales a cero sirve para definir la red en la que se ubica. Se denomina **dirección de red**.

- La dirección que tiene los bits correspondientes a host iguales a uno, sirve para enviar paquetes a todos los hosts de la red en la que se ubica. Se denomina **dirección de broadcast**.

- Las direcciones 127.x.x.x se reservan para designar la propia máquina. Se denomina **dirección de bucle local** o **loopback**.

1.2.2.2. DIRECCIONES PRIVADAS [17]

Hay ciertas direcciones en cada clase de dirección IP que no están asignadas y que se denominan direcciones privadas. Las direcciones privadas pueden ser utilizadas por los hosts que usan traducción de dirección de red (NAT) para conectarse a una red pública o por los hosts que no se conectan a Internet. En una misma red no pueden existir dos direcciones iguales, pero sí se pueden repetir en dos redes privadas que no tengan conexión entre sí o que se conecten mediante el protocolo NAT. Las direcciones privadas son:

- Clase A: 10.0.0.0 a 10.255.255.255 (8 bits red, 24 bits hosts).
- Clase B: 172.16.0.0 a 172.31.255.255 (16 bits red, 16 bits hosts). 16 redes clase B contiguas, uso en universidades y grandes compañías.
- Clase C: 192.168.0.0 a 192.168.255.255 (24 bits red, 8 bits hosts). 256 redes clase C contiguas, uso de compañías medias y pequeñas además de pequeños proveedores de internet (ISP).

Muchas aplicaciones requieren conectividad dentro de una sola red, y no necesitan conectividad externa. En las redes de gran tamaño a menudo se usa TCP/IP. Por ejemplo, los bancos pueden utilizar TCP/IP para conectar los cajeros automáticos que no se conectan a la red pública, de manera que las direcciones privadas son ideales para estas circunstancias. Las direcciones privadas también se pueden utilizar en una red en la que no haya suficientes direcciones públicas disponibles.

[17] "*Dirección IP*" http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP

1.2.3 EVOLUCIÓN DE IPv4 a IPv6 [18]

Actualmente la red utiliza mayoritariamente la versión 4 del protocolo de Internet. Sin embargo, el gran número de usuarios, dispositivos, aplicaciones, servicios, y en general el éxito de Internet en sí misma, está llevando la versión 4 a sus límites.

Se habla de escasez de direcciones, y aunque no es del todo correcto literalmente hablando, en la práctica, las restricciones que impiden que un usuario pueda tener no sólo una sino múltiples direcciones para todos sus dispositivos y aplicaciones, dificultan y retardan el crecimiento de la red, y por tanto la creación de nuevas aplicaciones, con más posibilidades que las actuales.

IPv4, ha servido con éxito por más de 20 años pero comienza a dar señales de encontrarse al límite de su diseño, los 32 bits que se tienen para el direccionamiento, ya no son suficientes y carece además de algunas características deseables por usuarios y aplicaciones actuales, tales como movilidad, seguridad y calidad de servicio.

Por ello se comenzó, en los años 90, la búsqueda de un sustituto, el cual permitirá la continua evolución de Internet, y así surgió IPv6, la versión 6 del protocolo de Internet.
Diseñado por Steve Deering de Xerox PARC y Craig Mudge, IPv6 está destinado a sustituir al estándar IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir el crecimiento de Internet y su uso, especialmente en China, India, y otros países asiáticos densamente poblados.

IPv6 y tiene como ventaja fundamental un amplio espacio de direcciones, utiliza direcciones de fuente y destino de 128 bits, muchas más direcciones que las que provee IPv4 con 32 bits. También se agregan varias funciones adecuadas a la nueva Internet tales como: calidad de servicio y clase de servicio, autentificación y privacidad, autoconfiguración, etc. Esta versión mejorará el servicio globalmente; por ejemplo,

[18] "*Comparación entre IPV4 - IPV6*"
http://www.ilustrados.com/documentos/eb-Comparacion%20IP4%20y%20IPV6.pdf

proporcionando a futuras celdas telefónicas y dispositivos móviles con sus direcciones propias y permanentes.

Las versiones de la 0 a la 3 están reservadas o no fueron usadas y la versión 5 fue usada para un protocolo experimental orientado al flujo de streaming que intentaba soportar voz, video y audio. Otros números han sido asignados, usualmente para protocolos experimentales, pero no han sido muy extendidos.

1.2.4. IPv6 (PROTOCOLO DE INTERNET VERSION 6) [19]

IPv6, es el protocolo de internet versión 6, se encuentra definido en el RFC 2460, y se creó para reemplazar al protocolo de internet versión 4 (IPV4), que es usado en la actualidad para que gran variedad de equipos puedan acceder a internet, ya que IPV4 presenta en la actualidad un limitante en cuanto al número de direcciones de red, de esta manera impediría el crecimiento de internet.

A través del protocolo de internet versión 4 solo teníamos la posibilidad de 2^{32} direcciones de red es decir 4.294.967.296, con este número nos resultaría incorrecto el brindar a cada equipo como PC, Palms, vehículos de una dirección IP, para su acceso.
El protocolo IPV6 permite proporcionar 2^{128} direcciones de red, es decir un valor de 340.282.366.920.938.463.463.374.607.431.768.211.456 o 340 sextillones de direcciones a nivel mundial.

Los nodos IPv6 se configuran automáticamente al conectarse a una red ruteada de IPv6, a través de los mensajes de los routers ICMPv6 (Internet Control Message Protocol v6), en caso de que la configuración automática de direcciones libres, no sea la apropiada para una determinada aplicación se puede utilizar DHCPv6 (Dynamic Host Configuration Protocol), o bien se puede configurar de manera estática a los nodos.

IPv6 no implementa broadcast, que es la capacidad de enviar un paquete a los nodos conectados del enlace, pero este efecto se puede obtener enviando un paquete al grupo

[19] IPv6, "*Protocolo de Internet Versión 6*" http://es.wikipedia.org/wiki/IPv6

de multicast de enlace local de todos lo hosts, por lo tanto la dirección de red más alta de broadcast en IPv4 se considera una dirección normal en IPv6.

El cifrado y autenticación son la parte integral y obligatorio de IPv6, a través de IPsec(Internet Protocol Security).

En el protocolo IPv4 se tenía un límite para los paquetes de 64KB de carga útil, en cambio IPv6 puede soportar paquetes que superen este limite a base de un soporte opcional, los paquete que superan este límite se les conoce como jumbogramas y pueden llegar a ser de hasta 4GB, a través de estos se puede obtener mayor eficiencia en redes de altos MTU.

1.2.4.1. CABECERA IPv6 [20]

Los primeros 40 bytes son la cabecera del paquete y contiene los siguientes campos:

A continuación se describe los segmentos:

OFFSET DEL OCTETO		0								1								2								3							
	Bit Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				Clase de Trafico								Etiqueta de Flujo																			
4	32	Cabecera Siguiente																Cabecera Siguiente								Limite de Saltos							
8	96	Direccion de Origen																															
C	128																																
10	160																																
14	192	Direccion de Destino																															
1C	224																																
20	256																																
24	288																																

Figura. 1.20. Cabecera IPv6

Versión: 6 debido a que es IPv6

Prioridad: se utiliza para diferenciar entre paquetes a los cuales se les puede controlar el flujo y a los que no se puede.

[20] "Cabecera IPv6" http://www.dei.uc.edu.py/tai2003/ipv6/cabecera.htm

Etiqueta de Flujo: Aún es experimental, pero se usará para permitir a un origen y a un destino establecer una seudoconexión con prioridades y requisitos particulares.

Longitud de Carga Útil: Indica cuantos bytes siguen en la cabecera de 40 bytes (es lo que en el IPv4 era la Longitud Total).

Cabecera siguiente: indica cuales de la 6 cabeceras de extensión, entre las cabeceras se puede tener: opción salto por salto, enrutamiento, fragmentación, verificación de autenticidad, carga útil cifrada seguridad, opciones de destino.

Límite de Saltos: Se usa para evitar que los paquetes vivan eternamente. Campo de Dirección de origen. Campo de Dirección de Destino.

En el protocolo anterior IPv4 la fragmentación de paquetes la podían realizar los Routers, pero en la versión 6 la fragmentación se puede realizar solo en el nodo origen, además las opciones también desaparecen de la cabecera estándar, y se especifican en el campo de Cabecera Siguiente.

1.2.4.2. DIRECCIONAMIENTO IPv6 [19]

De acuerdo a las direcciones IPv6 que son 2^{128} que corresponde a 32 dígitos hexadecimales, y cada uno de estos dígitos puede tomar 16 valores, por lo general una dirección de esta comprendida de dos partes, una de 64bits que es un prefijo, y otra de 64bits que es la que identifica la interfaz, y en la mayoría de la veces esta se genera partiendo de la dirección MAC(de la interfaz) a que se le asignara la dirección.

NOTACIÓN PARA LAS DIRECCIONES IPV6

Las direcciones IPv6, de 128 bits de longitud, se escriben como ocho grupos de cuatro dígitos hexadecimales. Por ejemplo:

2001:0db8:85a3:08d3:1319:8a2e:0370:7334 es una dirección IPv6 válida.

[19] IPv6, "*Protocolo de Internet Versión 6*" http://es.wikipedia.org/wiki/IPv6

Es posible comprimir un grupo de 4 dígitos si estos dígitos tienen el valor “0000”, por ejemplo,

2001:0db8:85a3:0000:1319:8a2e:0370:7344
2001:0db8:85a3::1319:8a2e:0370:7344

Siguiendo esta regla, si más de dos grupos consecutivos son nulos, también pueden comprimirse como "::". Si la dirección tiene más de una serie de grupos nulos consecutivos la compresión sólo se permite en uno de ellos. Así, las siguientes son representaciones posibles de una misma dirección ejemplo:

2001:0DB8:0000:0000:0000:0000:1428:57ab
2001:0DB8:0000:0000:0000::1428:57ab
2001:0DB8:0:0:0:0:1428:57ab
2001:0DB8:0::0:1428:57ab
2001:0DB8::1428:57ab

Pero si tendrían la siguiente dirección

2001::25de::cade

Esta no sería válida debido a que no sabríamos cuantos grupos nulos existía a cada lado.

IDENTIFICACIÓN DE LOS TIPOS DE DIRECCIONES

Los tipos de direcciones IPv6 pueden identificarse tomando en cuenta los primeros bits de cada dirección.

:: La dirección con todo ceros se utiliza para indicar la ausencia de dirección, y no se asigna ningún nodo.

::1 La dirección de loopback es una dirección que puede usar un nodo para enviarse paquetes a sí mismo (corresponde con127.0.0.1 de IPv4). No puede asignarse a ninguna interfaz física.

::1.2.3.4 La dirección IPv4 compatible se usa como un mecanismo de transición en las redes duales IPv4/IPv6. Es un mecanismo que no se usa.

::ffff:0:0 La dirección IPv4 mapeada se usa como mecanismo de transición en terminales duales.

fe80:: El prefijo de *enlace local* (*link local*) específica que la dirección sólo es válida en el enlace físico local.

fec0:: El *prefijo de emplazamiento local* (*site-local prefix*) específica que la dirección sólo es válida dentro de una organización local. La RFC 3879 lo declaró obsoleto, estableciendo que los sistemas futuros no deben implementar ningún soporte para este tipo de dirección especial. Se deben sustituir por direcciones Local IPv6 Unicast.

ff00:: El prefijo de multicast.

1.3 CAMINO HACIA LA CONVERGENCIA DE NIVELES:

ARQUITECTURA IP SOBRE ATM [21]

IP fue ganando terreno como protocolo de red a otras arquitecturas en uso en la época de los 90s como (SNA, IPX, AppleTalk, OSI...). El crecimiento explosivo de la Internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. La respuesta de los NSPs (Network Service Provider) fue el incremento del número de enlaces y de la capacidad de los mismos, aprovechando mejor los recursos de red y utilizando eficazmente el ancho de banda de todos los enlaces.

[21] BARBERÁ, José, "*MPLS: Una arquitectura de backbone para la Internet del siglo XXI*"

Buscando dar solución a los problemas de crecimiento de los NSPs, se busco combinar de diferentes maneras la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los Routers IP, obteniendo así nuevas redes con mayores velocidades (155 Mbps) y con facilidad de implementación de soluciones de tráfico.

La integración de IP sobre ATM utilizando circuitos virtuales ya sean permanentes conmutados otorga un esquema de entrega de datos rápido a través de una red confiable, con ventajas como reserva de recursos, diferentes clases de direccionamiento y con comunicaciones multicast.

El funcionamiento IP/ATM supone la superposición de una topología virtual de routers IP sobre una topología real de conmutadores ATM. El backbone ATM se presenta como una nube central (el núcleo) rodeada por los routers de la periferia. Cada router comunica con el resto mediante los circuitos virtuales permanentes (PVCs) que se establecen sobre la topología física de la red ATM. Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los routers de la periferia.

Estos, sin embargo, desconocen la topología real de la infraestructura ATM que sustenta los PVCs. Los routers ven los PVCs como enlaces punto a punto entre cada par. En la Figura 1.21 se representa un ejemplo en el que se puede comparar la diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta a la anterior.

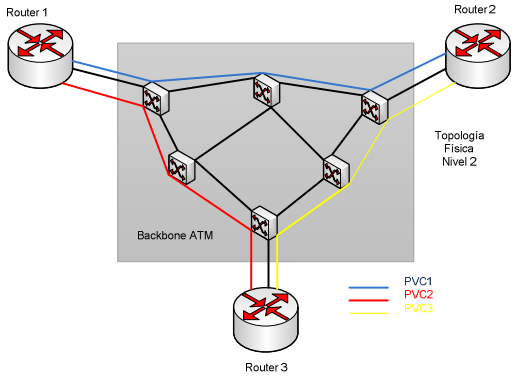

Figura. 1.21. Topología física ATM y topología lógica IP superpuesta

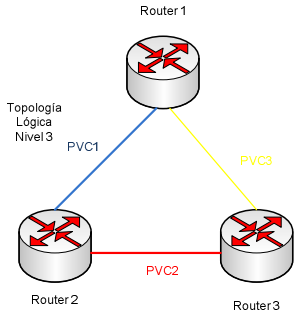

Figura 1.22. Topología Lógica IP

Los protocolos IP de control se ejecutan directamente sobre los conmutadores ATM, los cuales reenvían los paquetes usando intercambio de etiquetas, pero los protocolos IP de control se encargan de establecer las tablas de reenvío y reservar los recursos.

La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y routing) y el envío de las celdas por hardware (conmutación). En realidad, los PVCs se establecen a base de intercambiar etiquetas en cada conmutador de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los correspondientes PVCs.

En la figura 1.23 se representa el modelo IP/ATM con la separación de funciones entre lo que es routing IP en el nivel 3 (control y envío de paquetes) y lo que es conmutación en el nivel 2 (control/señalización y envío de celdas). Aunque se trata de una misma infraestructura física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y proporcionadas para dos finalidades totalmente distintas.

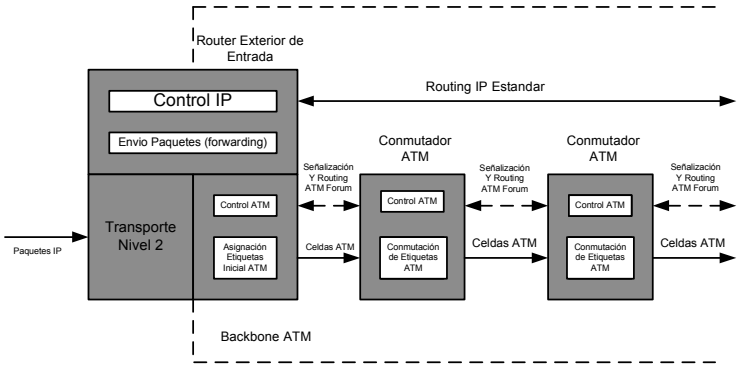

Figura. 1.23. Modelo funcional IP sobre ATM

La solución de superponer IP sobre ATM permite aprovechar la infraestructura ATM existente. Las ventajas inmediatas son el ancho de banda disponible y la rapidez de transporte de datos que proporcionan los conmutadores. En los casos de NSPs de primer nivel, ellos poseen y operan el backbone ATM al servicio de sus redes IP. Los caminos físicos de los PVCs se calculan a partir de las necesidades del tráfico IP, utilizando la clase de servicio ATM UBR (Unspecified Bit Rate), ya que en este caso el ATM se utiliza solamente como infraestructura de transporte de alta velocidad. La ingeniería de tráfico se hace a base de proporcionar a los routers los PVCs necesarios, con una topología lógica entre routers totalmente mallada.

El modelo IP/ATM tiene también sus inconvenientes: hay que gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio mayores costos de gestión global de sus redes. Existe, además, lo que se llama la "tasa impuesta por la celda", un overhead aproximado del 20% que causa el transporte de datagramas IP sobre las celdas ATM y que reduce en ese mismo porcentaje el ancho de banda disponible. Por otro lado, la solución IP/ATM presenta los típicos problemas de crecimiento exponencial n x (n-1) al aumentar el número de nodos IP sobre una topología completamente mallada. Por ejemplo, en una red con 5 routers externos con una topología virtual totalmente mallada sobre una red ATM, son necesarios 5 x 4 =20 PVCs (uno en cada sentido de transmisión). Si se añade un sexto router se necesitan 10 PVCs más para mantener la misma estructura (6 x 5=30).

Se puede decir que el modelo IP/ATM, si bien presenta ventajas evidentes en la integración de los niveles 2 y 3, lo hace de modo discontinuo, a base de mantener dos redes separadas. MPLS, logra esa integración de niveles sin discontinuidades.

1.3.1 ENCAPSULAMIENTO DE DATAGRAMAS IP SOBRE ATM

Para comunicarse con las redes ATM el transporte de paquetes IP será dentro del campo de carga útil de AAL5 (ATM Adaptation Layer 5). Para lo cual este campo presenta las siguientes características:

• Servicio confiable
• Servicio no confiable
• Fragmentación de datos en bloques y segmentos
• Operación multipunto
• Modo mensaje y modo flujo AAL5 especifica un formato de paquete con un tamaño máximo de 64 Kbytes de datos de usuario.

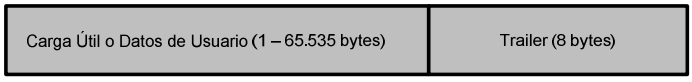

Figura. 1.24. Formato de paquetes básico que AAL5 acepta y entrega

La información de control que coloca la capa de adaptación AAL5 dentro del formato de paquete se encuentra al final de los datos en un campo de 8 bytes denominado Trailer. Puesto que AAL5 no tiene un campo en el Trailer donde se indique el tipo de protocolo a transportarse, los extremos deben previo acuerdo fijar un método para conocer qué tipo de información se transmitirá para lo cual se ha implementado dos tipos de multiplexación.

Multiplexación por ´Circuito Virtual VC, se encarga de fijar la condición de que el circuito virtual será usado solamente para un único protocolo durante esa conexión, de esta manera se evita colocar información adicional; pero si se tiene que enviar más de un

protocolo de alto nivel, en la misma sesión se duplicarán los circuitos virtuales ya que por cada protocolo se debe crear un circuito virtual por separado.

Multiplexación de Control Lógico del Enlace LLC (Link Logical Control) se encarga de introducir información en el campo de datos para indicar el tipo de Carga útil o datos de usuario (1 – 65.535 bytes) Trailer (8 bytes) protocolo a enviarse. De esta manera puede usarse un solo circuito virtual para protocolos distintos, permitiendo así que todo tráfico pueda enviarse por un solo circuito; pero para esto se debe incluir información de cada tipo de protocolo, además de que al no existir distinción de información todos los datos viajan con igual prioridad y retraso.

TCP/IP tiene un tamaño máximo de datagrama de 9180 bytes, si este es más grande, el protocolo IP lo fragmenta para entregar cada fragmento a AAL5, esta capa de adaptación coloca el trailer y segmenta la información en bloques de 48 bytes, para enviarlos como celdas de tamaño fijo de 53 bytes a la red ATM.

La subcapa Convergente Sublayer (CS) de AAL5 recibe los fragmentos de IP y le añade un relleno de longitud variable (PAD) y un trailer de 8 bytes formando una trama que se la llama Unidad de Protocolo de Datos (PDU). El PAD debe ser lo suficientemente largo para asegurar que el PDU resultante sea exactamente divisible para 48 bytes. La subcapa Segmentation and Reassembly (SAR) divide el PDU de la subcapa CS en bloques de 48 bytes.

Luego de este proceso se añaden 5 bytes de cabecera para formar la celda ATM de 53 bytes que luego será transmitida por la red ATM. La figura 1.25 que se muestra a continuación detalla el proceso de Encapsulamiento de Datagramas IP utilizando AAL5.

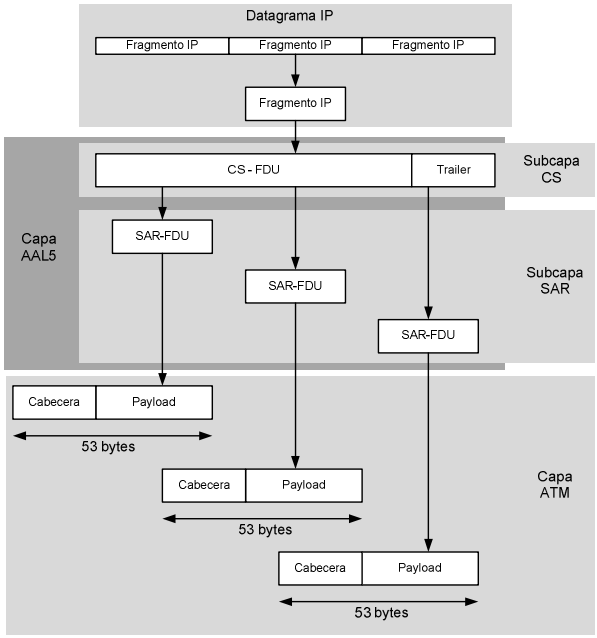

Figura 1.25. Encapsulamiento de Datagramas IP utilizando AAL5

BIBLIOGRAFÍA – CAPÍTULO 1

[1] WIKIPEDIA, "*Jerarquía Digital Plesiocrona*", mayo 2011 http://es.wikipedia.org/wiki/Jerarqu%C3%ADa_Digital_Plesi%C3%B3crona

[2] OCHOA, Edgar, Material de la asignatura "*Comunicaciones III*", Universidad Politécnica Salesiana, 5 año.

[3] WIKIPEDIA, SDH, "*Jerarquía Digital Síncrona*", mayo 2011 http://es.wikipedia.org/wiki/Jerarqu%C3%ADa_digital_s%C3%ADncrona

[4] WIKIPEDIA,TDMA, "*Multiplexación por División de Tiempo,* mayo 2011 http://es.wikipedia.org/wiki/Acceso_m%C3%BAltiple_por_divisi%C3%B3n_de_tiempo

[5] ISDN, "*Red digital de servicios integrados*", mayo 2011 http://www.frm.utn.edu.ar/comunicaciones/isdn.html

[6] ISDN, "*Red digital de servicios integrados*", mayo 2011 http://personales.mundivia.es/jtoledo/angel/SE.HTM

[7] WIKIPEDIA, "*Norma X.25*", mayo 2011 http://es.wikipedia.org/wiki/Norma_X.25

[8] "*Redes X.25*", mayo 2011 http://www.angelfire.com/wi/ociosonet/5.html

[9] D'SOUSA, Carmen, "*Tecnología Frame Relay*", mayo 2011 http://www.monografias.com/trabajos11/frame/frame.shtml

[10] WIKIPEDIA, ATM, "*Modo de Transferencia Asíncrona*", mayo 2011

http://es.wikipedia.org/wiki/Asynchronous_Transfer_Mode

[11] "*Redes ATM*", mayo 2011
http://www.angelfire.com/wi/ociosonet/29.html

[12] SOTO, Miguel, "Protocolo *TCP/IP*", mayo 2011
http://usuarios.multimania.es/janjo/janjo1.html

[13] TRAVERSO, Damián, "*Tecnologías en las Redes de Acceso*", junio 2011
http://www.monografias.com/trabajos13/tecnacc/tecnacc.shtml

[14] VALERA, Isabel, "*Tecnología DSL*", junio 2011
http://www.monografias.com/trabajos5/tecdsl/tecdsl.shtml

[15] WIKIPEDIA**,** IP, "*Protocolo de Internet*", junio 2011
http://es.wikipedia.org/wiki/Internet_Protocol

[16] WIKIPEDIA**,** "*Cabecera IP*", junio 2011
http://es.wikipedia.org/wiki/Cabecera_IP

[17] WIKIPEDIA**,** "*Dirección IP*", junio 2011
http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP

[18] PÉREZ, Jorge, y otros, "*Comparación entre IPV4 - IPV6*" , junio 2011
http://www.ilustrados.com/documentos/eb-Comparacion%20IP4%20y%20IPV6.pdf

[19] WIKIPEDIA**,** IPv6, "*Protocolo de Internet Versión 6*", junio 2011
http://es.wikipedia.org/wiki/IPv6

[20] VELÁSQUEZ, Ana y SAINEA, Fabio **"***Cabecera IPv6"*, junio 2011
http://www.dei.uc.edu.py/tai2003/ipv6/cabecera.htm

[21] BARBERÁ, José, "*MPLS: Una arquitectura de backbone para la Internet del siglo XXI*"
http://www.rediris.es/rediris/boletin/53/enfoque1.html

CAPITULO 2

METRO ETHERNET Y MPLS

2.1 ESTUDIO DE LA RED METRO ETHERNET Y LA CONVERGENCIA REAL MPLS.

2.1.1 INTRODUCCIÓN[1]

En los últimos años la tecnología Ethernet ha evolucionado muy rápidamente y se ha convertido en la tecnología dominante en las Redes de Área Local, sobre todo en el ámbito empresarial, manejando casi en su totalidad el tráfico de todas las empresas, utilizando millones de puertos Ethernet en Redes Metropolitanas o Redes Troncales (Backbones) de interconexión de LAN.

Las LAN con tecnología Ethernet no garantizan la mayoría de los parámetros necesarios para la obtención de Calidad en el Servicio tales como: disponibilidad, reordenamiento de tramas, duplicación de tramas, tiempo de vida de la trama, etc. Por lo tanto, Ethernet no fue diseñada pensando en la calidad de los servicios, por tal razón, la solución más extendida ha sido, sobredimensionar el sistema para que no se congestione. Aquí es donde entra MPLS (Multiprotocol Label Switching), una tecnología de conmutación de paquetes que se encuentra entre los niveles 2 y 3 del modelo OSI, lo que posibilita mejorar la funcionalidad de capa 2 en Ethernet sin sacrificar sus prestaciones, puesto que ofrece una clasificación y conducción rápida de paquetes, y dispone de un mecanismo de túnel eficiente. EoMPLS (Ethernet Over MPLS) ofrece servicios de determinación de rutas en grandes redes, proporciona calidad de servicios, establece grupos de usuarios privados, ancho de banda reservado, mecanismos de seguridad e ingeniería de tráfico. Ambas arquitecturas se complementan perfectamente: el encapsulado MPLS y la conmutación Ethernet en la red metropolitana, ofreciendo conectividad punto a punto y el soporte para un servicio de LAN privada virtual (VPN).

[1] http://sistemas.itlp.edu.mx/ponencias/3.pdf

2.1.2. RED METRO ETHERNET[2]

La Red Metro Ethernet, es una arquitectura tecnológica destinada a brindar conectividad WAN/MAN de nivel 2, mediante UNIs Ethernet. En este sentido Bob Metcalfe desarrolla en 1972 un sistema para permitir la comunicación entre computadoras e impresoras, constituyéndose en la primera red de área local (LAN).

Se quiso que esta red sea tan compatible y versátil independientemente sobre el medio físico en el cual funcione, denominada en su inicio por su creador como “Ethernet”, con el paso del tiempo fue estandarizado por la IEEE bajo la norma “Ethernet 802.3”, dominando las redes LAN por su simplicidad, prestaciones y bajo coste.

Los órganos de estandarización (IEEE, IETF, ITU) y los convenios entre fabricantes, han jugado un papel muy importante en la evolución de Ethernet. De tal forma que se ha creado el MEF (Metro Ethernet Forum), organismo encargado únicamente a definir Ethernet como servicio metropolitano, llegando a soportar estas redes una amplia gama de servicios, aplicaciones, contando con mecanismos donde se incluye el soporte al tráfico en tiempo real, como puede ser la Telefonía IP y Video IP.

2 .1.2.1. CARACTERISTICAS DE UNA RED METRO ETHERNET [3]

A continuación se citan algunas características que Ethernet presenta.

VENTAJAS

Configuración rápida: Ethernet es flexible y fácilmente ampliable, ofrece una gran variedad de velocidades de transmisión, (desde 10 Mbps hasta 10 Gbps), en incrementos de 1 Mbps o incluso menos.

---

[2] “*Redes Metro Ethernet*” http://www.coit.es/publicaciones/bit/bit149/64-66.pdf
[3] “*Redes Metro Ethernet*” http://es.wikipedia.org/wiki/Metro_Ethernet

Interconexión: Facilidad de comunicación e integración con otras redes, debido a que el 98% de las redes LAN están implementadas sobre Ethernet, no siendo necesaria una conversión de protocolos entre redes LAN y MAN.

Bajo coste: Los costes de implementación, configuración y mantenimiento de infraestructura de red Ethernet (cable, conectores, tarjetas, equipos de interconexión, etc.) son mucho menores. Ethernet sólo requiere conectar los equipos, sin configuraciones complejas.

DESVENTAJAS

La distancia: Era una gran limitación ya que las redes Ethernet sobre cobre solo podían extenderse hasta 100 m antes de que la atenuación de la señal causara una degradación seria en la calidad de la comunicación.

La fiabilidad y Redundancia: Ethernet no era considerado fiable, los mecanismos de redundancia y recuperación ante fallos, como Spanning Tree, que consistía en la eliminación de bucles infinitos, eran lentos e ineficientes.

El crecimiento: El broadcast necesario y la necesidad de aprendizaje de direcciones físicas (MAC) de todos los usuarios en todos los Nodos de Red, ponían en duda la capacidad de crecimiento de la tecnología Ethernet.

La seguridad: Ethernet se presentaba como una tecnología de medio compartido en el que los usuarios fácilmente podían acceder al tráfico de otros, estando en riesgo la confidencialidad de la información de los mismos.

AVANCES

En la actualidad la tecnología nos brinda las herramientas necesarias para cubrir dichas limitaciones que presentaba Ethernet y que citábamos anteriormente; es decir:

La distancia: Este aspecto ya no limita la implementación de Ethernet en sitios geográficamente distantes, porque las tecnologías ópticas y de radio nos permiten transportar Ethernet a centenares de Km.

La fiabilidad y la redundancia: Esto ya a dejado de ser un problema puesto que los fabricantes de equipos Ethernet aportan ya soluciones fiables con tiempos de protección similares a la de la telefonía tradicional.

El crecimiento: Gracias a la evolución de la tecnología misma, las redes Ethernet se han incrementado en magnitudes muy elevadas.

La seguridad: Se ha dado soluciones a este problema mediante técnicas de tunelización.

2.1.2.2. MODELO BASICO DE UNA RED METRO ETHERNET[4]

El modelo básico de una red Metro Ethernet está formado por tres componentes como se puede apreciar en la figura 2.1:

- CE (Customer Equipment): El dispositivo instalado en el lado del usuario que puede ser un Switch o un Router. Los usuarios pueden acceder a la red a través de el.
- UNI (User Network Interfaz): La interfaz de conexión del usuario a la red; es decir es el conocido puerto Ethernet RJ-45.
- MEN (Metro Ethernet Network): La Red Metropolitana.

[4] *"Metro Ethernet"* http://www.monografias.com/trabajos17/metro-ethernet/metro-ethernet.shtml

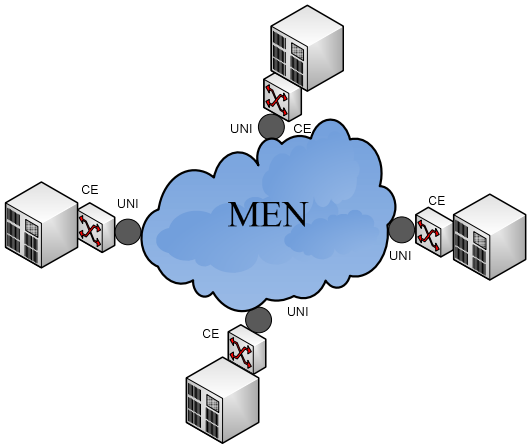

Figura 2.1 Modelo Básico de una Red Metro Ethernet

En la red Metropolitana los servicios pueden soportar una variedad de protocolos y tecnologías de transporte tales como SONET, DWDM, MPLS, GFP, etc.

2.1.2.3. APLICACIONES EN UNA RED METRO ETHERNET [2]

Ethernet Virtual Connection (EVC): Se define como a la asociación entre dos o más puntos (Interfaces UNI) en la red MEN. Los EVCs equivalen a los Circuitos Virtuales Privados (PVC) en Frame Relay o Virtual Chanel en ATM (VC).

Un **ECV** tiene la función de conectar dos o más sitios (UNIs) como ya dijimos, pero habilitando la transferencia de tramas Ethernet entre ellos e impidiendo la transferencia de tramas entre usuarios que no son parte del mismo EVC, obteniendo así seguridad y privacidad.

Redes de Área Local Virtual (VLAN): Una VLAN es una red de Área local (LAN) virtual que proporciona enrutamiento de tramas a nivel 2. El estándar IEEE 802.1 Q especifica el formato de la trama Ethernet, donde se incluye un campo para identificar la VLAN a la que pertenece (VLAN ID).

En una Red Metropolitana MEN, el VLAN ID nos permite crear EVCs Ethernet, en donde cada uno está identificado con una etiqueta equivalente a un VLAN ID distinto.

[2] "*Redes Metro Ethernet*" http://www.coit.es/publicaciones/bit/bit149/64-66.pdf

IEEE 802.1 AD O Q-IN-Q: Es un estándar experimental que está en investigación, y consiste en la multiplexación de las VLANs de cliente en VLANs del operador de la MEN.

MAC-in-MAC: Consiste en la "tunelizaciòn" de las tramas Ethernet de cliente en tramas Ethernet del operador de la MEN. En la actualidad se está buscando su estandarización.

2.1.2.4. SERVICIOS ETHERNET [5]

Un **EVC** puede ser usado para construir Virtual Private Network (VPN) de nivel 2. El MEF (Metro Ethernet Forum) ha definido dos tipos de EVC:

- Punto a Punto (E-Line)
- Multipunto a Multipunto (E-LAN)

2.1.2.4.1. SERVICIO PUNTO A PUNTO (E-LINE).

Este servicio proporciona un EVC punto a punto entre dos interfaces UNI, se utiliza para proporcionar una conexión Ethernet punto a punto. Dentro de E-Line se incluye una amplia gama de servicios, el más sencillo consiste en un ancho de banda simétrico para la transmisión bidireccional de datos, sin garantizar la seguridad de los mismos. Al igual que los que con los PVCs de Frame Relay o ATM, se pueden multiplexar varios EVCs punto a punto en un mismo puerto físico (UNI).

E-Line se puede utilizar para crear los mismos servicios que puede ofrecer una red Frame Relay (a través de PVCs) o una línea alquilada punto a punto, pero proporcionando un ancho de banda mucho mayor.

---

[5] "Las redes de Área Metropolitana basadas en Ethernet en el Ecuador" http://www.docstoc.com/docs/25917668/LAS-REDES-DE-AREA-METROPOLITANA-BASADAS-EN-ETHERNET-EN

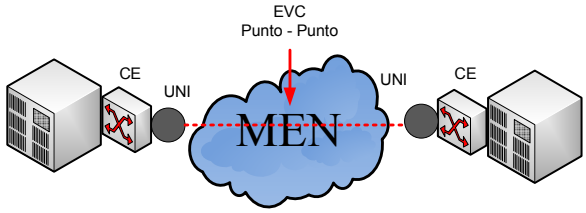

Figura 2.2 Servicio E-Line

2.1.2.4.2. SERVICIO MULTIPUNTO A MULTIPUNTO (E-LAN).

Este servicio proporciona conectividad multipunto a multipunto; es decir conectara dos o más interfaces UNI. Los datos enviados desde un UNI llegara a 1 o más UNI destino, en donde cada uno de ellos esta conectando a un EVC multipunto.

A medida que crece la red y se van adicionando más UNI, estos se conectan al mismo EVC multipunto, simplificándose la configuración de la misma.Desde el punto de vista del usuario, la E-LAN se comporta como una LAN y al igual que E-Line, este tipo de servicio abarca una gama muy amplia de servicios.

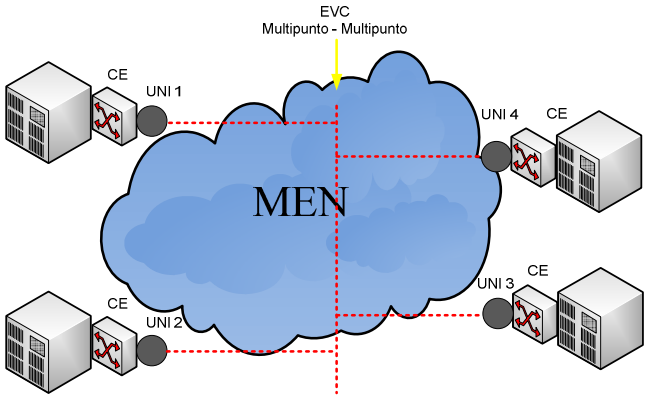

Figura 2.3 Servicio E-LAN

2.1.2.5. CLASES DE SERVICIOS ETHERNET (CoS) [4]

Metro Ethernet provee varias clases de servicios al usuario, en donde cada una puede ofrecer diferentes niveles de desempeño, como retardos, jitter y tramas perdidas. Si un proveedor de servicio soporta múltiples clases de servicio entre UNIs, el tráfico y los parámetros de desempeño deben ser los especificados para cada clase. A continuación se citan y definen las clases de servicio.

- Puerto Físico
- CE-VLAN CoS (802.1p)
- DiffServ/IP TOS

Puerto Físico: En este caso todo el tráfico que entra y sale de un puerto físico recibe la misma clase de servicio. Si se requieren múltiples clases de servicio, se separan tantos puertos físicos como sean requeridos, cada uno con su clase de servicio.

CE-VLAN CoS (802.1p): Esta clase de servicio utiliza 802.1Q para etiquetar las tramas, cuando se utiliza hasta 8 clases de servicio pueden ser indicadas. El proveedor de servicio especifica el ancho de banda y los parámetros de desempeño.

DiffServ/IP TOS Values: Pueden ser usados para determinar la clase de servicio IP TOS, en general, es usada para proveer 8 clases de servicio conocidas como prioridad IP o prioridad de envio. DiffServ es definido como PHS (Per-hop behaviors), con una calidad de servicio más robusta cuando se compara con IP TOS y 802.1p. DiffServ provee 64 diferentes valores para determinar las clases de servicio. Casi todos los Routers y Switches soportan estas clases de servicio.

Soporte VLAN TAG: Las VLAN soportan una variedad de servicios Ethernet. Un UNI puede soportar tagged (etiquetado), Untagged (No etiquetado) o Tagged (etiquetado) y Untagged (No etiquetado)

[4] *"Metro Ethernet"* http://www.monografias.com/trabajos17/metro-ethernet/metro-ethernet.shtml

2.1.2.6. SERVICIO DE MULTIPLEXACION [4]

Este servicio se usa para utilizar varios canales virtuales (EVC) de diferentes velocidades simultáneamente en una sola conexión (UNI). Con este servicio se elimina la necesidad de tener diferentes interfaces físicas para tener diferentes velocidades de transmisión. Optimizando de esta manera el coste, puesto que la cantidad de equipos (Routers y Switches) necesarios se reduce, se minimiza el espacio y el cableado, y se simplifica la activación de servicios adicionales.

Figura 2.4 Servicio de Multiplexación para UNI A

2.2 EVOLUCION DE LAS REDES PRIVADAS VIRTUALES [5]

2.2.1 INTRODUCCION

Actualmente las redes se han convertido en el factor principal de las empresas, puesto que de ellas depende la comunicación de información útil entre las sucursales y oficinas remotas, cumpliendo con factores de calidad tales como seguridad, fiabilidad, alcance y velocidad. El tema de seguridad es muy importante, porque las redes han sido puestas a prueba por algunas personas dedicadas a robar información confidencial de las empresas con distintos propósitos. Es por esto que las organizaciones por más pequeñas que estas sean ya hablan de los famosos Firewalls y las VPNs.

Cuando una empresa desea enlazar o comunicar su oficina matriz con el resto de sucursales se enfrenta con varias opciones. Una de ellas sería la utilización de módems

---

[4] "*Metro Ethernet*" http://www.monografias.com/trabajos17/metro-ethernet/metro-ethernet.shtml

[5] "Las redes de Área Metropolitana basadas en Ethernet en el Ecuador" http://www.docstoc.com/docs/25917668/LAS-REDES-DE-AREA-METROPOLITANA-BASADAS-EN-ETHERNET-EN

en donde la desventaja principal seria el costo de la llamada, es decir, por minuto conectado, resulta muy caro en el caso de una llamada de larga distancia.

En el caso de optar por líneas privadas, se tendría que tender cobre o fibra óptica de un punto a otro, en donde resultaría sumamente elevado el costo si se quiere enlazar sucursales que se encuentren geográficamente distantes. Una solución a estas opciones limitantes de comunicación son las VPNs, en donde solamente se realizan llamadas locales, teniendo la posibilidad de que la información viaje a una velocidad acordad, segura y de buena calidad.

2.2.2 VPN (RED PRIVADA VIRTUAL) [6]

Una VPN es una tecnología de red que permite una extensión de la red local (LAN) sobre una red pública (Internet) (fig.2.5). La idea es que la red pública se vea desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

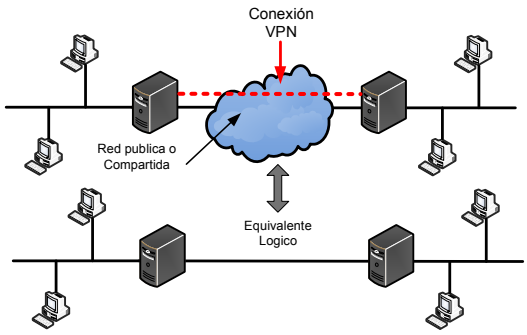

Figura 2.5 Equivalente lógico de una VPN a través de una red pública [6] .

La forma de comunicación de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de

[6] CARREON, Roberto, “Redes Privadas Virtuales”
http://www.monografias.com/trabajos11/repri/repri.shtm

encriptación y autentificación que aseguran la confidencialidad e integridad de los datos transmitidos.

La tecnología de túnel (fig. 2.6) es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original.

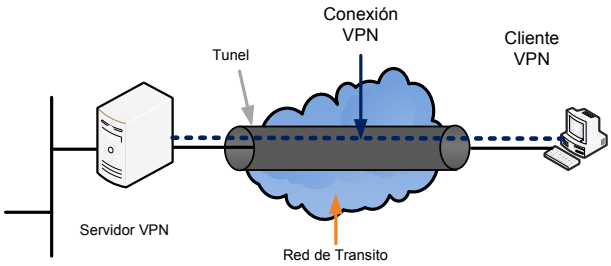

Figura 2.6 VPN (Tecnología de túnel) [6]

VPN hace posible enlazar usuarios móviles, oficinas remotas, oficinas corporativas (Partners) a través de protocolos como IP, Frame Relay, ATM, MPLS etc, utilizando como medio común una red pública, permitiendo al personal tener gestión de la sucursal, a través de una conexión, por ejemplo, desde su casa hacia el departamento de sistemas de la empresa, o mejor aun desde cualquier sitio remoto público como un hotel, un mal, todo esto utilizando la misma plataforma (Internet).

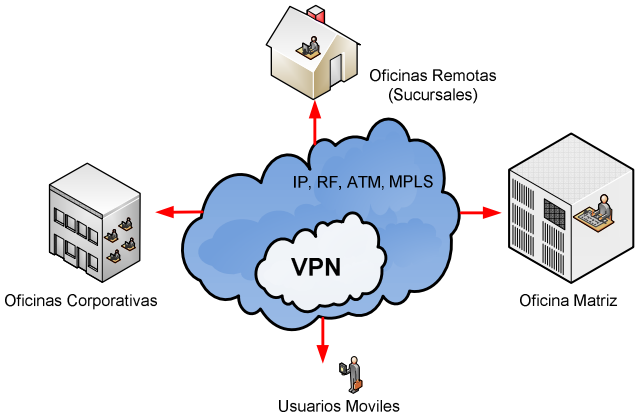

Figura 2.7 Alcance de VPN [6]

[6] CARREON, Roberto, “Redes Privadas Virtuales”
http://www.monografias.com/trabajos11/repri/repri.shtm

Las Redes Privadas Virtuales deben ser capaces de identificar la identidad de los usuarios y restringir el acceso a intrusos, proporcionando registros estadísticos de la información y un historial completo y detallado de los usuarios que ingresaron al sistema. Las VPN deben establecer direcciones del cliente en la red privada, y asegurarse de que las mismas direcciones se conserven así. Los datos que van a ser transmitidos a través de la red pública deben ser previamente encriptados para que no puedan ser interferidos por usuarios no autorizados por la red.

Las VPN deben ser capaces de generar y renovar las claves de codificación para el cliente y el servidor, manejando los protocolos comunes que se utilizan en la red pública, como el protocolo de internet (IP), el intercambio de paquete de internet (IPX) entre otros.

2.2.2.1 AUTENTICACION Y ENCRIPTACION [8] [9]

La autenticación es muy importante, ya que asegura que los usuarios de la red estén intercambiando información con el destino o dispositivo correcto.

La autenticación en VPNs es conceptualmente parecido al portal de ingreso al sistema de una empresa con nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados están basados en un sistema de claves compartidas.

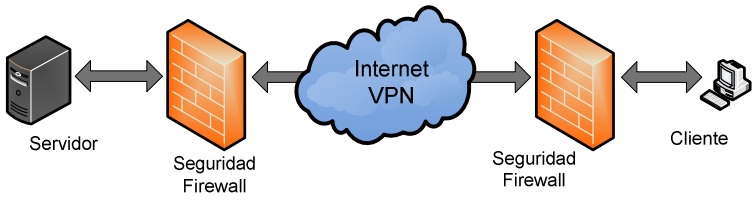

Figura 2.8 Esquema General de Seguridad de una VPN [6]

---

[6] CARREON, Roberto, “Redes Privadas Virtuales” http://www.monografias.com/trabajos11/repri/repri.shtm

[8] “Redes Privadas Virtuales” http://www.monografias.com/trabajos12/monvpn/monvpn.shtml

[9] http://es.wikipedia.org/wiki/CHAP

La autenticación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no haya interferencia de ajenos a la conversación. La autenticación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo que deriva un valor incluido en el mensaje como checksum. Cualquier alteración en el checksum indica que los datos fueron corruptos en la transmisión o interceptados y modificados en el camino. Como sistemas de autenticación tenemos:

Challenge Handshake Authentication Protocol (CHAP): Es un protocolo de autentificación remota o inalámbrica, utilizado por algunos proveedores de servicios para autentificar, por ejemplo, a un usuario frente a un ISP.

CHAP verifica periódicamente la identidad del cliente remoto usando un intercambio de información en varias etapas. Después del establecimiento del enlace, el agente autentificador manda un mensaje de verificación al usuario basado en algoritmo unidireccional. El usuario responde con un valor calculado mediante una suma de comprobación. El autentificador verifica la respuesta con el resultado de su propio cálculo. Si el valor coincide, el autentificador informa de la verificación, de lo contrario terminaría la conexión. A intervalos aleatorios el autentificador manda mensajes de comprobación de veracidad, y en cada mensaje se repite el mismo proceso.

RSA (Rivest, Shamir y Alemán): La seguridad de este algoritmo radica en el problema de la factorización de números enteros. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto por el algoritmo.

Todas las VPNs tienen algún tipo de tecnología de encriptación y lo que hacen todos es envolver los datos en un paquete seguro. La encriptación es considerada tan importante como la autenticación, ya que protege los datos transportados, para poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión. Existen dos tipos de técnicas de encriptación que se usan en las VPN: encriptación de clave secreta, o privada, y encriptación de clave pública.

En la encriptación de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad.

La encriptación de clave pública implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación. Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las VPNs, la encriptación debe ser realizada en tiempo real. Por eso, los flujos encriptados a través de una red son encriptados utilizando encriptación de clave secreta con claves que son solamente buenas para sesiones de flujo.El protocolo más usado para la encriptación dentro de las VPNs es IPSec, que consiste en un conjunto de proposals del IETF que delinean un protocolo IP seguro para IPv4 y IPv6. IPSec provee encriptación a nivel de IP.

El método de túneles, como fue descrita anteriormente, es una forma de crear una red privada. Permite encapsular paquetes dentro de paquetes para acomodar protocolos incompatibles. Dentro de los protocolos que se usan para la metodología de túneles se encuentran Point-to-Point Tunneling Protocol (PPTP), Layer-2 Fowarding Protocol (L2FP) y el modo túnel de IPSec.

Al hablar de tipos de VPN se tienen 2 básicamente:

• Intranet: Una Intranet es aquella red que interconecta sitios geográficamente separados de la misma empresa y tiene aplicaciones que permiten a los clientes internos utilizar adecuadamente la información.

• Extranet: Una Extranet es una red en la cual se han conectado al menos dos sitios de compañías distintas, y el tema de la seguridad es un factor muy importante debido a que se permite el acceso a los usuarios remotos a la información necesaria exclusivamente.
El estudio de las VPNs según las responsabilidades y el manejo de las políticas, que le competen al proveedor de servicio y al usuario, se lo puede dividir bajo dos modelos, Modelo de Sobrecapas (Overlay Model) y Modelo Par a Par (Peer to Peer Model)

2.2.2.2 MODELO SE SOBRECAPAS (OVERLAY MODEL)

También conocido con el nombre de capa superpuesta, el proveedor se encarga de proporcionar las tecnologías de transmisión como ATM, TDM, Frame relay, es decir la conectividad a nivel de capa 2, y el cliente es quien se encarga de configurar las conexiones de sus enrutadores, y controlar los dispositivos de capa 3.

Es uno de los modelos más usados por los clientes, debido a no se trata de un medio compartido, se trata de una estructura de canales dedicados. En la figura 2.9 podemos ver una apreciación de este modelo.

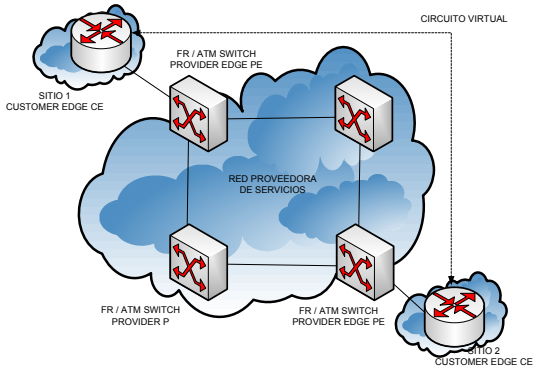

Figura 2.9 Modelo de capa superpuesta.

2.2.2.3 MODELO PAR A PAR (PEER TO PEER MODEL)

Con este modelo se trata de superar las desventajas que se presentaban en el modelo anterior, se basado en el backbone del proveedor de servicios, como una vía óptima para el transporte de información, en este caso la estructura se orienta a tener un medio compartido a nivel de capa 3 entre el usuario y el proveedor. El proveedor puede participar de forma activa en el proceso de enrutamiento, ya que el enrutador del proveedor se conecta a los enrutadores de los clientes, y entorno a esto se tiene una sola tabla de enrutamiento. En este caso el proveedor es el encargado de dar acceso, direccionar y enrutar, para así impedir que se mezclen distintas VPNs clientes.

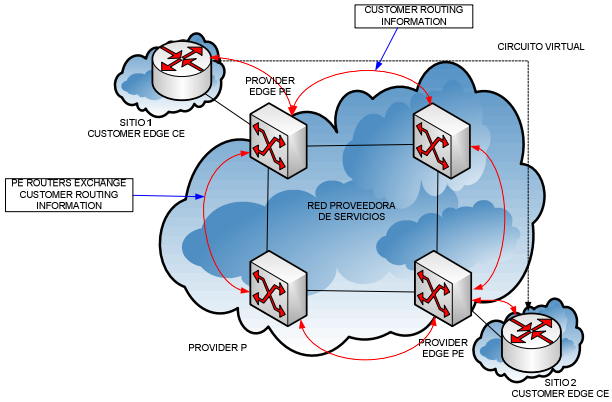

Figura 2.10 Modelo par a par.

2.2.2.4. DISTRIBUCIÓN RESTRINGIDA DE LA INFORMACIÓN DE ENRUTAMIENTO [11]

Es importante realizar la restricción del flujo de información a través de los routers de la red, ya que un cliente de una VPN, no deberá tener acceso al resto de VPNs ajenas, y la tabla de enrutamiento de un cliente no debe ser publicado al resto de VPNs que estén utilizando los servicios del mismo proveedor, todo esto con la finalidad de seguridad de la red. La distribución de información se realiza de la siguiente manera:

[11] http://dspace.epn.edu.ec/bitstream/15000/8678/5/capitulo_2.pdf

La información de enrutamiento, se la debe realizar desde el CE(cliente) hacia el PE(proveedor de servicios), usando los protocolos de enrutamiento, entre los que tenemos: RIP(*Routing Information Protocol*), OSPF (*Open Shortest Path First*), BGP o rutas estáticas. La información que ingresa al PE (proveedor de servicios), es exportada hacia el núcleo de la red(BGP), y luego esta información se envía hacia los enrutadores PE.

En el enrutador PE de egreso, se importa la información desde el proveedor de BGP. El enrutador PE se encarga de enviar la información de enrutamiento hacia el enrutador CE, todo esto usando los protocolos de enrutamiento que ya se mencionaron anteriormente.

Aparece el término *BGP community*, el cual se trata de una técnica de filtrado de rutas, y se usa para restringir información de enrutamiento, ya que se usa como un identificador que se vincula a determinada ruta, y también para diferenciar entre las VPNs.

2.2.2.5. MÚLTIPLES TABLAS DE ENRUTAMIENTO

Una de las desventajas que tiene el modelo *par a par*, es que distintos clientes pueden utilizar la mismas direcciones, MPLS/VPN propone tener una tabla de enrutamiento en el PE, para cada una de las VPNs, así los clientes únicamente tendrán acceso a las tablas de las rutas de la VPN a la que pertenecen.

Una *VRF (VPN routing fowarding table VRF)*, consiste en una combinación de una VPN tradicional y la tabla de enrutamiento VPN que se basa en etiquetas, ya que la tabla de enrutamiento en MPLS contiene toda la información necesaria para enrutar el paquete hacia el destino.

“Cada VRF en un router PE se conforma desde dos fuentes: la primera de ellas es el conjunto de rutas correspondientes al router CE de la VPN directamente conectada. La segunda fuente es el conjunto de rutas que recibe de los otros routers PE, las cuales, para

mantener correspondencia a la misma VPN, y no sean mezcladas con otras, pasan por el mecanismo de filtrado de rutas basado en la Comunidad BGP." **[11]**

2.2.2.6. DIRECCIONES VPN-IP [11]

El protocolo BGP, es usado para el enrutamiento entre PEs, y el uso en una red *par a par*, es debido a las siguientes razones; la red del proveedor, es un sistema autónomo, por lo tanto los paquetes que se envíen a otros sistemas autónomos, deberán pasar por él. Al tratarse de un sistema autónomo, este deberá tener conexión a múltiples sistemas autónomos, además tiene la capacidad de manejar múltiples familias de direcciones, por ejemplo: VPN-IP, IP, IPX.

BGP, trabaja con direcciones IP que sean únicas, en cambio las VPN pueden trabajar con plan direccionamiento iguales, para realizar un distinción es decir que las direcciones IP sean únicas, se le agrega un campo denominado *route distinguisher* (distinguidor de rutas), de esta manera se crea un nuevo tipo de direcciones IP-VPN.

Atributo de Comunidad Extendida BGP:

Cuando las rutas aprendidas (ruta objetivo) se publican nuevamente en el mismo sitio, se crean los lazos, y para evitar estos lazos se dispone de *site of origin*(sitio de origen), el cual se encarga de identificar en que sitio se originó la ruta, y así ya no recibirá la ruta desde ningún otro router PE.

2.2.2.7. MPLS COMO MECANISMO DE ENRUTAMIENTO [11]

El distinguidor de ruta se utilizaba con la finalidad de reconocer los paquetes de manera única, el enrutamiento se puede reconocer a través de este campo, que está conformado de 96 bits(*VPN+IP*), se usa MPLS para enrutar las direcciones VPN-IP, ya que se separa

[11] http://dspace.epn.edu.ec/bitstream/15000/8678/5/capitulo_2.pdf

la información de la cabecera IP, de la información de los datos del paquete, es posible que a una ruta VPN-IP se le asocie un Label Switched Path (LSP) y poderlo enrutar a través de MPLS.

Cada router PE necesita un identificador único mediante una dirección IP, el cual se propaga a través de la red de routers P usando BGP. Esta dirección IP se usa como el atributo del siguiente salto de BGP (BGP next hope attribute) para todas las VPNs publicadas en un router. PE. Una etiqueta se asigna en cada router P para cada ruta hacia un router PE y propagada hacia todos sus vecinos. Los demás routers PE reciben la etiqueta asociada con el router de egreso PE de los demás routers PE a través de un proceso de distribución de etiquetas. Luego de que la etiqueta asociada al router de egreso se recibe en el router de ingreso, se crea el LSP y el intercambio de paquetes VPN puede comenzar. Este procedimiento solo ocurre en el plano de control, pues en el plano de datos lo único que se intercambia son etiquetas asociadas a las VRFs y etiquetas para la conmutación entre los routers PE, la figura 2.11 nos muestras el transporte de datos en una red BGP/MPLS.

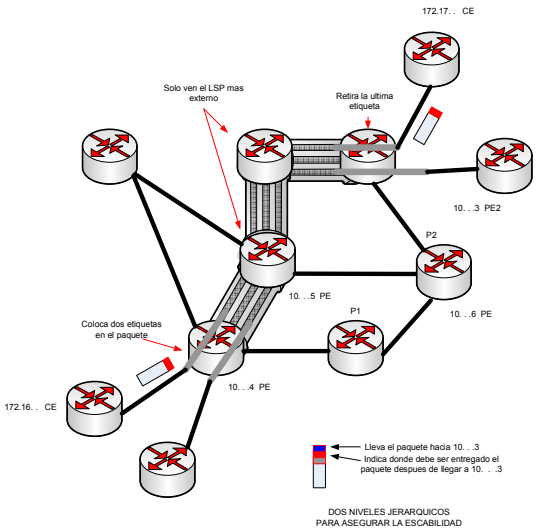

Figura 2.11 Transporte de datos en una red BGP/MPLS [11]

Cuando el router PE2 recibe una ruta con información que permite alcanzar la red 172.17/16, desde el CE2, el router PE2 convierte la información de esa ruta desde IP

tradicional a VPN-IP, coloca el atributo extendido de Comunidad BGP y exporta esta ruta hacia el proveedor BGP. En el atributo BGP del siguiente salto se coloca la dirección del router PE2. Además, a toda la información BGP adicional, la ruta también lleva una etiqueta asociada con esa ruta VPN-IP. Esta información es distribuida hacia el router PE1 usando BGP. Cuando PE1 recibe la ruta, convierte de IP-VPN a IP y lo usa para publicar la VRF asociada con la VPN.

Además, existe un LSP desde el router PE1 al router PE2, el cual está asociado con una ruta hacia el router PE2 que se puede mantener mediante LDP (Label Distribution Protocol) o Ingeniería de Tráfico MPLS. Hay que notar que la ruta distribuida a través de BGP lleva como Atributo de Siguiente Salto (Next Hope BGP Attribute) la dirección del router PE2, y la ruta hacia ese router está dada por BGP. Es entonces la dirección del router PE2 la que establece la correspondencia entre el enrutamiento interno del proveedor de servicios y las rutas de la VPN detallada (por ejemplo, la ruta hacia 172.17/16). En este punto, la VRF en el router PE1 contiene una ruta para la red 10.1.1/24 y una pila de etiquetas en donde la etiqueta más interna es la etiqueta que el router PE1 recibe vía BGP y la etiqueta externa es la asociada con la ruta hacia el router PE2.

Si se lo expone de una manera más simple, el router CE1 envía un paquete con destino 172.17.0.1 cuando el paquete arriba al router PE1, determina la apropiada VRF para esa VPN que está asociada a la interfaz de entrada (*que está directamente conectada a CE1)*. El router PE1 coloca dos etiquetas L1 y L2 envía el paquete hacia el router P1. Éste a su vez, usa la etiqueta más externa (*top label*) para tomar su decisión de enrutamiento y enviarlo hacia el router P2, el cual es el penúltimo salto antes de llegar a un LSR de borde, entonces P2 retira la etiqueta externa L1 antes de enviarla hacia el router PE2. Cuando PE2 recibe el paquete, usa la etiqueta interna L2 para realizar su decisión de enrutamiento. El router PE2 retira la etiqueta y envía el paquete hacia el router CE2.

2.2.2.8 ESCALABILIDAD

Esta característica, hace referencia a la cantidad de información que se puede intercambiar entre el proveedor y el cliente, que a pesar de que se agreguen más sitios, debe de permanecer constante, los enrutadores P, no deben ninguna información de enrutamiento IP-VPN, ya que los enrutadores PE, son los únicos que tienen esta información, y solo de los sitios que se encuentren conectados directamente a él.

Ninguno de los componentes de la red del proveedor, debe manejar la información de todas las VPN, la capacidad de enrutamiento del proveedor no está delimitada a algún componente individual de su red, esto resulta en una escalabilidad de enrutamiento ilimitada.

2.2.2.9 SEGURIDAD

Cuando se realiza el diseño de una VPN, uno de sus factores más importantes se refiere a la seguridad de la red, el proveedor de servicios realiza el enrutamiento, basado en la conmutación de etiquetas, y ya no en el enrutamiento IP, se conoce que un LSP se debe conectar a los routers PE, los cuales deberá tener en particular su tabla de enrutamiento.
La tabla de enrutamiento está asociada a través de una interfaz con el router PE, y las interfaces están asociadas con los sitios de las VPNs, de esta manera los paquetes se enviaran a sus destinos.

2.2.2.10 QoS EN UNA RED BGP/MPLS VPN

Para referirse a calidad de servicio en una VPN, tenemos: el modelo en tubo, y el modelo en manguera.

2.2.2.10.1. MODELO EN TUBO (Pipe Model)

Cuando existe conexión de un router CE de un usuario a otro, se tiene un pensamiento, que los dos sitios de la VPN están conectados mediante un tubo, por el que se enviara el tráfico, y a este se ofrecen garantías como: el mínimo ancho de banda, prioridades de tráfico, de acuerdo a la aplicación que se esté tratando.

El enrutador PE del extremo del tubo, es a que se le configura, para que tome la decisión sobre que tráfico es el que se va a enrutar, puede ofrecer un servicio asimétrico con garantías pero solamente unidireccional.

2.2.2.10.2. MODELO EN MANGUERA (Hose Model)

Este modelo principalmente maneja dos parámetros, la velocidad convenida de ingreso ICR, y la velocidad convenida de egreso ECR. A la cantidad de tráfico que un enrutador CE puede enviar a otros enrutadores CE, se le conoce como ICR. Y la cantidad de tráfico que un que un CE puede recibir de otros enrutadores CEs, se le conoce como ECR, de esta manera un ICR y un ECR no necesariamente serán iguales. A manera de ejemplo un ICR puede tener la capacidad de manejar 20Mbps y un ECR 12Mbps.

Este modelo puede soportar diferentes clases de servicio, similar a Diff-Serv, en una red es posible implementar los dos modelos vistos, el Router PE se encarga de designar que tipo de trafico recibe QoS, en base al análisis de requerimientos, de la interfaz, de las dirección IP origen y destino, etc. Existe la posibilidad de que un cliente pueda contratar un límite de tráfico que pueda recibir QoS, al sobrepasar este límite, el tráfico puede ser descartado la parte que excede, o por otra parte se puede seguir enviar con un inferior QoS.

2.3. DESCRIPCION FUNCIONAL DE MPLS (MULTIPROTOCOL LABEL SWITCHING)

2.3.1. DEFINICIÓN DE MPLS

MPLS (Multiprotocol Label Switching), es un método para transportar datos, tanto en redes basadas en circuitos como en paquetes, su la finalidad es brindar soluciones de conmutación multinivel, tiene la capacidad de transportar diferentes tipos de tráfico, tráfico de voz, paquetes IP, etc. Y priorizar cada uno de estos.

En definitiva MPLS pretende obtener todas las ventajas de ATM pero evitando sus inconvenientes, para realizar una conmutación más rápida, a cada datagrama asigna una etiqueta única, la cual es interpretada por el router, el cual solamente interpreta la etiqueta y no toma en cuenta su dirección de destino.

En la figura 2.12 de muestra el funcionamiento básico del funcionamiento de MPLS.

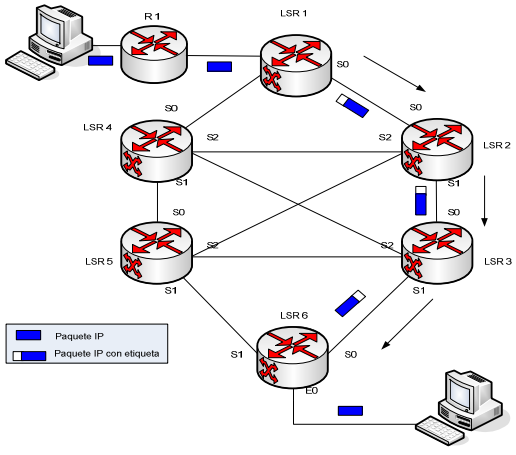

Figura 2.12 funcionamiento básico MPLS

Los pasos para que la información a ser transmitida llegue a su destino son los siguientes:

Para que la información pueda ser enviada, primero se debe de establecer un camino, entre los routers, aquí se definirán parámetros específicos como por ejemplo el QoS, al ingresar un paquete a la red MPLS, mediante un LSR(Label Switching Router), que será quien defina los requerimientos tales como QoS, etc. Luego de esto el paquete el asignado a una FEC y un LSP, para que sea etiquetado y enviado.

Estando el paquete dentro del dominio de MPLS, se realiza la conmutación de etiquetas, y antes de llegar a su destino final, la etiquetas es retirada.

2.3.2. Elementos de una red MPLS.

Dentro de MPLS tenemos los siguientes elementos: **FEC, LSR, LER, LSP, LDP, LIB.**

2.3.2.1. FEC (Forwarding Equivalence Class)

Conjunto de paquetes que comparten una misma etiqueta, de esta manera todos reciben el mismo tratamiento en el conmutador, un paquete se asigna a un determinado FEC, una vez que el paquete ingresa a la red, los requerimientos de servicio ya sea para varios paquetes o una dirección fija son determinados por un FEC.

2.3.2.2. LSR (Label Switched Router)

Es un router, que se encarga de conmutar etiquetas a gran velocidad, principalmente participa en los establecimientos de los LSP empleando los protocolos de señalización de una manera correcta.

2.3.2.3. LER (Label Edge Router)

Es un router que se encuentra en los extremos de la red, o elemento de entrada y salida, y hace posible la conexión entre diversas redes tales como ATM, Frame Relay, Ethernet,

etc,. Cuando el trafico es entrante a la red MPLS utiliza un protocolo de señalización de etiquetas, y distribuye el trafico saliente entres las diferentes redes.

2.3.2.4. LSP (Label Switched Path)

A un paquete dentro de la red, se le realiza un análisis y a través de este, se asocia un LSP, es decir un camino MPLS que se establece entre los extremos, y es unidireccional.

2.3.2.5. LDP (Label Distribution Protocol)

Es un protocolo que se encarga de distribuir etiquetas MPLS a los equipos que se encuentren conectados a la red.

2.3.2.6. LIB (Label Information Base)

Aquí se encuentra la información sobre las etiquetas.

2.3.3. ARQUITECTURA MPLS

Para que la asignación de las etiquetas sea de manera única, MPLS está formado por el plano de control y el plano de datos.

2.3.3.1. PLANO DE CONTROL.

Para realizar la conmutación y la clasificación de paquetes, es necesario que se realice el intercambio de las tablas de enrutamiento, acción que se la realiza en el plano de control, a través de sus distintos mecanismos, y protocolos como son: OSPF, BGP, EIGRP, IS÷IS, y para realizar el intercambio de etiquetas se tiene los protocolos como TDP y el LDP.

2.3.3.2. PLANO DE DATOS.

En este plano se envían los paquetes basados en etiquetas, la forma de envío se hace mucho más simple, ya que aquí se encuentra la LIB, y con esta, la información para enviar dichas etiquetas, los datos de la LIB son proporcionados mediante los protocolos TDP y LDP, protocolos para intercambiar etiquetas.

Las funciones que cada equipo desempeña dentro de la red, se explicó anteriormente en elementos de la red.

2.3.4. CABECERA Y CAMPOS MPLS

Las etiquetas nos indican la ruta que un paquete tiene que atravesar, así el paquete etiquetado viajara a través de la red y será analizado al pasar por cada Router, el cual consultara con sus tablas, para decidir con que etiqueta e interfaz deberá ir. Para realizar la asignación de etiquetas, se puede basa en criterios de envió, ya sea que se trate de VPN, ingeniería de tráfico y QoS.

Figura 2.13 etiquetas MPLS [13]

Cada campo contiene la siguiente información:

Label; tiene un tamaño de 20 bits, y se utiliza para identificar el LSP, es el valor de la etiqueta.

Exp: de tamaño de3 bits, se utiliza para experimentos, se utiliza para permitir servicios diferenciados.

13 http://dspace.ups.edu.ec/bitstream/123456789/209/3/Capitulo%202.pdf

S: de tamaño de 1 bit, proviene del inglés stack y nos indica el final de pila de las cabeceras, al tener el valor de S=1, nos indica que la cabecera es la última de la pila.

TTL: de tamaño de 8bits, nos indica el número de saltos máximo que puede realizar un paquete a través de la red, al superar este límite el paquete es descartado.

2.3.5. PILA DE ETIQUETAS.

Cada pila de etiquetas es representados por cuatro campos, como se muestra en la figura 2.2, dentro de la cabecera que MPLS agrega al paquete, puede existir una o varias etiquetas, y al conjunto de etiquetas se le llama pila, con un funcionamiento LIFO(Last In, First Out).

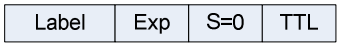

Figura 2.14 Pila de etiquetas

Cada entrada a la pila de etiquetas se encuentra dividida en los campos: Label, Exp, S y TTL, que se definieron anteriormente. Se facilita la creación de túneles MPLS, ya que cada pila de etiquetas corresponde a un nivel jerárquico.

Dentro de un dominio MPLS, pueden existir otros dominios, las cabeceras se crean de acuerdo al número de dominios existentes, la pila de etiquetas está conformada por todas estas cabeceras. La ilustración de esto se muestra en la figura

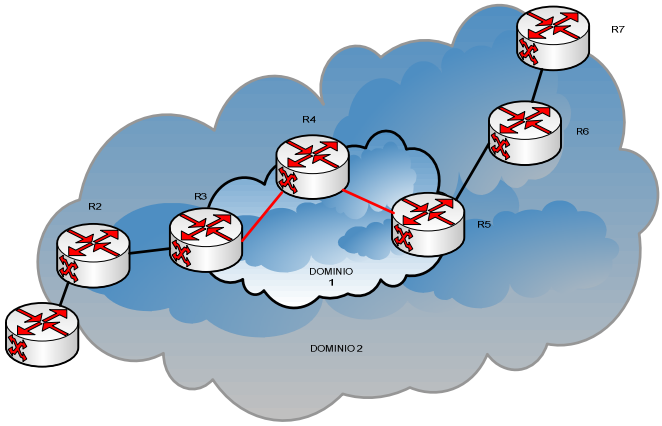

Figura 2.15 Dominio MPLS dentro de otro dominio MPLS

2.3.6. DOMINIO MPLS

Es el conjunto de routers con funcionalidad MPLS, para que un paquete viaje con un determinado FEC, es necesario que se establezca LSP, para esto existen dos mecanismos:

2.3.6.1 ENCAMINAMIENTO SALTO A SALTO

La selección de los saltos para un FEC, los realiza un LSR, el cual selecciona el siguiente salto de manera independiente a los otros LSRs, este método usado es similar al que se utiliza en las redes IP, entre los protocolos más utilizados para el routing se utiliza el OSPF (Open Shortest Path First), el cual es uno de los más sencillos, no posee todas las ventajas de MPLS, como la ingeniería de tráfico, ni policitas de ruteo para poder manejar QoS.

2.3.6.2. ENCAMINAMIENTO EXPLÍCITO

En el encaminamiento explicito el LER establece las secuencia de saltos o LSRs por los que un LSP deberá pasar dentro de un determinado FEC. Se cumple el ruteo explicito

completamente cuando el LER define todos los LSR, y si no es así se trata de un ruteo explicito parcial, con estas técnicas de ruteo es posible utilizar todas las ventajas que presenta MPLS, tales como ingeniería de tráfico y QoS.

En el caso del encaminamiento explicito, las rutas se pueden especificar de manera previa o de manera dinámica, al definir de manera dinámica se tiene beneficios en cuanto al alcance de las técnicas de ingeniería de tráfico, todo esto es posible si el LER contiene la información de la topología de la red y los requisitos de calidad de servicio del dominio.

Al establecerse un LSP, para un determinado FEC, este es de manera unidireccional, y el tráfico de vuelta debe establecer otro LSP, en el momento que se detecte un cambio o un fallo en la red, se debe crear un nuevo LSP para reencaminar el tráfico. Si se trata de rutas explicitas estrictas el único que puede reencaminar el tráfico es el LER, una vez que ha informado de un error, y así este generara una ruta alternativa.

En el caso de que se detecte un fallo en una ruta explicita tolerante, cualquiera de los LSP, puede escoger caminos alternativos, una vez que haya detectado un fallo vecino.

2.3.7. DISTRIBUCIÓN DE ETIQUETAS

Para lograr que se realice la configuración de un camino o trayectoria MPLS, es necesario que los LSR realicen varias operaciones como:

Se asigna una etiqueta al LSP, a través de la cual será posible identificar los paquetes que pertenecen a determinado FEC.

Luego se dará a conocer a los elementos de la red, que mandan información, que el LSR ha asignado una nueva etiqueta, al FEC en tratamiento, el propósito de

esto es que los nodos etiqueten de manera correcta los paquetes dirigidos al LSR que los contacto.

Se debe tener conocimiento del siguiente salto del LSP, para esto el Next Hop LSR le asigna una etiqueta, y a través de este proceso es posible mapear una etiqueta de entrada a una de salida.

De los operaciones mencionadas anteriormente, la primera se realiza de manera local, mientras que las otras dos se realizan usando un protocolo de distribución de etiqueta de de forma manual.

Los protocolos de distribución de etiquetas permiten a los LSR informar al resto de LRS de las operaciones que se ha realizado a las etiquetas del FEC, de esta manera se tiene conocimiento de las capacidades MPLS de cada LSR a los demás LSR.

2.3.8. ENRUTADOR DE ETIQUETAS CONMUTADAS LSR

El Label Switched Router, posee generalmente las mismas funciones que un router, pero al ser configurado como LSR, el equipo tomara un tratamiento a los paquetes, ya que para su envió no se basara en tablas de enrutamiento IP, sino en la conmutación de etiquetas, LSR cumple las siguientes funciones con el manejo de etiquetas.

Agregación (*Aggregate*): en esta parte la etiqueta es retirada y buscada en la tabla de enrutamiento en base a información IP.

Remoción (*Pop*): aquí se retira la primera etiqueta de la pila, y se continúa transmitiendo el paquete que resta, basándose en etiquetas o direcciones IP.

Adición (*Push*): la etiqueta es reemplazada por un arreglo de etiquetas.

Conmutación (*Swap*): una etiqueta es reemplazada por otra.

Eliminación (*Untag*): el paquete es enviado al siguiente salto IP, luego que se haya quitado la etiqueta.

2.3.8.1. LSR en una red de paquetes

Para entender el funcionamiento básico de un LSR, se muestra la figura 2.16:
En la que el procedimiento del envió del paquete es el siguiente; en esta figura tenemos un LSR1, el cual se encuentre en el borde, este identifica el prefijo. Luego de aplicar los protocolos de enrutamiento, asigna la etiqueta inicial, y envía el paquete al LSR2.

LSR2 al recibir el paquete, reconoce la información de la etiqueta, la conmuta por una nueva, y el paquete es enviado nuevamente, en este caso a LSR5, de acuerdo a la información de la etiqueta de entrada. LSR5 al recibir el paquete, reconoce la información de la etiqueta, remueve la etiqueta, y busca en la tabla de enrutamiento, para determinar el próximo salto, y al saber cuál es este, el paquete es enviado.

Una vez que el LSR2 recibe el paquete, examina la información de la etiqueta, la conmuta por una nueva y envía el paquete al LSR4 basado en la información que traía la etiqueta al ingresar. Al llegar el paquete al LSR4, éste examina la información de la etiqueta, remueve la etiqueta, realiza una búsqueda en la tabla de enrutamiento para determinar cuál será el siguiente salto en la red y una vez lo determina, envía el paquete.
Este es el procedimiento básico y se repite para cada paquete de la red, dependiendo del tamaño de la red, se puede obtener un gran número de prefijos que formen la LFIB.

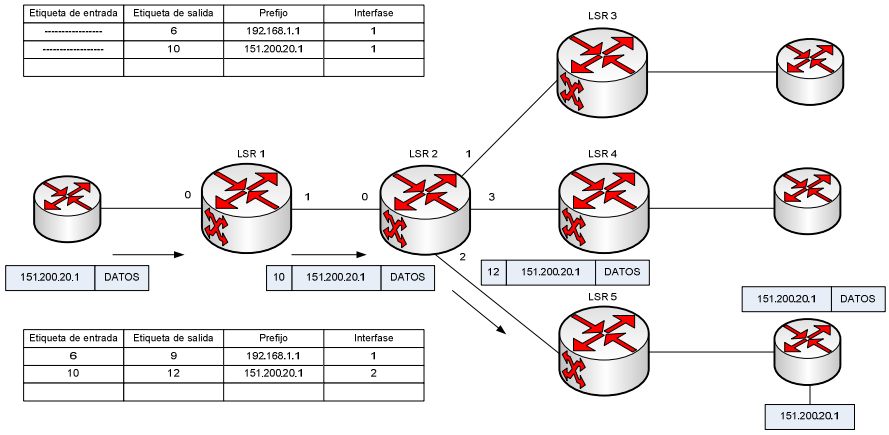

Figura 2.16 LSR en modo paquetes.

2.3.8.2. LSR EN MODO DE PAQUETES CON MULTIETIQUETA.

En ciertas aplicaciones que utilizan VPNs, o ingeniería de tráfico, es necesario que las etiquetas usen identificadores adicionales, para la trayectoria de la etiqueta conmutada, por esta razón existen paquetes que manejan más de una etiqueta, en la figura 2.16 se ilustra en modo multietiqueta, se observa que la etiqueta adicional no se conmuta durante la trayectoria, el valor de esta sirve para identificar una trayectoria para él envió de paquetes con determinadas características, como puede ser ingeniería de tráfico.

En este caso LSR1 identifica el prefijo, le asigna la etiqueta y envía el paquete, el paquete es recibido en LSR2, donde la etiqueta es conmutada, y se envía el paquete basado en la información de la etiqueta, en este caso a LSR5, donde se quita la etiqueta y se envía el paquete al salto siguiente, basándose en el direccionamiento IP.

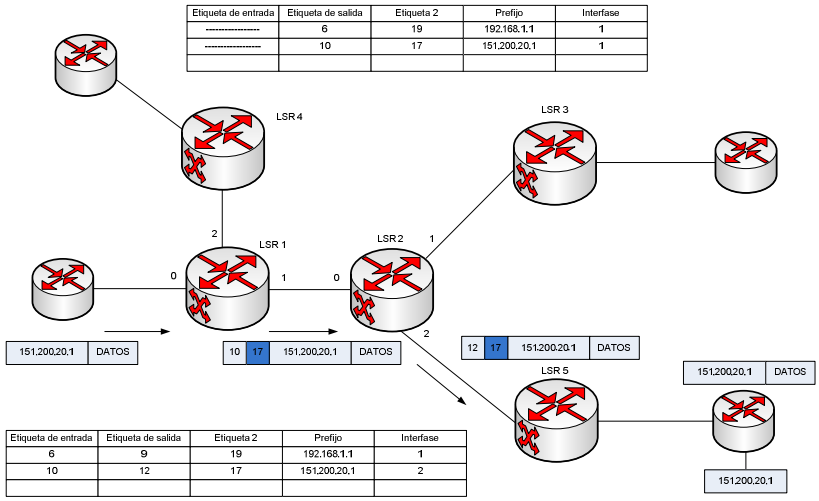

Figura 2.17 LSR modo multietiqueta

Los esquemas de envío de paquetes mostrados anteriormente no son los mejores, por lo que se busca optimizarlos, puesto que los LSR que se encuentra en los extremos o fronteras deben realizar doble función, en primer lugar deben de remover la etiqueta, y buscar en su tabla de enrutamiento el siguiente destino del paquete para enviarlo, la solución será que el LSR que se encuentre antes del LSR de borde sea quien se encargue de remover la etiqueta, para esto a través del LDP se debe enviar una etiqueta nula implícita, que tendrá su valor respectivo de acuerdo a la tabla de valores reservados de etiquetas.

2.3.8.3. Valores reservados de etiquetas en MPLS.

Valor de la Etiqueta	Descripción
0	IPv4 etiqueta nula explicita. Indica que la etiqueta debe ser removida y el paquete debe ser enviado en base a la información de IPv4
1	Alerta de etiqueta de Router
2	IPv6 etiqueta nula explicita. Indica que la etiqueta debe ser removida y el paquete debe ser enviado en base a la información de IPv6

3	Etiqueta nula implícita. Se utiliza para remoción de etiquetas POP
4 a 15	reservado para uso futuro

Tabla 2.1 Valores reservados de etiquetas en MPLS [12]

2.3.8.4. REMOCIÓN DE ETIQUETA (*pop*)

Para optimizar el envío de paquetes, se realiza la función de remoción de etiquetas en el LSR que se encuentra antes del LSR frontera. El procedimiento se ilustra en la figura 2.17

En este caso el LSR1 identifica el prefijo, y asigna la etiqueta, luego de esto el paquete es enviado, en este caso a LSR2, en donde la etiqueta es removida y se envía el paquete aLSR4, LSR4 envía el paquete al salto siguiente basándose en el direccionamiento IP.

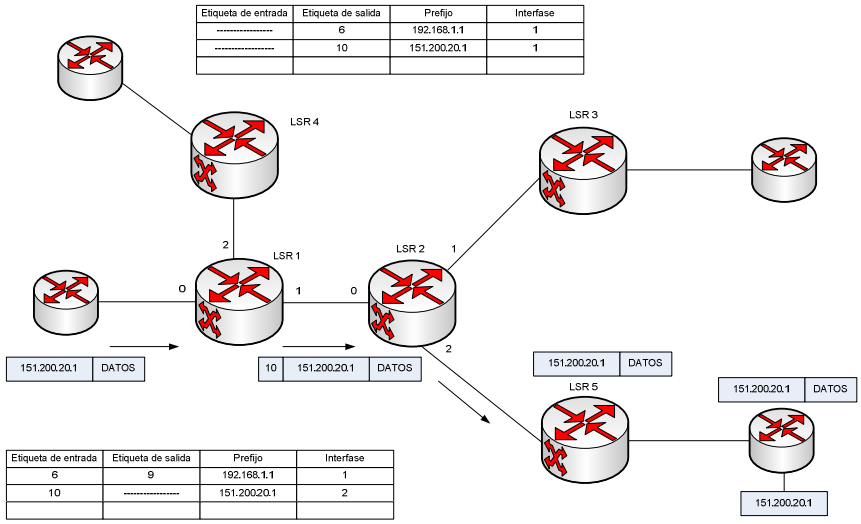

Figura 2.18 Remoción de etiquetas POP

[12] http://es.wikipedia.org/wiki/Multiprotocol_Label_Switching

2.3.8.5. LSR EN UNA RED DE CELDAS ATM

El funcionamiento de MPLS en ATM es un caso particular, para que los conmutadores ATM se transformen en un LSR, se les debe adicionar un LSC (Label Switch Controlled) o control de conmutación de etiquetas, las etiquetas en los LSR de ATM, son representadas a través de un VPI/VCI, que es creado por la red ATM de una manera dinámica, VPI/VCI emulan la trayectoria de la etiquetas conmutadas del modelo de paquetes.

La matriz ATM de conmutación se transforma en el equivalente de la LFIB, en los extremos normalmente se tiene un LSR ATM que está conectado a un LSR de la red de paquetes, en esta parte el LDP se encarga de realizar correspondencias de etiquetas a los VPI/VCI, completando de esta manera las trayectorias virtuales dentro de la red.

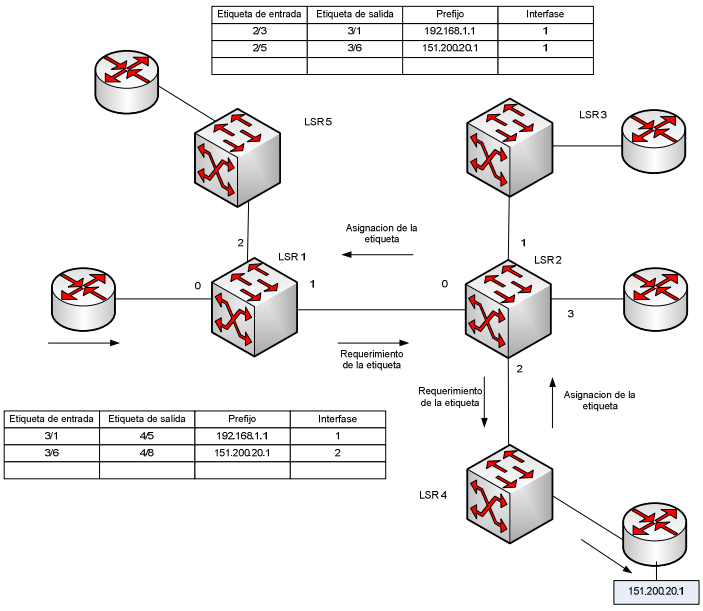

Figura 2.19 LSR en una red de celdas ATM

La asignación de etiquetas en las celdas, se las realiza bajo demanda, es decir los PVC en ATM o trayectoria de etiquetas, se establecerán solo cuando los LSR lo soliciten.

En la figura 2.6 podemos observar que LSR1 requiere de una etiqueta al LSR2, de la misma manera que el LSR2 se la requiere al LSR4; LSR4 en este caso asigna la etiqueta y se la envía al LSR2, LSR2 al recibir la etiqueta que le envió el LSR4, la conecta a una etiqueta local, luego de esto el valor de esta etiqueta local es enviado al LSR1, la etiqueta es usada por LSR1 para de esta forma completar la trayectoria.

El inconveniente del modelo de las celdas es que el número de VPI/VCI es limitado, los prefijos IP en la red pueden crecer tanto que sobrepasen los límites de PVC (VPI/VCI) que un equipo ATM puede soportar, para superar esta limitante se puede usar técnicas de optimización en el uso de PVC, pero la mejor recomendación es migrar de redes basadas en celdas a redes basadas en paquetes.

2.3.9. TRAYECTORIA DE ETIQUETAS CONMUTADAS LSP

Las trayectorias de la etiquetas conmutadas, se trata de un camino ya establecido a través del cual se va a enviar los paquetes en la red MPLS, como se mencionó anteriormente los LSP son unidireccionales, es decir que la trayectoria de envío no necesariamente será la misma de regreso, de acuerdo a esto los LSP, se pueden establecer ya sea por: control independiente, o control ordenado.

2.3.9.1. CONTROL INDEPENDIENTE

Al tratarse de control independiente, los LSR identifican los diferentes prefijos como FECs, luego a cada uno de los FECs se le asigna una etiqueta, que conjuntamente con la tabla de correspondencias, se envían a todos los LSR de la red a través del protocolo LDP.

Los LFIB son creados por los LSR de acuerdo a la correspondencia entre los FEC y los saltos siguientes, para determinar los saltos siguientes los LSR usan el protocolo de enrutamiento por lo general el OSPF, En la figura 2.19 se puede apreciar una red de LSR, y luego en la tabla 2, se muestra la LFIB que se genera luego que las etiquetas han sido propagadas a mediante el protocolo LDP.

En la LFIB se indica el salto siguiente para cada LSR, hasta llegar al prefijo 10.12.20.0/24, una de las mayores importancias es, que establece la LFIB, rápidamente luego que converge el protocolo de enrutamiento.

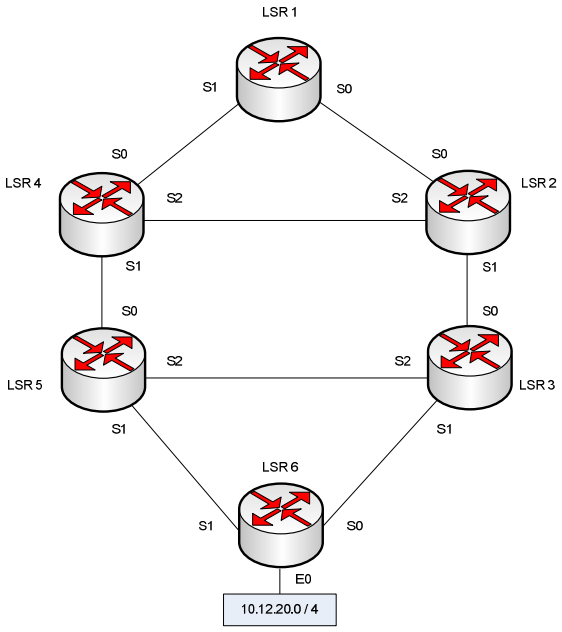

FIGURA 2.20 LSP control independiente.

LSR	Etiqueta entrante	Etiqueta saliente	siguiente salto	Interface saliente
LSR1	22	37	LSR2	S0
LSR2	37	42	LSR3	S1
LSR3	42	72	LSR6	S1
LSR4	72	66	LSR5	S1
LSR5	66	51	LSR6	S1
LSR6	51	---	LSR6	E0

TABLA 2.2 LFIB después de la distribución de etiquetas [12]

2.3.9.2. Control ordenado

En este tipo de control, los requerimientos de las etiquetas lo realiza un router de borde, la asignación de etiquetas sigue un orden de extremo a extremo. La selección de los FECs la realiza el LSR iniciador, y el resto de LSRs de la red utilizaran el mismo FEC.

La exigencia principal del control ordenado es la propagación de todas las etiquetas antes que se establezca el LSP, por esta razón la convergencia es lenta ante cualesquier variación que se presente en la red. A pesar de esto se previene la aparición de bucles mientras se genera las etiquetas. En la figura 2.21 podemos apreciar la generación de etiquetas desde el un extremo hasta el otro en una red.

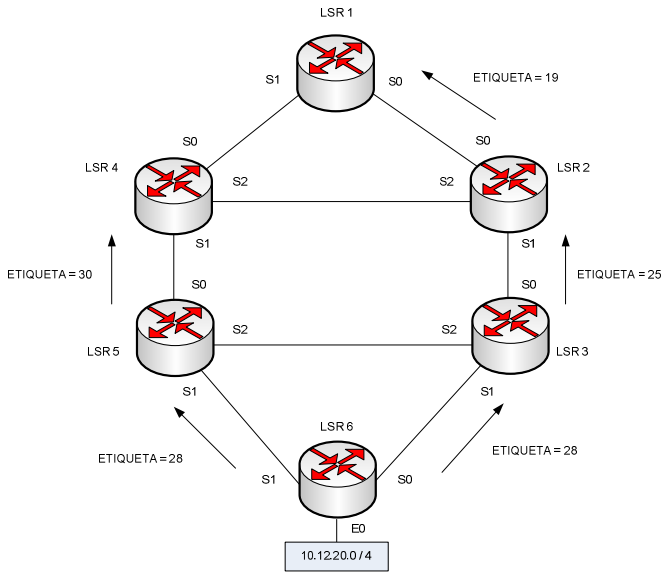

Figura 2.21 LSP control ordenado

2.3.10. PROTOCOLOS DE DISTRIBUCIÓN DE ETIQUETAS

2.3.10.1. Protocolo LDP

El Label Distribution Protocol (LDP) es el encargado en distribuir etiquetas a través de todos los LSR de la red, a través de puerto TCP 646 distribuye las etiquetas a los LSRs vecinos. A través de este protocolo es posible cualquier tipo de negociación, en la que

los LSRs que estén dispuestos a participar necesitan entablar para tener conocimientos sobre cuáles son las capacidades MPLS de cada uno de ellos.

Para la asignación y distribución de etiquetas, LDP cuenta con los siguientes modos: por demanda, por asignación no solicitada, retención de etiqueta liberal y retención de etiqueta conservador.

Modo LDP por demanda: las etiquetas son asignadas en base a requerimientos específicos para los FECs.

Modo LDP por asignación no solicitada: la asignación y distribución de la etiquetas, a los LSRs, se la realiza aunque estos no la hayan solicitado.

Modo de retención de etiqueta liberal: en este modo se puede borrar o se puede mantener las etiquetas recibidas de un LSR vecino, aunque este no sea salto siguiente para llegar al prefijo.

Modo de retención de etiqueta conservador: en este modo las etiquetas pueden ser descartadas si se ha recibido de un LSR vecino que no sea el siguiente salto para alcanzar al prefijo, así solo quedaran las etiquetas que identifican a los FEC para enviar los paquetes directamente.

2.3.10.1.1. Categorías de mensajes LDP

Para que la asignación y distribución de etiquetas entre los LSR, y sus interfaces se encuentren activas para MPLS, el LDP debe realizar acciones a través de los siguientes mensajes: Discovery Message, session messages, advertisement messages, notification Message.

Discovery Message: Anuncio y mantenimiento de la presencia de un LER/LSR en la red.

Session Message: se encarga de establecer, mantener y liberar las sesiones entre los LSR.

Advertisement Message: comunica los vínculos de las etiquetas al FEC y actualización de estos vínculos.

Notification Message: Informa de algún error producido.

Dentro de estas categorías, en cada una de estas se encuentran nuevos mensajes como se muestra en la siguiente tabla:

Categoría	**Mensaje**
notification	Notification
discovery	Hello
Session	Initialization, Keep alive, address, address withdraw
advertisement	label mapping, label request, label withdraw, label release, label abort request

Tabla 2.3. Mensajes LDP

Un ejemplo de la aplicación de estos mensajes lo podemos ver en la figura 2.22.

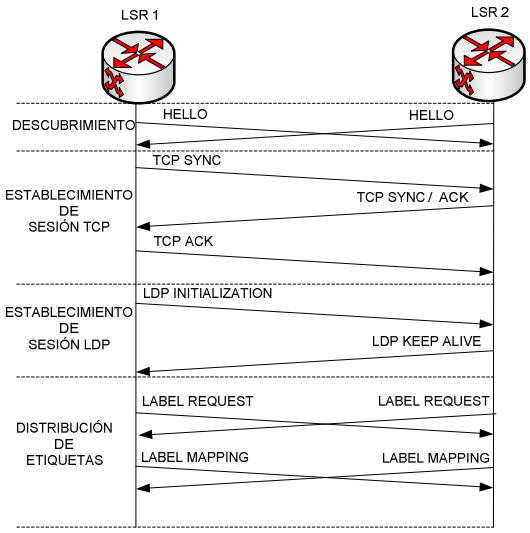

FIGURA 2.22 Establecimientos de sesión LDP

Los mensajes se encargan de lo siguiente:

Durante el *Discovery*, se envía mensajes *hello* a todos los LSR, para indicar la presencia de un LSR que esta emitiendo.

En los mensajes de *session*, tenemos el *initialization* que se encarga de iniciar la sesion LDP, y el que mantiene activa dicha sesion en este caso *Keep alive.*

En los mensajes de *advertisement*, para enviar las etiquetas a los determinados FEC, se usa *Label mapping*, y para la solicitud de una etiqueta para un FEC el *Label request*.

Los mensajes *notification*, para indicar que ha existido errores, o recomendar a cerca del estado de la sesión.

LDP utiliza los siguientes métodos para la distribución de etiquetas:

"**Downstream on demand:** Este modo de distribución de etiquetas permite que un LSR pida explícitamente de su router downstream la etiqueta correspondiente para un prefijo destino particular, conocido como distribución de etiquetas *downstream on demand."*[12]

"**Unsolicited downstream:** mediante este modo de distribución se permite que un LSR distribuya etiquetas a los LSRs upstream que no lo han pedido explícitamente." [12]

2.3.10.2. CR-LDP (Constraint-based Routed Label Distribution Protocol)

CR-LDP o Protocolo de distribución de etiquetas basadas en restricciones, es un enrutamiento explicito, una de sus propiedades es realizar el análisis del estado de los enlaces, mientras se realiza el establecimiento de los PVCs.

12 http://es.wikipedia.org/wiki/Multiprotocol_Label_Switching

Utiliza la capa transporte TCP, con la finalidad de la negociación de los recursos necesarios para el envío de tráfico entre los LSRs, para el establecimiento de session se basa en los siguientes mensajes: label request, label mapping, label notificación, label error y label release.

Label Request: es el encargado de hacer la petición para que se pueda establecer un nuevo ER-LSP.

Label Mapping: una vez que un mensaje de estos llega a los nodos, cada uno se encarga de establecer los ER-LSP, ajustando las tablas de conmutación.

Label Notification: si durante el intercambio de mensajes se ha producido algún evento, este se encarga de informar.

Label Error: si durante el intercambio de mensajes CR-LDP, se ha producido un error, este se encarga de informar.

Label Release: este nos indica que un LSP ya establecido, ha sido liberado.

CR-LDP tiene la posibilidad de reservar recursos para las rutas explicitas, con características como: routing explicito, prioridad, velocidad de pico de datos, máximo tamaño del mensaje, velocidad de datos garantizada, de esta manera garantiza la calidad de servicio.

2.3.10.3. RSVP-TE (Resource Reservation Protocol - Traffic Engineering)

RSVP-TE, se trata de un protocolo de encaminamiento que se encarga de reservar recursos mediante una red de servicios integrados, ya sea canales o rutas en la red, para trasmitir con escalabilidad y robustez, para el uso en MPLS consta de nuevas capacidades necesarias para el establecimiento de rutas LSP, usando el modelo *por demanda*, explicado anteriormente.

Se trata de un encaminamiento explicito, pero la asignación de etiquetas se realiza en sentido contrario al flujo de datos, es decir desde el destino hacia el origen, por lo que se añade un Label como información adicional. Para establecer los túneles LSP se sigue el siguiente procedimiento:

Si un LER en entrada desea establecerse con un LER de salida, se iniciara a través de un mensaje tramo, la ruta a seguir por el LSP será determinada por un gestor de la red, esta ruta es diferente de la que se calcula mediante algoritmos.

El mensaje de tramo es enviado a los LSR intermedios, los que procesaran de acuerdo a lo especificado en el protocolo, y al darse cuenta que no son los extremos, enviaran el mensaje al nodo siguiente en la ruta.

Al llegar los mensajes a su LSR destino, se reserva los recursos internos, y se escoge las etiquetas necesarias para establecer el túnel LSP, a través de un mensaje de reserva (resv.) se propaga hacia el LSR anterior.

Los LSRs intermedios pueden realizar la reserva de recursos y etiquetas para el flujo, si estos han recibido la capacidad de asignar etiquetas con el mensaje resv., este es un procedimiento que se repite constantemente hasta que se alcanza al LSR origen, donde también se realiza la reserva de recursos, la asignación y propagación de la etiqueta no es necesario, puesto que se ha encontrado el origen del FEC.

RSVP no toma decisiones individuales de cada datagrama, maneja flujos de datos, esto se refiere a sesiones entre maquinas con origen y destino especifico.

Una sesión consta de: dirección destino, ID del protocolo y puerto destino, ya que una sesión es conocida como el flujo de datagramas hacia el destino y etiqueta de protocolos particular, y es posible soporta sesiones, simplex, unicast y multicast.

2.3.11. DIFFSERV (Modelo de servicios diferenciados)

Este modelo clasifica el tráfico, en clases, una de estas con sus respectivas políticas de cola y de reenvío independientes, reemplaza a un modelo anterior *IntServ* (servicios integrados), ya que este daba un tratamiento a tráfico basado en el flujo, por lo que no es posible usar políticas de clases de servicio (Cos).

Un LSP puede llevar uno o varios FEC, y también puede asignar, varios flujos de información para cada FEC, este protocolo es tan correcto que se pude determinar que cable físico llevara el tráfico dentro del dominio del LSP. Los canales se los puede asignar a nivel de FEC o de un grupo de FEC, a esto se puede incluir numerosos flujos de información diferentes, con la finalidad de disminuir la carga en los enrutadores.
A través de diferente mecanismos es posible seleccionar el tráfico en un número pequeño de clases de servicio, con distintas prioridades, ya sea como páginas web, correo electrónico, etc. y para otras aplicaciones donde no es permitido el retardo como la voz y video, se emplea ToS (Type of service), y esta se encarga de marcar los paquetes con QoS que se envían a la red.

Como la etiqueta de MPLS contiene un campo denominado “EXP”, es posible propagar CoS en el LSP correspondiente, razón por la que MPLS puede propagar diferentes clases de tráfico, puesto que:

Al tráfico que fluye por un LSP, se puede establecer a diferentes colas de salida para distintos saltos LSR, la información del campo EXP, define estos parámetros.
Es posible provisionar de múltiples LSPs, entre un par de LSR exteriores, y cada uno de estos puede tener diferentes prestaciones, pudiendo garantizar distintos anchos de banda, y distintos niveles de servicio, así desde un servicio de prioridad best effort hasta un servicio de alta prioridad.

2.3.12. PREVENCIÓN Y DETECCIÓN DE BUCLES.

Con la finalidad de mitigar la creación de los bucles en la red MPLS, se utiliza el campo TTL, el cual nos indica el tiempo de vida o número máximo de saltos que un paquete puede realizar en la red, al llegar al número máximo el paquete es descartado.

En otras tecnologías como ATM o Frame Relay, para disminuir los efectos de bucle, se realiza con la limitación de espacio en buffers, para un único Virtual Channel, ya que no es posible la utilización de TTL.

Se busca un mecanismo que impida que los paquetes queden circulando en la red por un tiempo indefinido, se tiene dos tipos de de detección y prevención: en modo paquetes, y modo celdas.

Una manera diferente para detectar los bucles es a través de la técnica llamada path vector (vector de rutas), este vector contiene la lista de los Label Switched Router (LSR) que atraviesa el Label Switched Path (LSP), LSR al enviar un mensaje de control del Label Distribution Protocol (LDP), le añade un identificador al vector que va en el mensaje, se detectara si existe el bucle en el momento, que un LSR recibe un mensaje en que el vector de caminos se encuentre su propio identificador, los bucles se producen en caminos salto a salto.

DETECCIÓN Y PREVENCIÓN EN MODO DE PAQUETES: como se menciono anteriormente una forma de estas se basa en el campo TTL del paquete, ya que los paquetes se descartan cuando el contador del campo TTL llega al máximo número de saltos permitidos para el paquete. Otra forma dentro de este mismo modo consiste en que el plano de control asigna a los protocolos de capa 3 que sean quien se encargue de detectar y prevenir los bucles.

DETECCIÓN Y PREVENCIÓN EN MODO DE CELDAS: se basa en el funcionamiento del campo TTL, pero en este caso en el plano de envío se tiene un

parámetro denominado TLV, que tiene un valor máximo, al pasar por cada salto el valor de este es incrementado, y al llegar al límite o número máximo de saltos el paquete es descartado.

2.3.13. APLICACIONES DE MPLS

Entre las aplicaciones que tiene MPLS, podemos encontrar: ingeniería de tráfico, Clase de servicio, VPNs:

2.3.13.1. INGENIERÍA DE TRÁFICO:

Se debe de adaptar el tráfico existente a los recursos físicos de los que dispone la red, se busca utilizar de manera óptima estos recursos, para evitar que algunos de estos recursos se congestionen y otros estén con poco uso con respecto al tráfico, los flujos de tráfico deben buscar el camino más corto a seguir, la ingeniería de tráfico se encarga reubicar ciertos flujos mediante el algoritmo IGP (*Internal Gateway Protocol*) sobre enlaces que se encuentren mayormente congestionados , hacia otros enlace que se encuentren más libres, sin la necesidad de que la ruta que puedan tener estos sea la más corta posible, de esta manera obtiene mejores tiempos de respuesta en la recuperación ante fallos.
Además de que se puede realizar la planificación de la red en base a estadísticas del uso de LSPs, determinando así, los enlaces con mayores cargas y cuellos de botella, es posible que el administrador de la red pueda dar prioridades a determinados servicios, con diferente calidad y garantías, realizando un encaminamiento restringido.

2.3.13.2. CoS (Clases de servicio)

De acuerdo al modelo de *DiffServ* brinda la posibilidad de clasificar diferentes servicios, a través de este modelo que tiene diferentes mecanismos para la clasificación del tráfico, en un pequeño número de clases de servicio, con distintas prioridades. A través del uso de *DiffServ* los usuarios tienen la posibilidad de elegir entre diferentes servicios como puede ser: correo electrónico, www, aplicaciones en tiempo real, etc., para los que se marca el campos TOS (*Type of service*), ya que se trata una técnica para marcar los paquetes con Qos. Y otras cualidades ya explicadas en el apartado DiffServ.

2.3.13.3. VPNs (Redes Privadas Virtuales)

La comunicación en las redes privadas virtuales no se da mediante una conexión física, para que exista la comunicación debe existir una red común (internet), de esta manera se consigue transmitir datos como si estuviesen conectadas físicamente, para la transferencia de datos de una manera segura y garantizando la confiabilidad, se puede usar mecanismos de cifrado, estos mecanismos de cifrado se pueden usar de manera opcional. De acuerdo también a políticas de seguridad, resulta confiable el acceso solamente a personas autorizadas, para la implementación de las VPNs, se usa un estándar llamado IPSec, ya que este es soportado tanto por Internet I (IPV.4) e Internet II.

Dependiendo de la configuración es posible tener las siguientes redes privadas virtuales tales como: Acceso remoto de VPN para empleados, Acceso de sucursales a petición, Acceso persistente de las sucursales, Extranet para socios comerciales, VPN y conexión telefónica con autenticación RADIUS.

Los costos han llevado a adoptar estas soluciones, ya que para interconectar a empleados resulta mucho más barato utilizar una infraestructura pública, que desplegar una red físicamente privada, existe un nivel de seguridad en cuanto al envío de información a través de un red pública, puesto que los datos que se envían poseen un encabezado, que contiene información de enrutamiento hasta su destino, y los paquetes que puedan ser interceptados en la red pública no serán descifrados, sin la respectiva clave de cifrado.

Al tratarse de enlaces denominados cliente-red, el encapsulamiento se los realiza mediante el protocolo PPP(*Point to Point Protocol*), en primera instancia las tramas del cliente son encapsuladas en PPP, y luego este conjunto es nuevamente encapsulado, y así está listo para enviarse dentro de su VPN, de una manera segura. El acceso es independiente del proveedor de servicios de internet, por lo que nos da gran facilidad en cuanto a movilidad.

Al tratarse de datagramas en encapsulamiento se puede realizar por medio de: PPTP, L2TP e IPSec.

"**PPTP (point to point tunneling protocol):** Encapsulado de tramas PPP en datagramas IP, utilizando una versión extendida del GRE (Generic Routing Encapsulation, protocolo IP 47). La conexión de control se realiza sobre TCP, puerto 1723. Actualmente este protocolo, aunque muy popular en el mundo Microsoft, está siendo sustituido por el L2TP. La implementación de Microsoft, además, sufre de varios importantísimos errores de diseño que hacen que su protección criptográfica sea inefectiva para alguien más motivado que un simple observador casual." [10]

"**L2TP (layer 2 tunnelling protocol)**: Encapsulado de tramas PPP sobre cualquier medio, no necesariamente redes IP. En el caso IP se usa UDP, puerto 1701. Tras un largo proceso como borrador, L2TP pasa a ser una propuesta de estándar en Agosto de 1.999." [1010]

También se hace uso del protocolo:

"**IPSec**: IPSec es el nuevo marco de seguridad IP, definido con el advenimiento del IPv6. Aunque IPv6 está muy poco difundido en este momento, la tecnología marco IPSec se está utilizando ya, lo que asegura, entre otras cosas, la interoperatividad de los sistemas de diversos fabricantes. IPSec integra confidencialidad, integridad y autentificación en un mismo marco interoperante." [14]

2.3.13.4. Elementos para una VPN basado en MPLS

Para la construcción de una VPN basada en MPLS, son necesarios los siguiente elementos: P, PE, CE, C.

[10] http://es.wikipedia.org/wiki/RSA
[14] http://biblioteca.usac.edu.gt/tesis/08/08_0221_EO.pdf

P router de núcleo de red del proveedor: este enrutador no tiene una conexión con los routers clientes, para su interconexión se usan topologías de alta disponibilidad, no tienen configuración.

PE router de borde de red del proveedor: tienen la configuración de las VPNs, y se conectan a los clientes y a otros PE, también pueden tener conexión con los enrutadores P.

C router de cliente: estos enrutadores no tienen conexión con los enrutadores PE, son parte interna de red del cliente. Solo requieren funciones tradicionales de capa 3, y no necesariamente deben soportar MPLS.

CE router de borde de cliente: estos enrutadores se encuentran conectados los enrutadores PE, requieren funciones de capa 3 y no necesariamente soportan MPLS.

En la figura 2.23 se puede observar los elementos VPN en una red basada en MPLS.

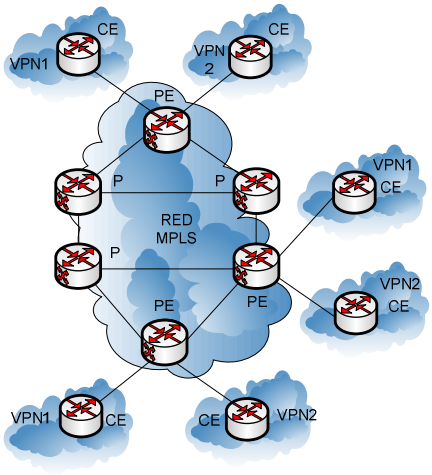

FIGURA. 2.23 Elementos de una VPN basada en MPLS

2.3.13.5. ESTRUCTURA DE UNA VRF (Virtual Routing and Forwarding)

Al hablar de VRF, nos referimos al enrutamiento virtual, al envío independiente y separado de cada una de las VPN dentro de la red MPLS.

Se necesita de una estructura lógica que será configurada en los routers, para la creación de la VRF, ya que P y PE deben de manejar VPNs con diferentes tipos de seguridad, y manteniendo la privacidad entre ellas. Para esto se analizara la estructura lógica que se encargara de esto: IBGP

2.3.13.6. MULTIPROTOCOLO IBGP (INTERNAL BORDER GATEWAY PROTOCOL)

Este protocolo se encarga lograr mayores características, como por ejemplo que un PE, tendría conocimiento de sobre las VRFs que se configurarían, y que no era posible que se vieran entre VRFs a nivel 3. M-IBGP permite manejar comunidades extendidas y otros protocolos además del IPv4, ya que este se encargara de distribuir información a los PEs sobre el enrutamiento para las VRFs.

M-IBGP debe tener una estructura de conexión en malla, con todos sus vecinos PE, esta conexión es de tipo lógica, si se quisiera realizar la configuración en una red de tamaño grande, resultaría tedioso y difícil, por lo que se usa el Router Reflector(RR), este nuevo router ayuda a simplificar la simplicidad de la configuración de M-IBGP, ya que solo es necesario disponer de un sesión entre los PEs y el RR, de esta manera los PEs enviaran información hacia los RR y estos se encargaran de difundir hacia los PEs faltantes.

2.3.13.7. RD IDENTIFICADOR DE RUTAS

Es un identificador que permite que las rutas que fueron creadas por el CE, se envíen a su respectivo PE. De esta manera los prefijos que se hayan creado en la VRF, van a ser únicos en toda la red. Quiere decir que si tenemos un paquete IPv4 a este se le adicionara 64bits, en total resultaría una dirección de 94bits conocida como VPNv4. Es posible reutilizar las direcciones IP que ya se han usado en otros clientes, todo esto gracias a los RD.

2.3.13.8 RT RUTA OBJETIVO

A las direcciones VPNv4, se les agrega más información para indicar que pertenecen a la VPN, esa información es el RT, y es importante, ya que en determinado momento, el RD no puede identificar su participación en más de una VPN, a partir de esto se puede realizar la configuración para escenarios más complejos de VPNs. Además con esta información o atributo, es posible la justificación de las operaciones que realiza el PE, y que permite la creación de VRFs.

En la figura 2.24, podemos observar el funcionamiento del envío de paquetes mediante una VRF.

En un inicio debe existir la trayectoria virtual, y esta va a estar asociada a un determinado FEC, y esto será útil en una VRF para enviar paquetes, el PE se basa en la pila de etiquetas, y con este asignara una etiqueta con la que será posible identificar al VRF. A través de la conmutación de etiquetas, se lograra enviar el paquete a su destino PE. Cuando el paquete llego a su PE destino, este a través de la información de la etiqueta, determinara la interface por la que se enviara el paquete, entonces removerá la etiqueta y enviara el paquete por dicha interface que se encontrara conectada al CE que corresponda.

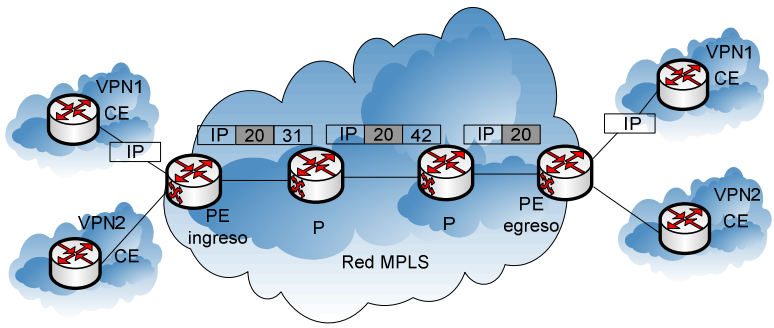

Figura. 2.24 Envío de paquetes en una VRF

Cuando el paquete ingresa en el PE, este informara de la etiqueta asignada al PE de egreso mediante el M-IBGP, de esta manera las los elementos físicos y lógicos, se comunicaran para hacer posible el funcionamiento de la VRF, y a su vez la VPN.

BIBLIOGRAFÍA – CAPÍTULO 2

[1] *"Tendencia en Tecnologías Ethernet Metropolitanas",* julio 2011
http://sistemas.itlp.edu.mx/ponencias/3.pdf

[2] ALLER, Conchi y otros, "*Redes Metro Ethernet*", julio 2011
http://www.coit.es/publicaciones/bit/bit149/64-66.pdf

[3] WIKIPEDIA**,** "*Redes Metro Ethernet*", julio 2011
http://es.wikipedia.org/wiki/Metro_Ethernet

[4] MAYA, Marcela y otros, *"Metro Ethernet"*, julio 2011
http://www.monografias.com/trabajos17/metro-ethernet/metro-ethernet.shtml

[5] LIMA, Servio, *"Las redes de Área Metropolitana basadas en Ethernet en el Ecuador"*, julio 2011
http://www.docstoc.com/docs/25917668/LAS-REDES-DE-AREA-METROPOLITANA-BASADAS- EN-ETHERNET-EN

[6] CARREON, Roberto, *"Redes Privadas Virtuales"*, julio 2011
http://www.monografias.com/trabajos11/repri/repri.shtml

[7] WIKIPEDIA**,** *"Redes Privadas Virtuales"*, julio 2011
http://es.wikipedia.org/wiki/Red_privada_virtual

[8] Hevia, Mariano, *"Virtual Private Networks (VPN)",* julio 2011
http://www.monografias.com/trabajos12/monvpn/monvpn.shtml

[9] WIKIPEDIA, *"CHAP",* agosto 2011
http://es.wikipedia.org/wiki/CHAP

[10] WIKIPEDIA, *"RSA"*, agosto 2011
http://es.wikipedia.org/wiki/RSA

[11] "*METRO ETHERNET Y MPLS*", Escuela Politécnica Nacional
http://dspace.epn.edu.ec/bitstream/15000/8678/5/capitulo_2.pdf

[12] WIKIPEDIA, **"***Multiprotocol Label Switching"*, agosto 2011
http://es.wikipedia.org/wiki/Multiprotocol_Label_Switching

[13] FLORES, Ricardo y GONZÁLEZ, Santiago, *"Protocolo múltiple por conmutación de etiquetas (MPLS): fundamentos y aplicaciones"*, Tesis Universidad Politécnica Salesiana, Cuenca, nov-2006
http://dspace.ups.edu.ec/bitstream/123456789/209/3/Capitulo%202.pdf

[14] SILVESTRE, Kelvin, *"Estudio de las ventajas e implementación de servicios IP VPN, sobre una infraestructura MPLS en la Región Centroamericana"*, Tesis Universidad de San Carlos de Guatemala, nov - 2008
http://biblioteca.usac.edu.gt/tesis/08/08_0221_EO.pdf

CAPITULO 3

DISEÑO DE LA RED METRO EHTERNET

3.1 PLANTEAMIENTO DEL DISEÑO DE LA RED.

3.1.1 INTRODUCCIÓN

En el presente capítulo se plantea el análisis y diseño de una red Metro Ethernet, para las Fuerzas Armadas Terrestres, estableciendo aspectos técnicos, como el transporte de información a través de una Red de Enlaces de Radio, el tipo de Protección de las Microondas, el tráfico que manejara la Red en base a los servicios a soportar, las consideraciones de ancho de banda que consumirá cada servicio y un estudio de factibilidad económica de implementación de red.

En el estudio no se contempla el marco legal referente a la concesión de frecuencia puesto que la Red Militar ya dispone la licencia de la misma; es decir, la red actual opera en 7GHz. Ha sido la necesidad y requerimiento actualizar la Red de Transporte existente por otra de mayor capacidad y de mayores prestaciones, con la cual se pueda migrar no solamente la conmutación de circuitos a conmutación de paquetes del servicio trunking existente, sino que también implementar servicios (convergencia) que ya se convierten el día de hoy en básicos para la mayoría de empresas y puntualmente para esta, en una solución a sus necesidades de monitoreo, seguridad y exclusividad de tráfico.

3.1.2. PARTES QUE CONSTITUYEN LA RED METRO ETHERNET MILITAR

3.1.2.1 NUBE METROEHTERHET: RED DE RADIO ENLACES

Las Fuerzas Militares Terrestres disponen de una red de radio enlaces ubicados geográficamente en zonas altas estratégicas y con línea de vista directa, actualmente

poseen toda la infraestructura montada para su servicio troncalizado (radio trunking). Al hablar de infraestructura nos referimos a Nodos (Estaciones Base) que poseen Torres de 30 metros de Altura en muy buen estado, Sistemas de Tierra, Sistemas de Energía, Sistema de Respaldo de Energía, etc. Paralelo a esto se presenta un diseño de Red Adicional que nos permitirá que la misma tenga una redundancia que garantice la conexión y que soporte la tecnología en estudio.

Para el caso puntual de la Red Redundante ha sido necesario realizar un survey en sitio en varios Nodos, para levantar información que nos permita validar los diferentes enlaces de repetición a incluirse en el diseño, el estudio de infraestructura de esta parte no se contempla en la tesis puesto que no es requerimiento esencial de la III Zona Militar y porque ellos ya manejan y disponen de esta información.

La ingeniería y los estudios Radioeléctricos se los ha realizado a través del software de diseño profesional licenciado PathLoss, el cual nos da según las características del enlace (coordenadas, tecnología, umbrales de ganancia, potencia, alturas, etc.) un reporte detallado real del radio enlace, el cual nos sirve para garantizar la eficiencia del mismo.

3.1.2.2 ESQUEMA DE LA RED

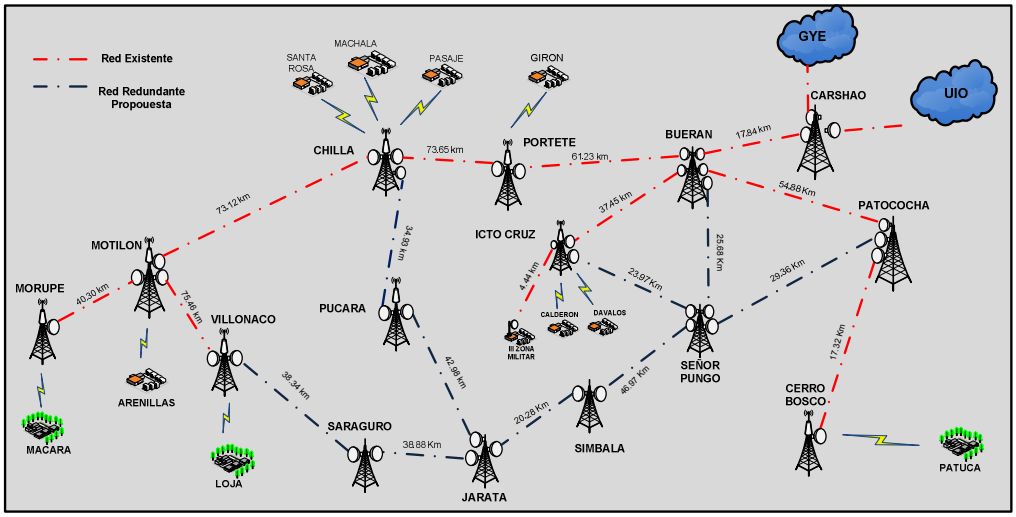

Figura 3.1. Esquema de la Red Metro Ethernet Militar

Además de la elección de los equipos de radio y de sus parámetros de funcionamiento, son factores importantes la buena ubicación de las antenas y la elección de un canal libre de interferencias y desvanecimientos de la señal, alcanzando una alta eficiencia del sistema.

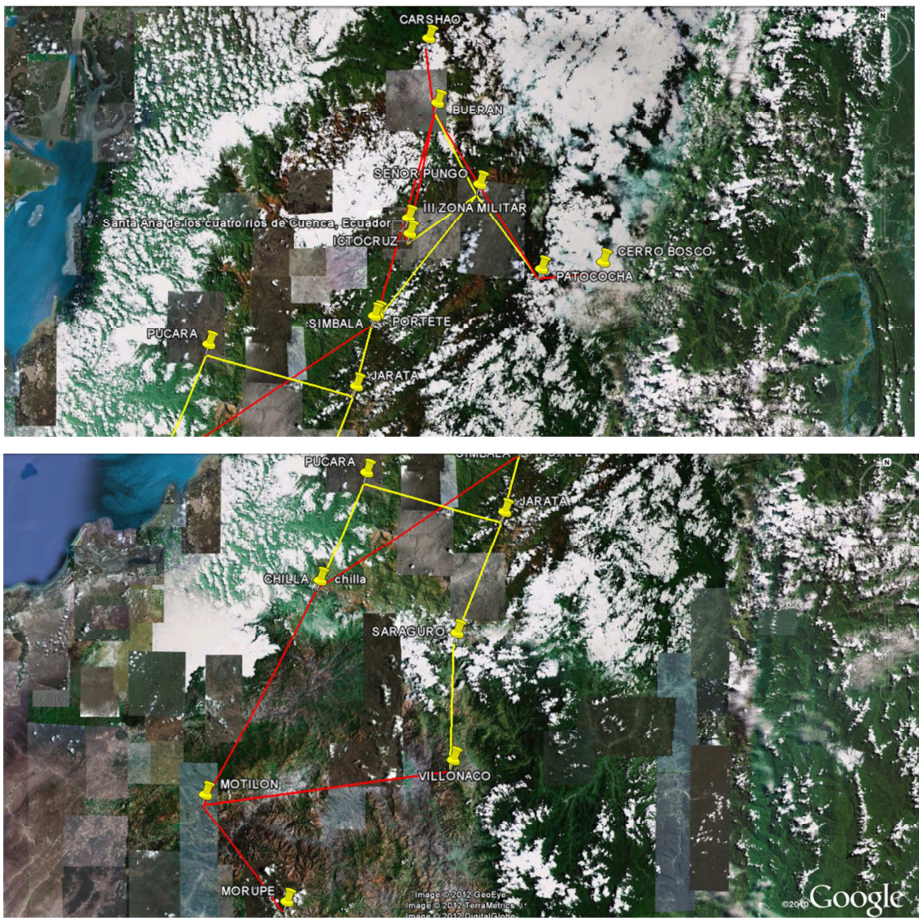

Figura 3.2. Ubicación Geográfica de la Red Militar (Google Earth)

3.1.2.3 DISEÑO DE LA RED DE RADIO ENLACES

El diseño en su primera parte está basado en la topología de red existente (figura 3.1); es decir, se utiliza las mismas coordenadas, alturas y ubicaciones de los Nodos para emitir el esquema de Red, siguiendo el objetivo del proyecto que es hacer que la Red sea MPLS, se estructura el complemento redundante de la misma, con la cual se pueda

garantizar la conexión y hacer uso de los beneficios y aplicaciones de la Tecnología (VRFs).

Se incluyen a continuación características y detalles de cada Radio Enlace que conforma de Red, los estudios de Ingeniería de la parte existente y redundante ambos realizados en el Software de Calculo Profesional Pathloss se presentan correspondientemente en la Parte de Anexos. En cuanto a la infraestructura física de la red redundante, se asume para el diseño el mismo escenario de los Nodos (Estaciones Base) existentes.

La red existente consta de 11 puntos de conexión los cuales se citan a continuación:

- III Zona Militar
- Icto Cruz
- Bueran
- Carshao
- Patococha
- Cerro Bosco
- Portete
- Chilla
- Motilón
- Morupe
- Villonaco

La red de redundancia consta de 4 puntos de conexión los cuales se citan a continuación:

- Señor Pungo
- Jarata
- Simbala
- Pucara
- Saraguro

Los cuales se ubican de acuerdo al diagrama de la figura 3.3:

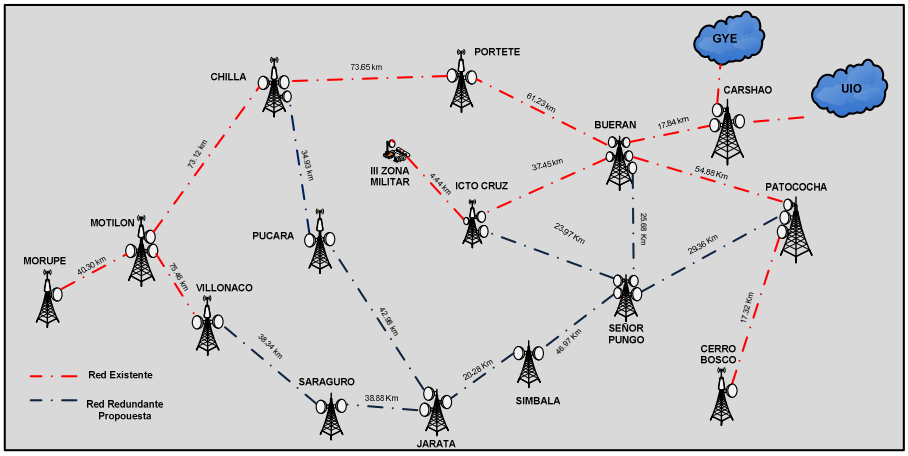

Figura 3.3. Red Metro Ethernet Fuerzas Armadas Militares

3.1.2.3.1 CARACTERISTICAS DE LOS ENLACES QUE CONFORMAN LA RED

NODO	UBICACIÓN GEOGRAFICA		ALTURA SOBRE EL NIVEL DEL MAR
	LATITUD	LONGITUD	
III ZONA MILITAR	02º53’27.46’’S	79º00’4.15’’ W	2554 msnm
ICTO CRUZ	2º55’51.59’’ S	78º59’51.70’’W	2833 msnm
BUERAN	2º35’58.30’’ S	78º55’43.60’’ W	3793 msnm
PATOCOCHA	3º01’07.00’’ S	78º39’52.00’’ W	3569 msnm
CERRO BOSCO	3º00’02.00’’ S	78º30’35.00’’ W	2372 msnm
PORTETE	3º07’56.49’’ S	79º04’43.61’’ W	3196 msnm
CHILLA	3º29’58.57’’ S	79º37’53.93’’ W	3509 msnm
MOTILON	4º04’58.89’’ S	79º56’29.44’’ W	2635 msnm
VILLONACO	3º59’18.19’’ S	79º16’06.78’’ W	2896 msnm
MORUPE	4º22’14.90’’ S	79º43’07.40’’ W	2644 msnm
CARSHAO	2°26'23.20" S	78° 57'3.80" W	3992 msnm

Tabla 3.1. Características de los Nodos que forman la Red Existente

NODO	UBICACIÓN GEOGRAFICA		ALTURA SOBRE EL NIVEL DEL MAR
	LATITUD	LONGITUD	
SIMBALA	3° 8' 12.90'' S	79° 5' 9.90'' W	3147 msnm
JARATA	3° 18'52.60" S	79° 7'52.70" W	3420 msnm
SARAGURO	3°31' 39.24'' S	79° 32' 46.63''W	3774 msnm
SEÑOR PUNGO	2°48' 19.60'' S	78° 49' 19'' W	3139 msnm
PUCARA	3°14' 1.3 '' S	79° 29' 8'' W	3168 msnm

Tabla 3.2. Características de los Nodos que forman la Red Redundante

3.1.2.3.2 DISTANCIAS ENTRE RADIO ENLACES

SITIO 1	SITIO 2	DISTANCIA DEL ENLACE (KM)
III ZONA MILITAR	ICTO CRUZ	4.44
ICTO CRUZ	BUERAN	37.45
BUERAN	PATOCOCHA	54.88
BUERAN	CARSHAO	17.84
PATOCOCHA	CERRO BOSCO	17.32
BUERAN	PORTETE	61.23
PORTETE	CHILLA	73.65
CHILLA	MOTILON	73.12
MOTILON	VILLONACO	75.46
MOTILON	MORUPE	40.30

Tabla 3.3. Distancia de Enlaces Existentes.

SITIO 1	SITIO 2	DISTANCIA DEL ENLACE (KM)
SEÑOR PUNGO	BUERAN	25.68
SIMBALA	JARATA	20.28
SARAGURO	VILLONACO	38.34
SEÑOR PUNGO	ICTO CRUZ	23.97

SEÑOR PUNGO	SIMBALA	46.97
SEÑOR PUNGO	PATOCOCHA	29.36
PUCARA	JARATA	42.98
PUCARA	CHILLA	34.93
JARATA	SARAGURO	38.88

Tabla 3.4. Distancia de Enlaces Redundantes.

3.1.2.3.3 ENLACE III ZONA MILITAR-ICTO CRUZ

Este enlace tiene 4.44 Km de distancia, los equipos a utilizar son SAF CFIP PHOENIX 7 GHz SDH de 100Mbps de Capacidad, estos equipos tienen protección 1+1 HSB. Las antenas son parabólicas COMHAT de 0.6 m de diámetro con una ganancia de 30,20 dBi, esto debido a la distancia corta que se tiene.

En la III Zona Militar se dispone de una torre de viento triangular de 30 cm de lado y de 12 metros de altura, se tiene línea de vista directa hacia el Nodo Icto Cruz. Este punto es muy importante porque es el punto de Administración de Red, el departamento técnico y de Soporte se encuentra en este sitio.

ESQUEMA

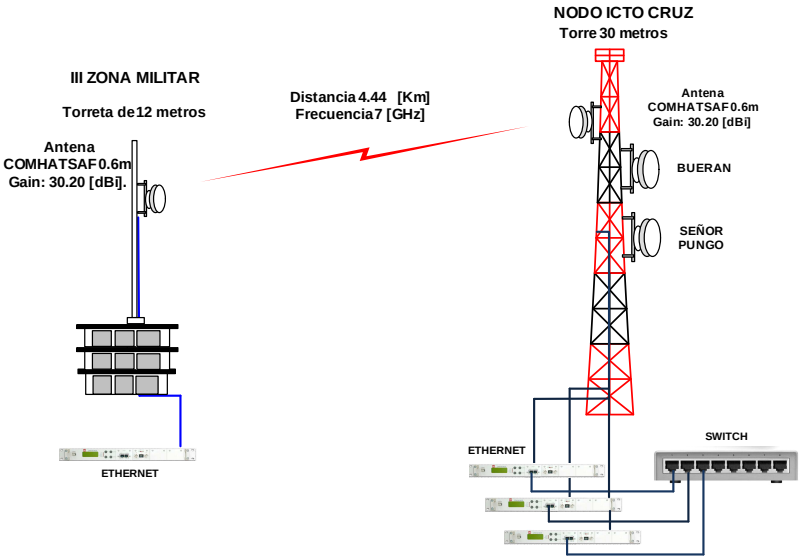

Figura 3.4. Esquema del enlace III Zona Militar-Nodo Icto Cruz

PERFIL

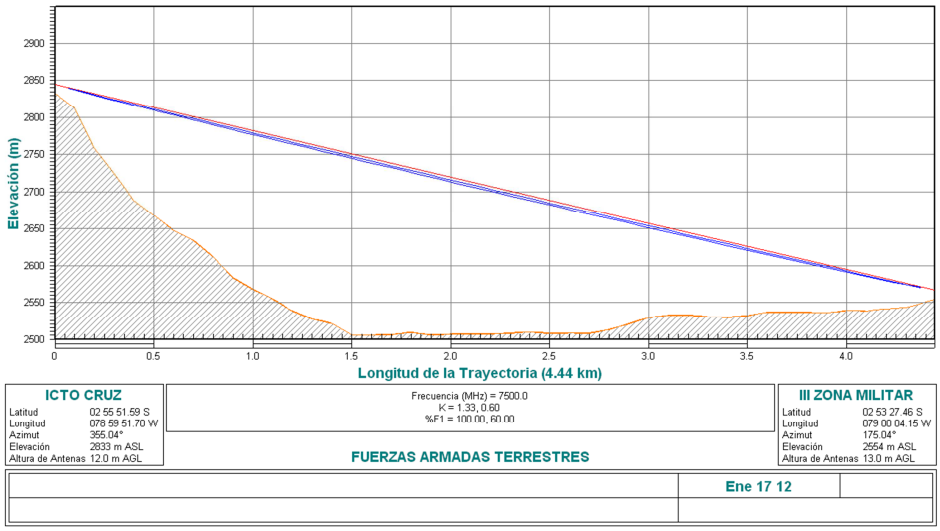

Figura 3.5. Perfil del enlace III Zona Militar-Nodo Icto Cruz

3.1.2.3.4. ENLACE ICTO CRUZ-BUERAN

Este es un enlace de 37.45 Km de distancia, los equipos a utilizar son SAF CFIP PHOENIX 7 GHz SDH de 100Mbps de Capacidad, estos equipos tienen protección 1+1 HSB. Las antenas son parabólicas COMHAT de 1,2 m de diámetro con una ganancia de 37.46 dBi.

ESQUEMA

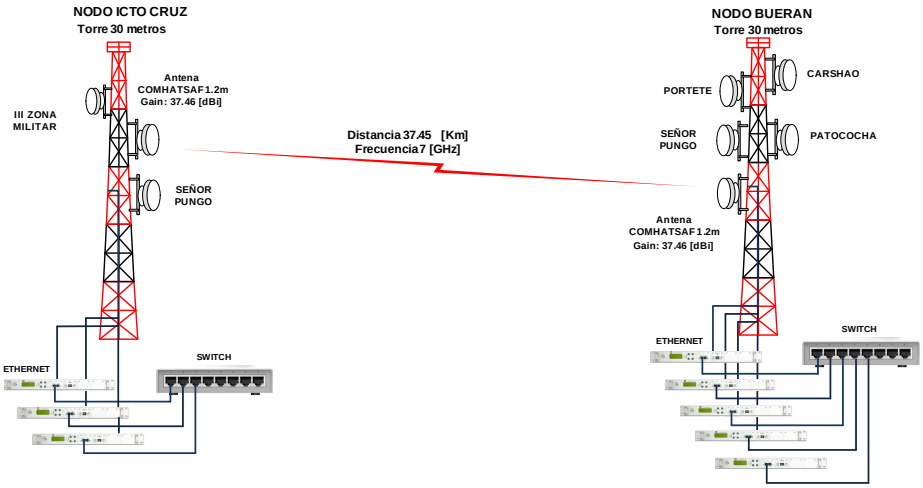

Figura 3.6. Esquema del enlace Icto Cruz-Bueran

PERFIL

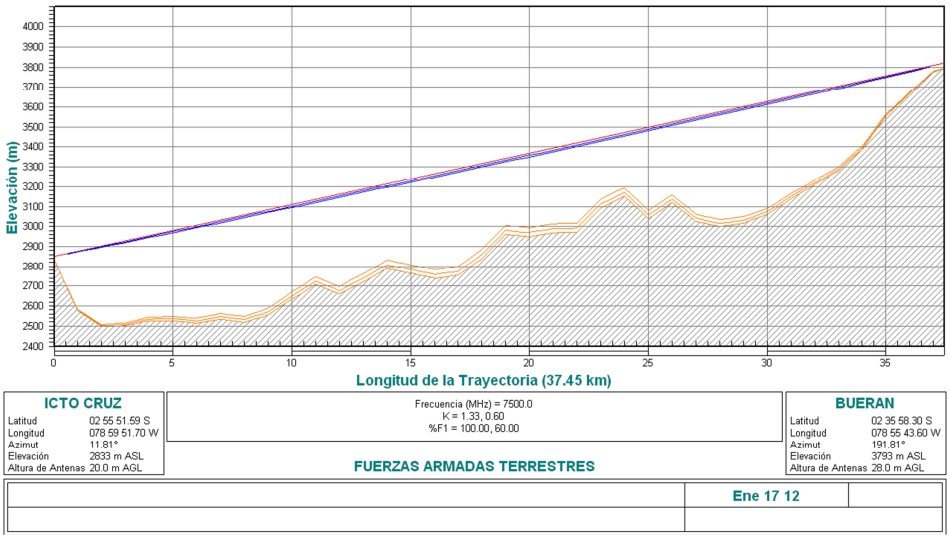

Figura 3.7. Perfil del enlace III Icto Cruz-Bueran

3.1.2.3.5. ENLACE BUERAN-CARSHAO

Este enlace es muy importante y critico porque une la Zona Sur del Ecuador, con la Zona Norte y con la Zona de Guayas. La distancia de este enlace es de 17.84 Km. Las antenas son parabólicas de 1,2 m de diámetro con una ganancia de 37.46 dBi.

ESQUEMA

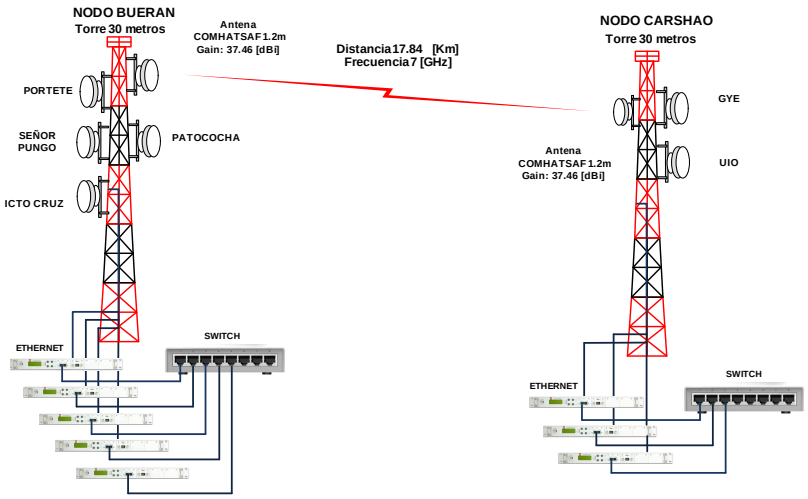

Figura 3.8. Esquema del enlace Bueran-Carshao

PERFIL

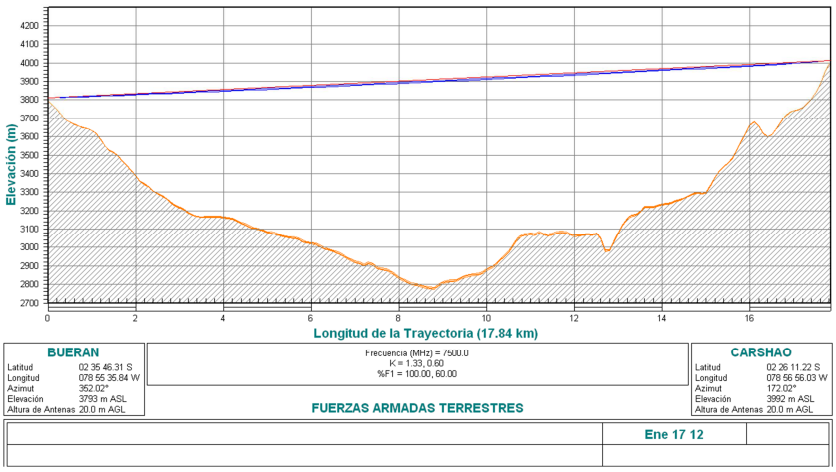

Figura 3.9. Perfil del enlace Bueran-Carshao

3.1.2.3.6. ENLACE BUERAN-PATOCOCHA

La Modulación de este enlace es QPSK por ser una Zona lluviosa. Este enlace tiene una distancia de 54.88 Km. Las antenas son parabólicas de 3,2 m de diámetro con una ganancia de 45.5 dBi.

ESQUEMA

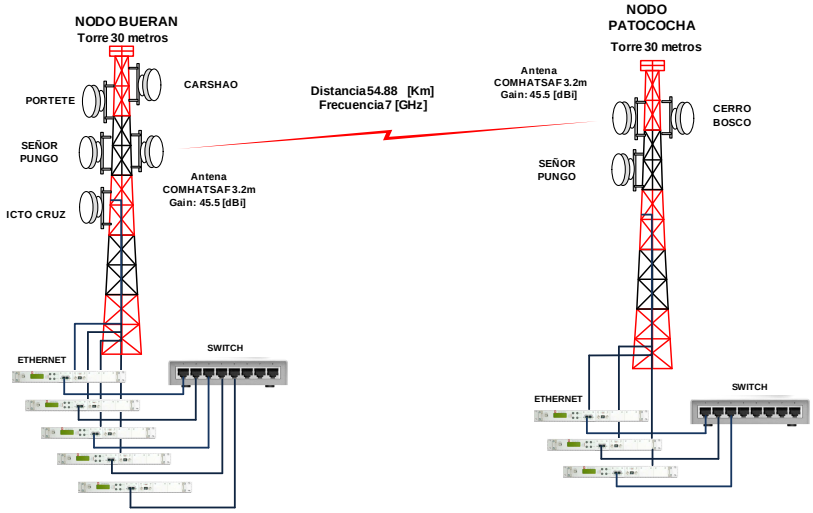

Figura 3.10. Esquema del enlace Bueran-Patococha

PERFIL

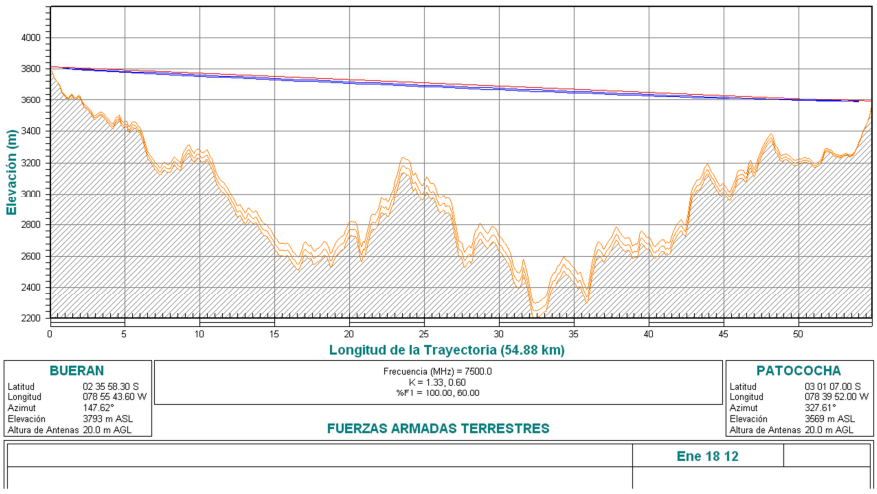

Figura 3.11 Perfil del enlace Bueran-Patococha

3.1.2.3.7. ENLACE PATOCOCHA-CERRO BOSCO

La Modulación de este enlace se la considera QPSK por ser una Zona muy lluviosa del Oriente Ecuatoriano, la distancia entre Nodos es de 17.32 Km. Las antenas son parabólicas de 1,8 m de diámetro con una ganancia de 41 dBi. El Nodo Cerro Bosco es la interconexión mediante el cual se da cobertura a la Zona de Morona Santiago (Destacamento Patuca).

ESQUEMA

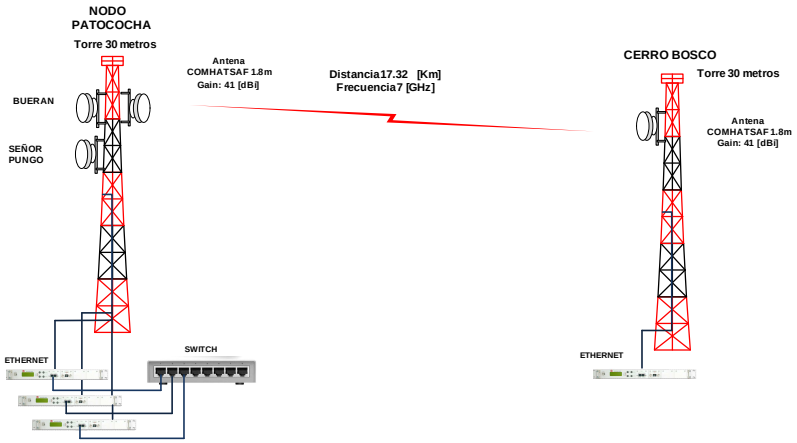

Figura 3.12 Esquema del enlace Patococha-Cerro Bosco

PERFIL

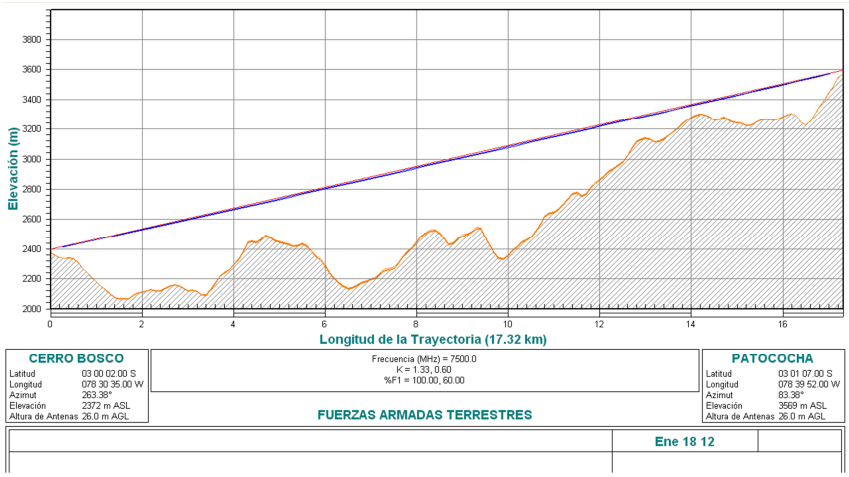

Figura 3.13 Perfil del enlace Patococha-Cerro Bosco

3.1.2.3.8. ENLACE BUERAN-PORTETE

La Modulación de este enlace se la considera en 32APSK, por su gran distancia de 61.23 Km, cabe recalcar que ya funciona un enlace con estas características, con una protección HSB 1+1. Las antenas son parabólicas COMHAT de 3,2 m de diámetro con una ganancia de 45.5 dBi. El gran diámetro de estas antenas nos proporciona mayor ganancia y por ende nos aseguran mayor eficiencia del enlace.

ESQUEMA

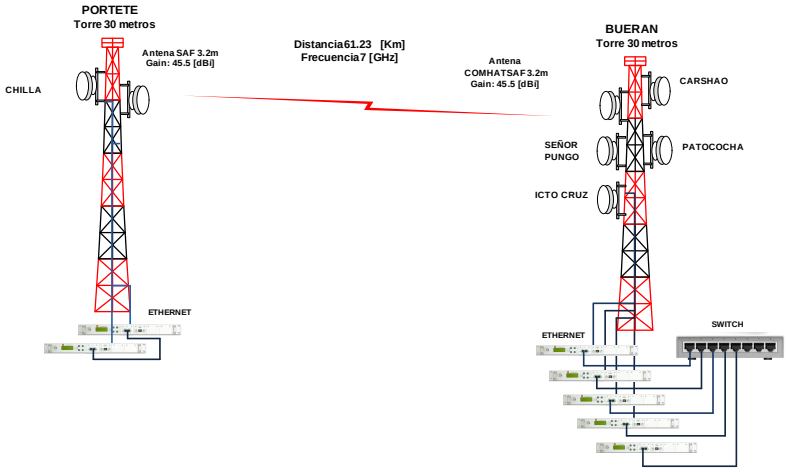

Figura 3.14. Esquema del enlace Portete-Bueran

PERFIL

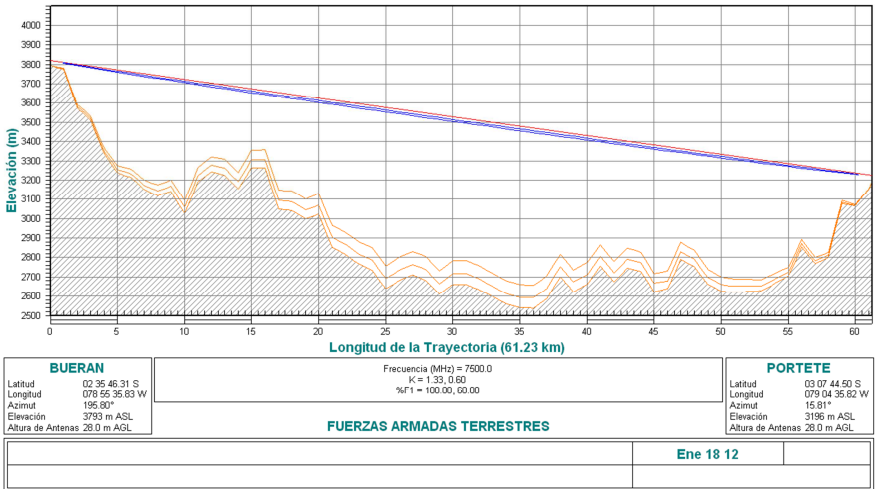

Figura 3.15. Perfil del enlace Portete-Bueran

3.1.2.3.9. ENLACE PORTETE-CHILLA

Este es otro enlace de gran distancia como la mayoría que conforma la red existente, el mismo tiene 73.65 Km. Las antenas son parabólicas de 3.2 m de diámetro con una ganancia de 45.5 dBi. El Nodo Portete da cobertura al Destacamento de Girón, mientras que el Nodo de Chilla da cobertura a los Destacamentos de Pasaje, Machala y Santa Rosa.

ESQUEMA

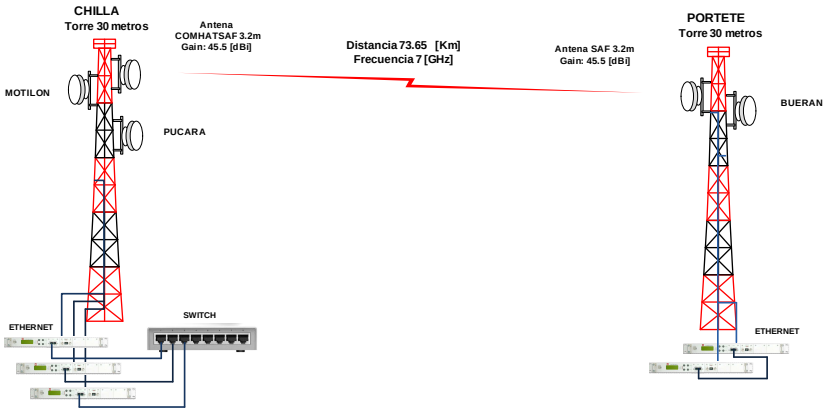

Figura 3.16. Esquema del enlace Portete-Chilla

PERFIL

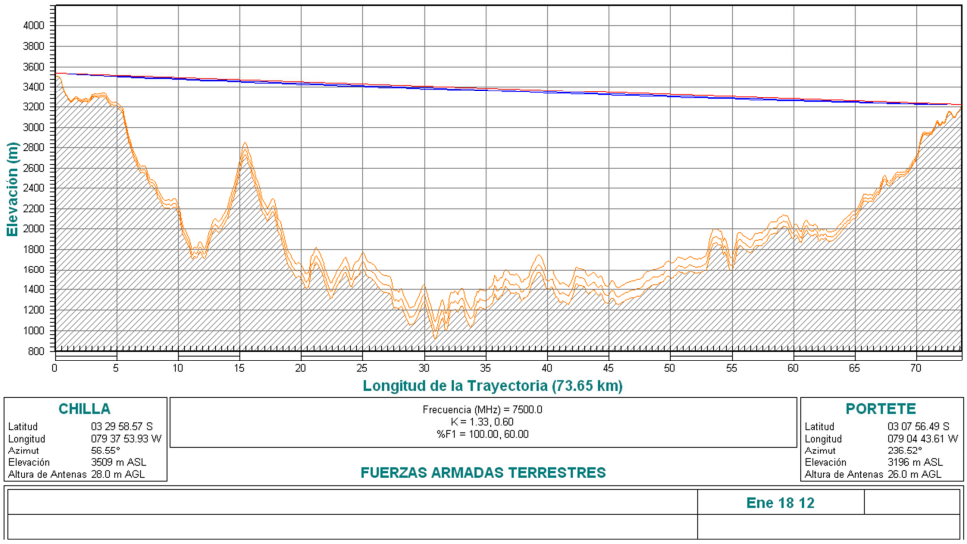

Figura 3.17. Perfil del enlace Portete-Chilla

3.1.2.3.10. ENLACE CHILLA-MOTILON

La distancia de este enlace es de 73.12 Km. Las antenas son de 3,2 m de diámetro con una ganancia de 45.5 dBi. El Nodo MOTILON da cobertura al Destacamento de Arenillas y el mismo sirve de interconexión con VILLONACO y MORUPE.

ESQUEMA

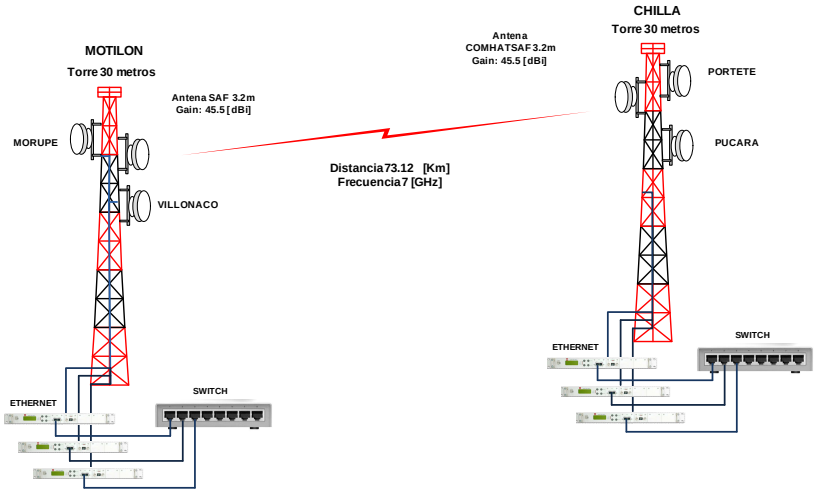

Figura 3.18. Esquema del enlace Chilla-Motilón

PERFIL

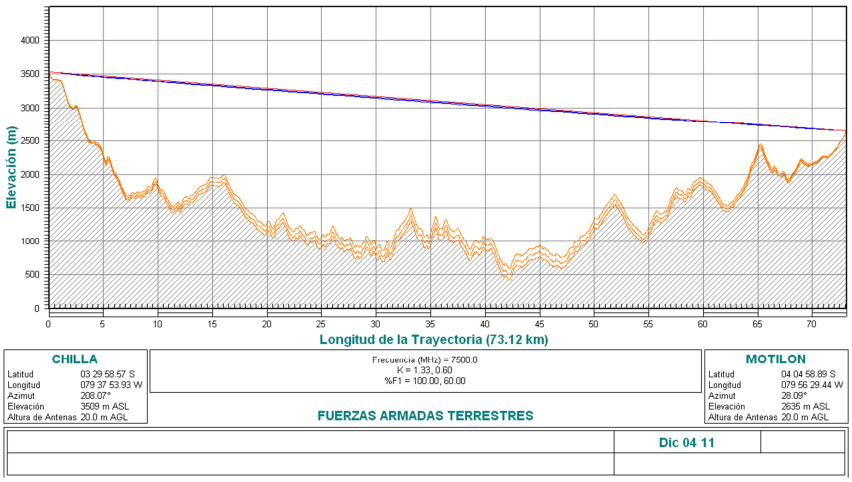

Figura 3.19. Perfil del enlace Chilla-Motilón

3.1.2.3.11. ENLACE MOTILON-VILLONACO

La distancia de este enlace es de 75.46 Km. Las antenas son de 3,2 m de diámetro con una ganancia de 45.5 dBi. El Nodo VILLONACO da Cobertura al Destacamento Loja.

ESQUEMA

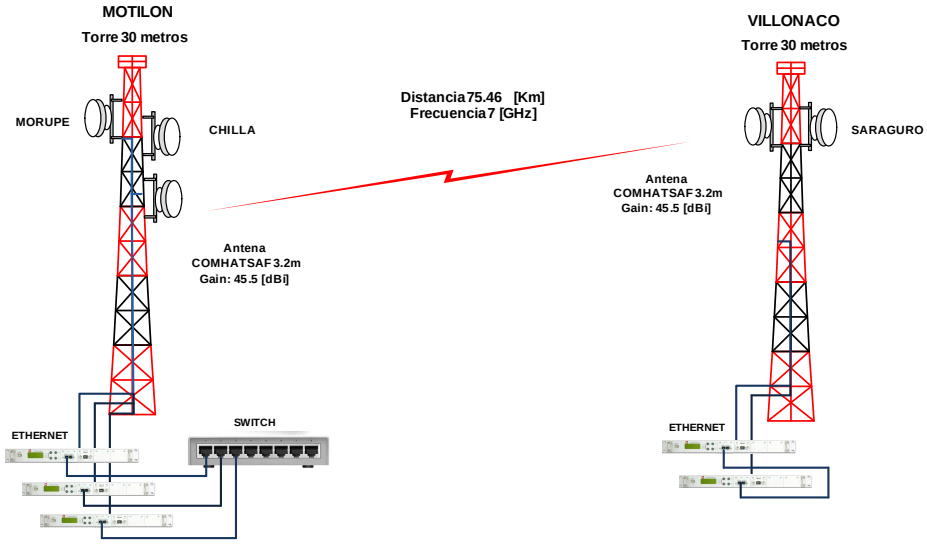

Figura 3.20. Esquema del enlace Motilón-Villonaco.

PERFIL

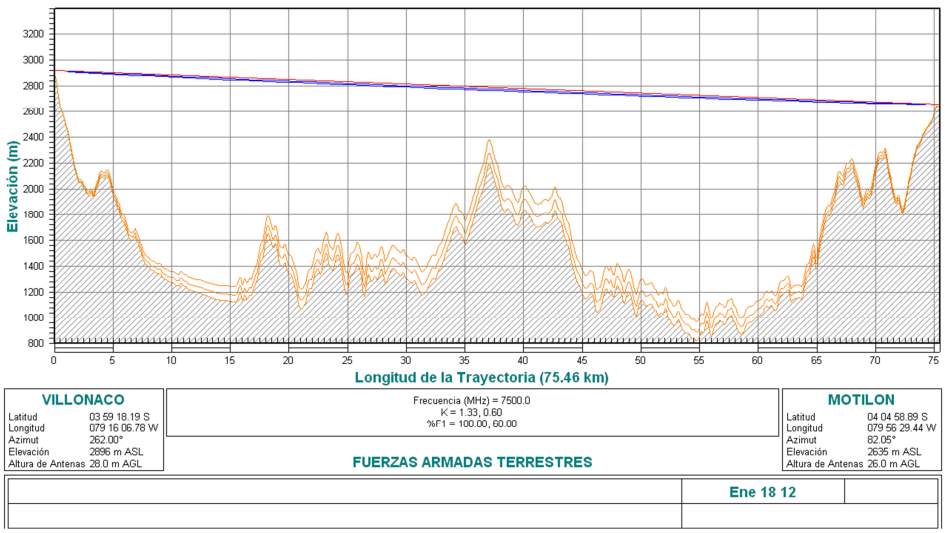

Figura 3.21. Perfil del enlace Motilón-Villonaco.

3.1.2.3.12. ENLACE MOTILON-MORUPE

El Nodo MORUPE da cobertura al Destacamento de Macara perteneciente a la provincia de Loja, esta localidad se encuentra en la Frontera con El Perú. Las antenas son de 2,4 m de diámetro con una ganancia de 43.5 dBi.

ESQUEMA

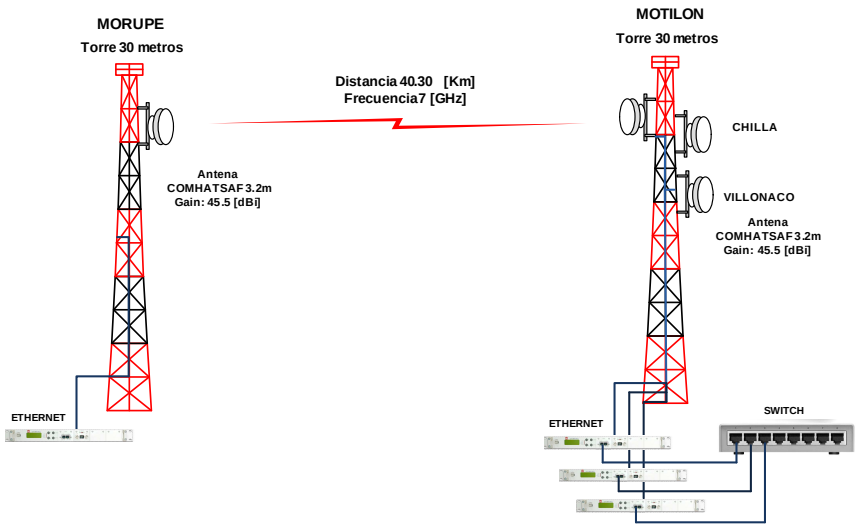

Figura 3.22. Esquema del enlace Motilón-Morupe.

PERFIL

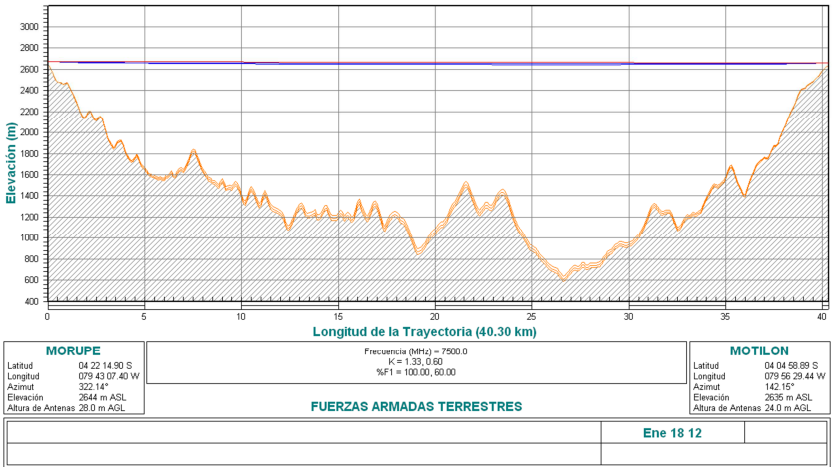

Figura 3.23. Perfil del enlace Motilón-Morupe.

RED REDUNDANTE MILITAR

Para aplicar las funcionalidades y ventajas de la tecnología MPLS a la Red Militar es necesario proponer un diseño de red que respalde la comunicación entre los diferentes puntos terminales de la misma; es decir que el servicio a prestar en los diferentes Destacamentos sea garantizado, para lo cual se presenta a continuación un detalle de los Nodos de Interconexión que forman parte de la Red Redundante, los estudios Radioeléctricos en donde constan todos los datos exactos del enlace se presentan en el Anexo Correspondiente. Es requerimiento de la III Zona Militar hacer el estudio de Ingeniería de los radio Enlaces.

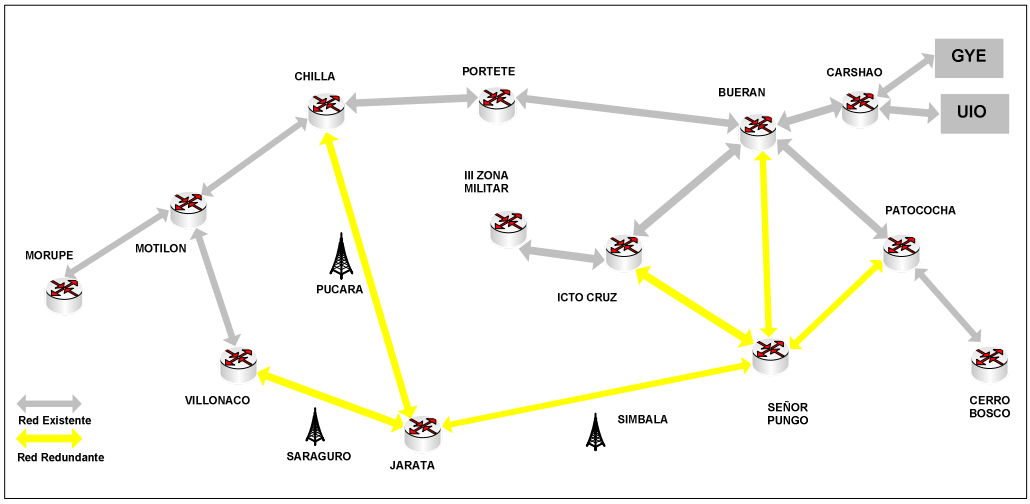

Figura 3.24 Redundancia de Red de la III Zona Militar

3.1.2.3.13. ENLACE BUERAN-SEÑOR PUNGO

El Nodo Señor Pungo sirve de Interconexión con 4 Nodos, este es una Zona estratégica desde la cual se respalda a la Red. Fue necesario realizar un survey en el sitio para tomar coordenadas y poder validar el enlace. La distancia de este enlace es de 25.68 Km. Las antenas son parabólicas de 2,4 m de diámetro con una ganancia de 43.5 dBi.

ESQUEMA

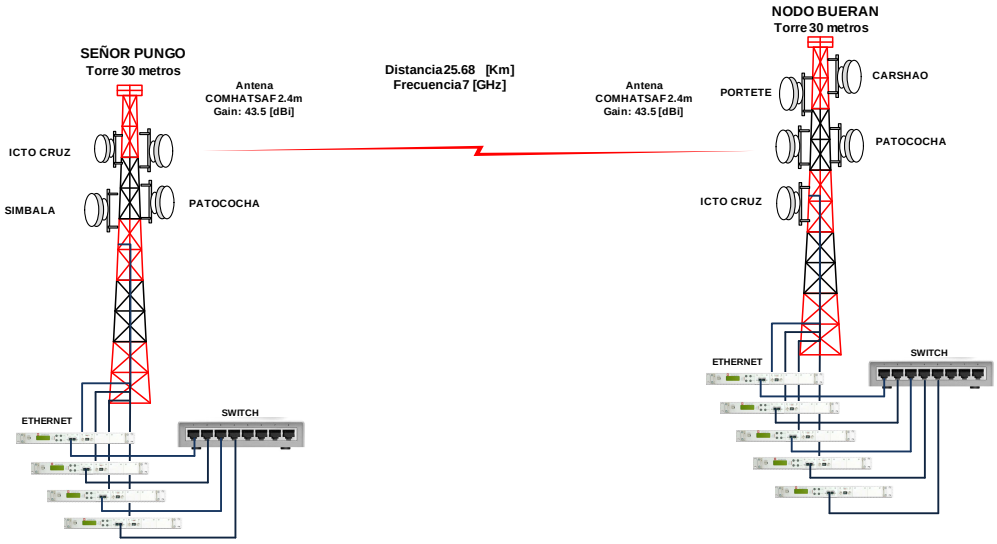

Figura 3.25. Esquema del enlace Bueran-Señor Pungo

PERFIL

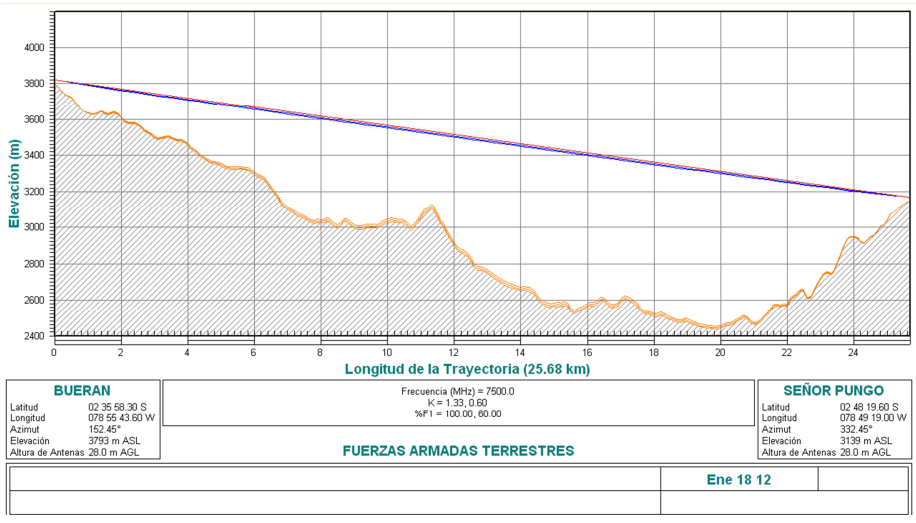

Figura 3.26. Perfil del enlace Bueran-Señor Pungo.

3.1.2.3.14. ENLACE SEÑOR PUNGO-ICTO CRUZ

Este enlace es importante porque en caso de caerse la conexión principal con el Nodo Bueran, el tráfico se enruta por el Nodo Señor Pungo. La distancia de este enlace es de 23.97 Km. Las antenas son de 2,4 m de diámetro con una ganancia de 43.5 dBi.

ESQUEMA

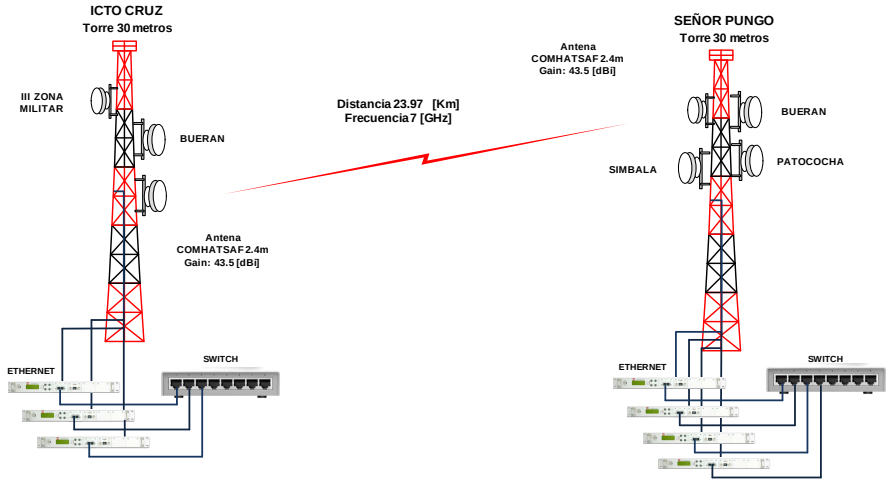

Figura 3.27. Esquema del enlace Señor Pungo-Icto Cruz

PERFIL

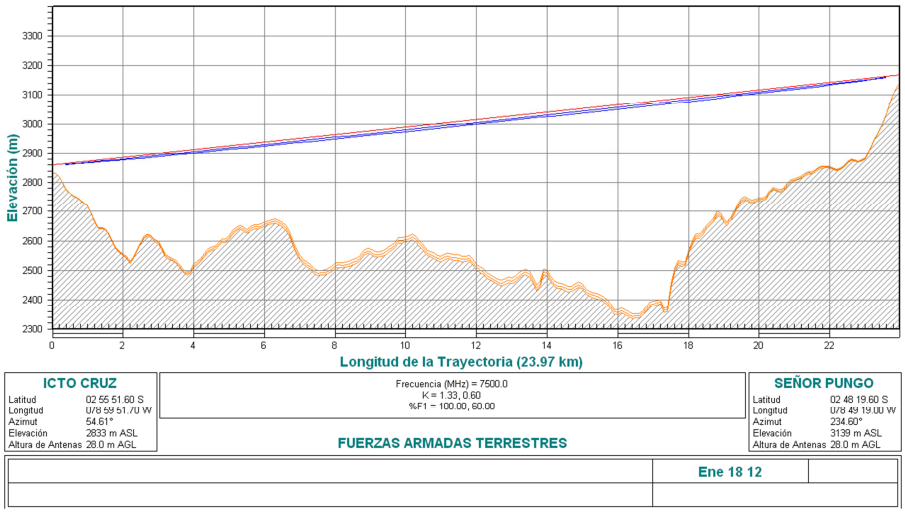

Figura 3.28. Perfil del enlace Señor Pungo-Icto Cruz.

3.1.2.3.15. ENLACE SEÑOR PUNGO-SIMBALA

Fue necesario tomar las coordenadas del Nodo Simbala en el sitio, puesto que este repetidor es muy importante para seguir con el anillo de la Red. La distancia de este enlace es de 46.97 Km. Las antenas son parabólicas de 3,2 m de diámetro con una ganancia de 45.5 dBi.

ESQUEMA

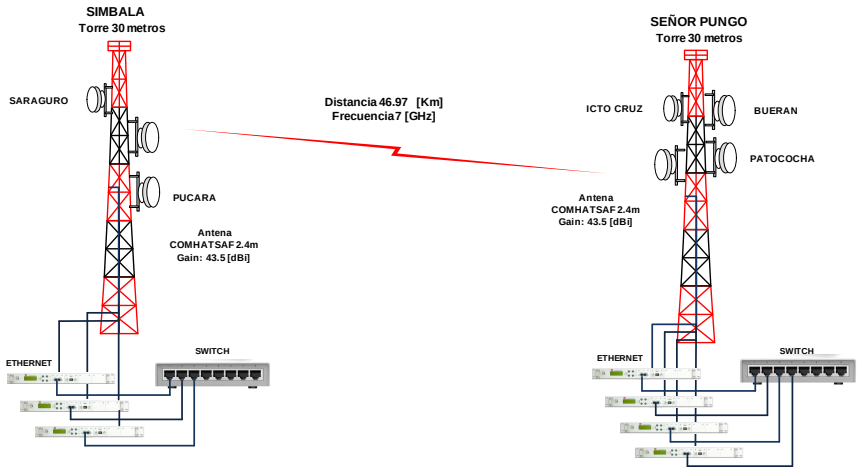

Figura 3.29. Esquema del enlace Señor Pungo-Simbala

PERFIL

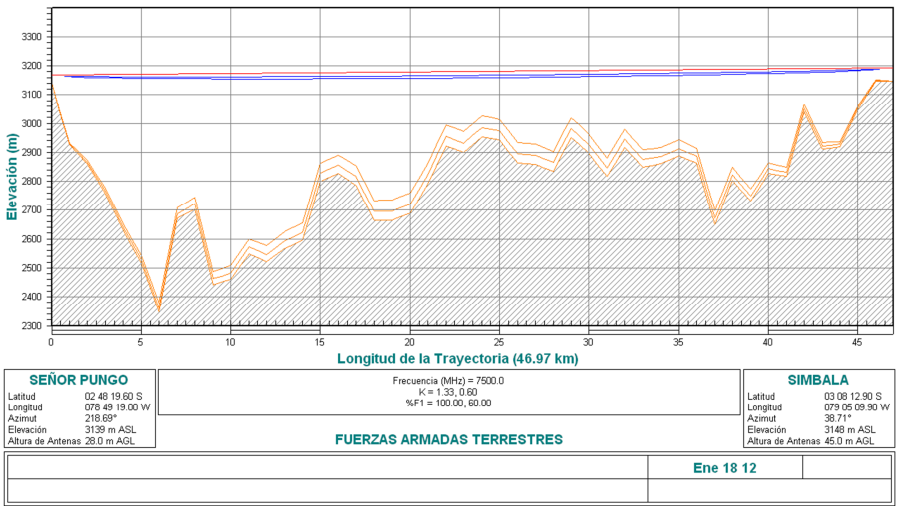

Figura 3.30. Perfil del enlace Señor Pungo-Simbala.

3.1.2.3.16. ENLACE SEÑOR PUNGO-PATOCOCHA

Este es un enlace redundante que sirve para asegurar la conexión con el Destacamento de Patuca en Morona Santiago, en un caso de caerse el principal con el Nodo Bueran. La distancia de este enlace es de 29.36 Km. Las antenas son parabólicas de 1,8 m de diámetro con una ganancia de 41 dBi.

ESQUEMA

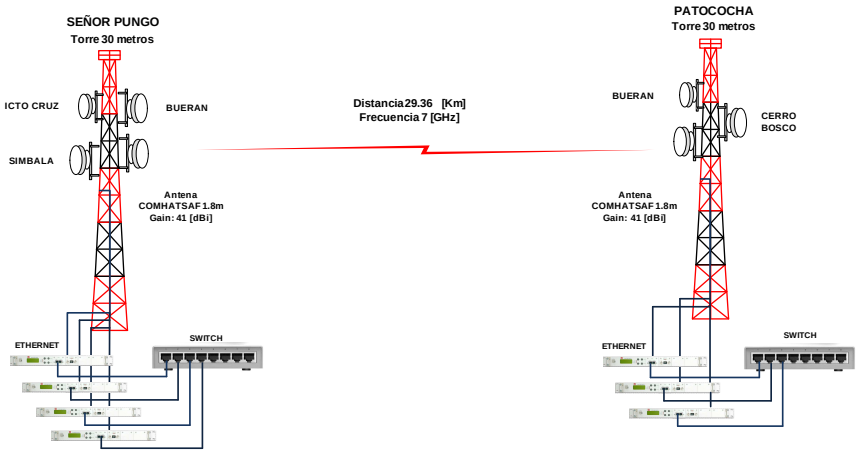

Figura 3.31. Esquema del enlace Señor Pungo-Patococha

PERFIL

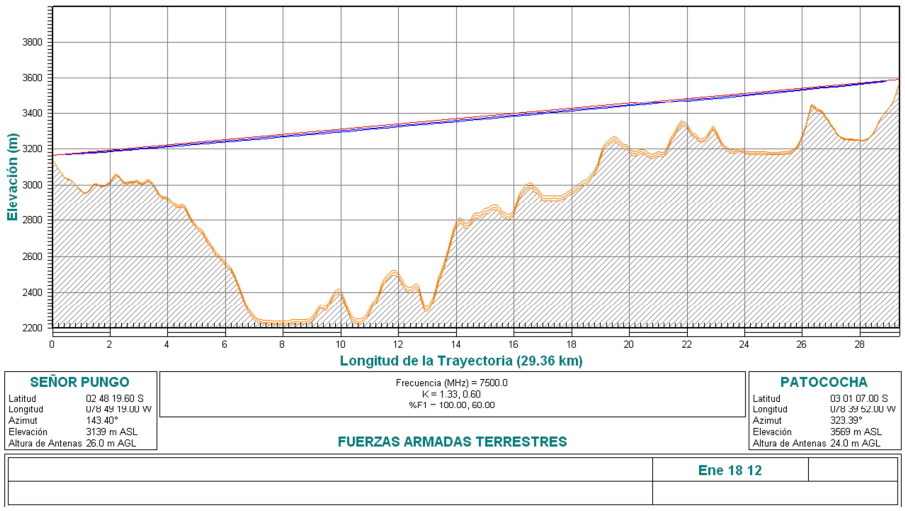

Figura 3.32. Perfil del enlace Señor Pungo-Patococha

3.1.2.3.17. ENLACE SIMBALA-JARATA

El Nodo Jarata sirve de redundancia para los destacamentos de Loja y El Oro. La distancia de este enlace es de 20.28 Km. Las antenas son parabólicas COMHAT de 1.8 m de diámetro con una ganancia de 37.5 dBi.

ESQUEMA

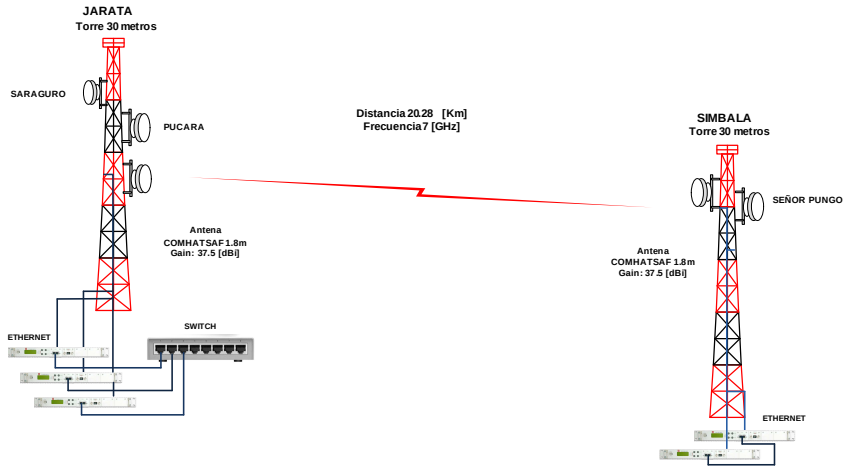

Figura 3.33. Esquema del enlace Jarata-Simbala

PERFIL

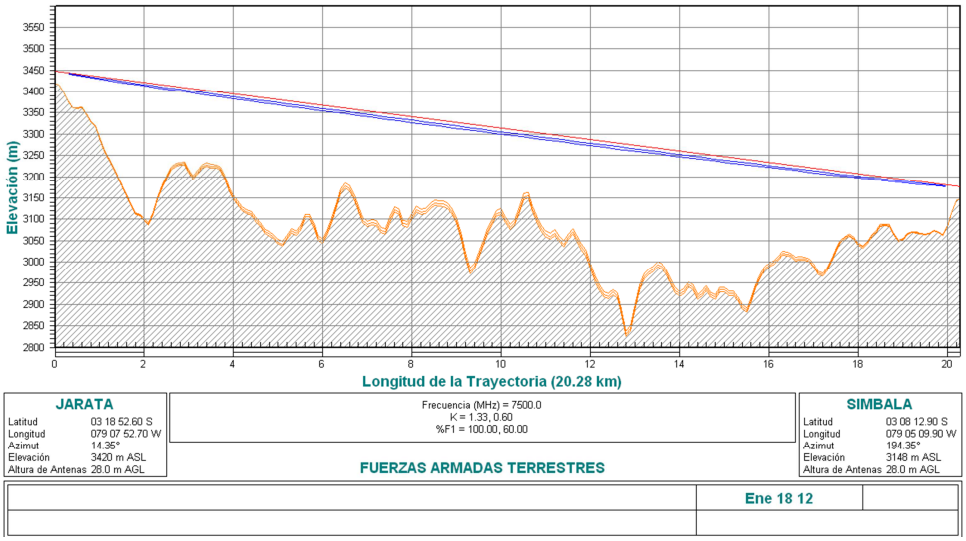

Figura 3.34. Perfil del enlace Jarata-Simbala

3.1.2.3.18. ENLACE SARAGURO-VILLONACO

El Nodo Saraguro se encuentra a 3283 msnm, en un cerro sobre la ciudad de Saraguro Cantón de la provincia de Loja, levantar la información de este sitio fue vital para unir la Red con el Nodo Villonaco y así cerrar el anillo de Red, respaldando al Destacamento de Loja. La distancia de este enlace es de 38.34 Km. Las antenas son parabólicas de 2.4 m de diámetro con una ganancia de 43.5 dBi.

ESQUEMA

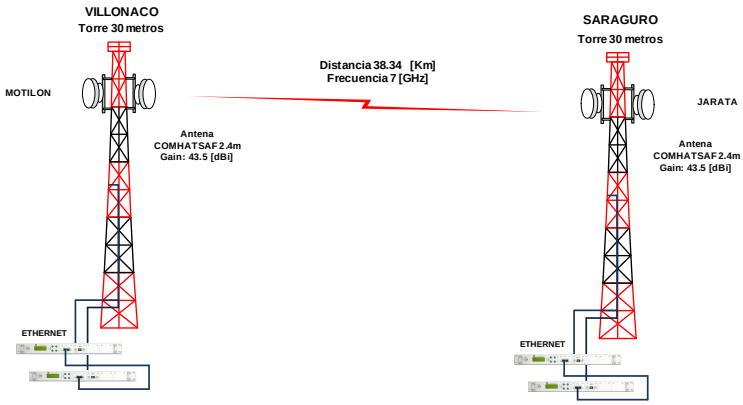

Figura 3.35. Esquema del enlace Saraguro-Villonaco

PERFIL

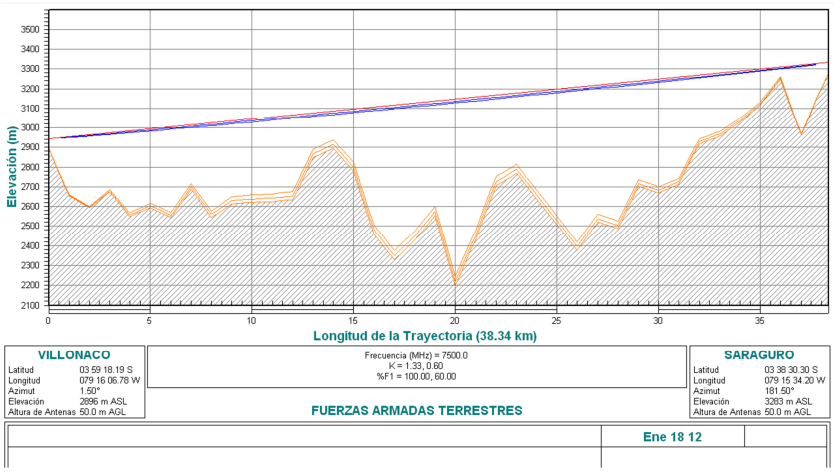

Figura 3.36. Perfil del enlace Saraguro-Villonaco

3.1.2.3.19. ENLACE JARATA-SARAGURO

La distancia de este enlace es de 38.88 Km. Las antenas son parabólicas de 2.4 m de diámetro con una ganancia de 43.5 dBi.

ESQUEMA

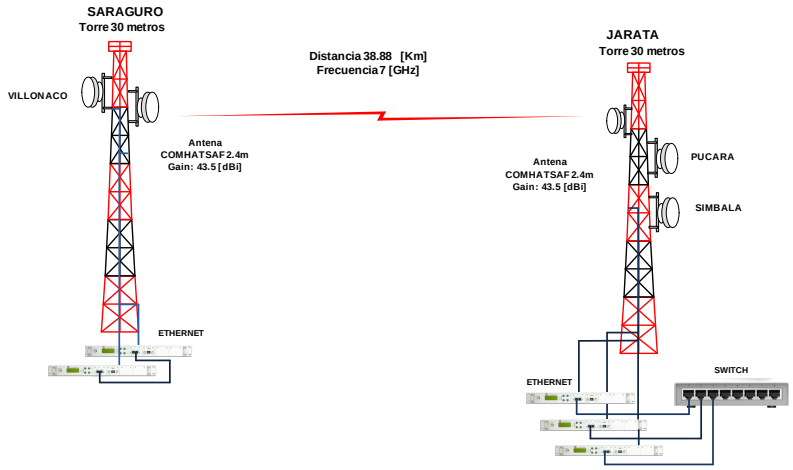

Figura 3.37. Esquema del enlace Jarata-Saraguro

PERFIL

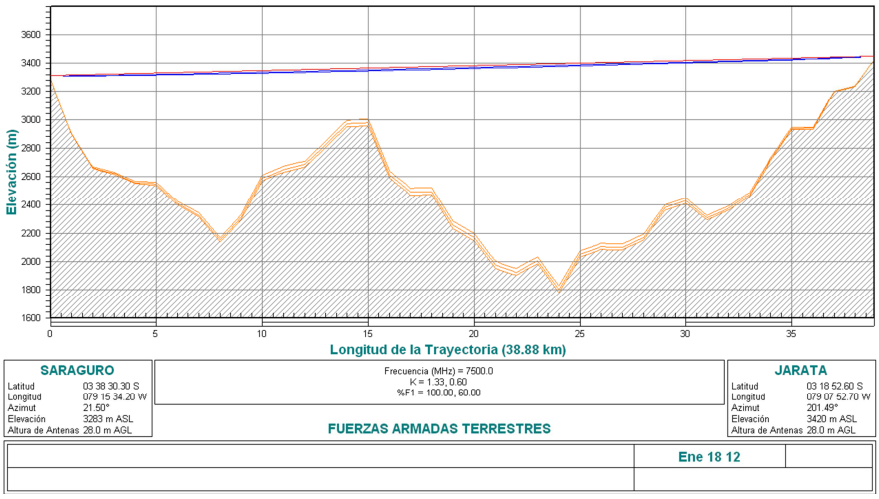

Figura 3.38. Perfil del enlace Jarata-Saraguro

3.1.2.3.20. ENLACE JARATA-PUCARA

El Nodo Pucara se encuentra ubicado en el cerro Muyo Pungo cerca del Cantón Pucara, Provincia del Azuay. Este Nodo es un repetidor que une la Ruta Redundante entre Azuay y El Oro. La distancia de este enlace es de 40.37 Km. Las antenas son parabólicas de 2.4 Km de diámetro con una ganancia de 43.5 dBi.

ESQUEMA

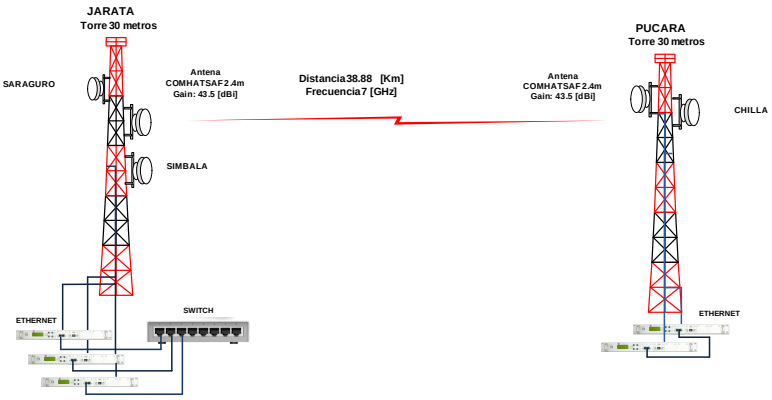

Figura 3.39. Esquema del enlace Jarata-Pucara

PERFIL

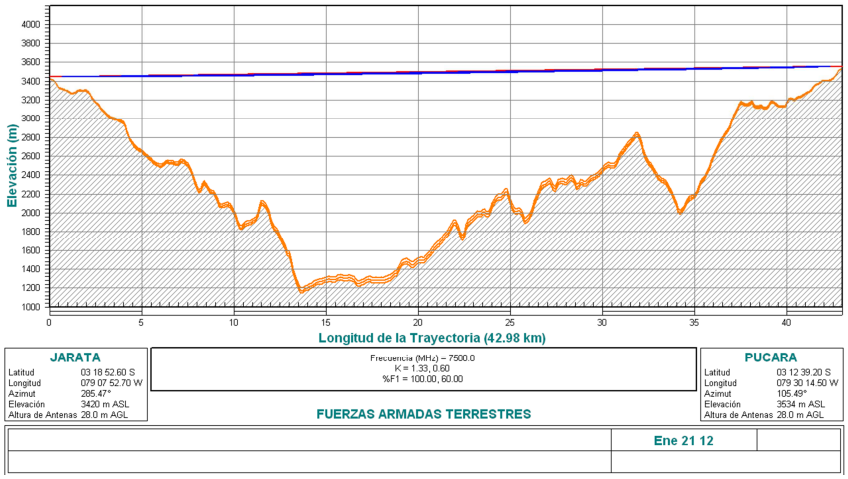

Figura 3.40. Perfil del enlace Jarata-Pucara

3.1.2.3.21. ENLACE PUCARA-CHILLA

La distancia de este enlace es de 34.93 Km. Las antenas son parabólicas de 2.4 m de diámetro con una ganancia de 43.5 dBi.

ESQUEMA

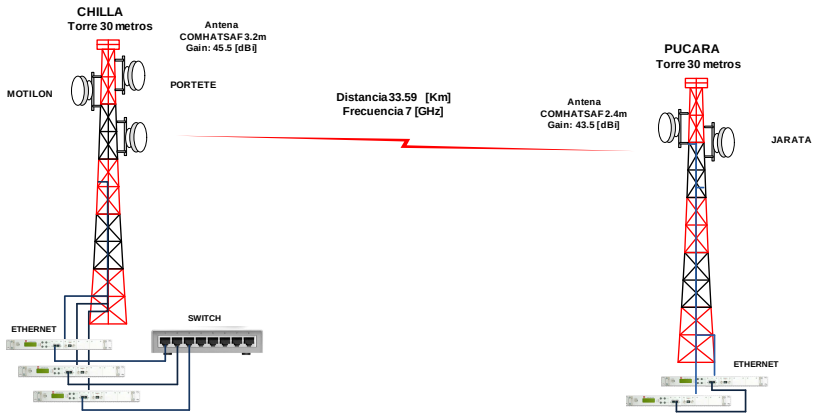

Figura 3.41. Esquema del enlace Pucara-Chilla

PERFIL

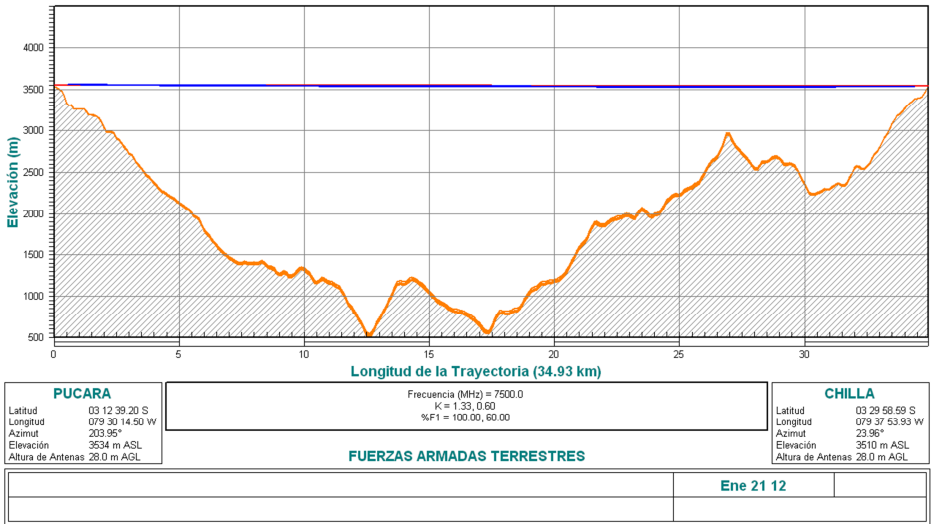

Figura 3.42. Perfil del enlace Pucara-Chilla

3.1.2.4. TECNOLOGIA Y CAPACIDAD DE TRANSPORTE DE LA RED

CFIP PhoeniX TDM / IP. [SAF TEKNICA.COM]

La Familia de Productos CFIP es la siguiente generación de la línea de productos SAF que dirige la creciente demanda de transmisión de datos sobre microondas de radio.

Como resultado, el tráfico de la interfaz principal de CFIP TDM / IP es Gigabit Ethernet, como CFIP es capaz de proporcionar una capacidad de hasta 366Mbps, es un aporte perfecto a la gama de productos de SAF. Aparte de toda la capacidad del sistema 366Mbps, es posible configurar la radio para cualquiera de los canales como 3,5, 7, 14 MHz, 28 MHz, 40 MHz y 56 MHz, así como a cualquiera de las siguientes modulaciones QPSK, 16APSK, 32APSK, 64QAM, 128QAM y 256QAM, proporcionando así capacidades diferentes para adaptarse a las necesidades particulares. SAF Tehnika ha empleado soluciones de diseño más moderno y componentes para crear sistemas de montaje con bajo consumo de energía - 25-35W por sistema.
CFIP es un elemento perfecto para cualquier red inalámbrica moderna futura, incluyendo proveedores de servicio móvil, proveedores de servicio fijo, operadores de servicio de datos, clientes empresariales, municipales y redes gubernamentales, entre otros.

3.1.2.4.1. CARACTERISTICAS DE LOS RADIOS A UTILIZAR

Características principales:
• Solución de sistema y división de montaje
• Capacidad: hasta 366Mbps
• Canales deTráfico:3.5/7/14/28/40/56MHz(dependiendo de la ODU)
• Modulaciones: QPSK, 16APSK, 32APSK, 64QAM, 128QAM, 256QAM
• Interfaces: 10/100/1000Eth
• Tráfico: solo Ethernet
• Bandas de frecuencias: 7 / 8 / 10/11 / 13/ 15 /18 / 23 / 24/ 26/ 38 GHz

• Potencia 25-35W de consumo

• ACM y ATPC con QoS, colas de cuatro prioridades

• Soporta 802.1Q VLAN

3.1.2.4.1.1. CFIP PhoeniX IDU

•1U de altura

•Dimensiones45x430x240mm, peso de 3 kg

Figura 3.43 CFIP PhoeniX IDU

3.1.2.4.1.2. CFIP PhoeniX ODU

- Unidad compacta, 285x285x80mm, 3,9 Kg, adaptación de la antena compatible con todas las unidades de las series CFM y CFQ.

- Seguro y fácil de usar

- Todos los conectores del lado de la unidad, siempre están a 45 ° con respecto del eje vertical, tanto para polarización Vertical y Horizontal.

Figura 3.44 CFIP PhoeniX ODU

3.1.2.4.1.3. CFIP PhoeniX 1+1 Hot Stand-by (HSB)

- HSB protección (1 +1) de configuración se utiliza con una sola antena y un acoplador.
- La configuración 1 +1 protege el módem y radio por fallas que puedan suceder.
- Conmutación sin errores (Tx conmutación < 50 ms)

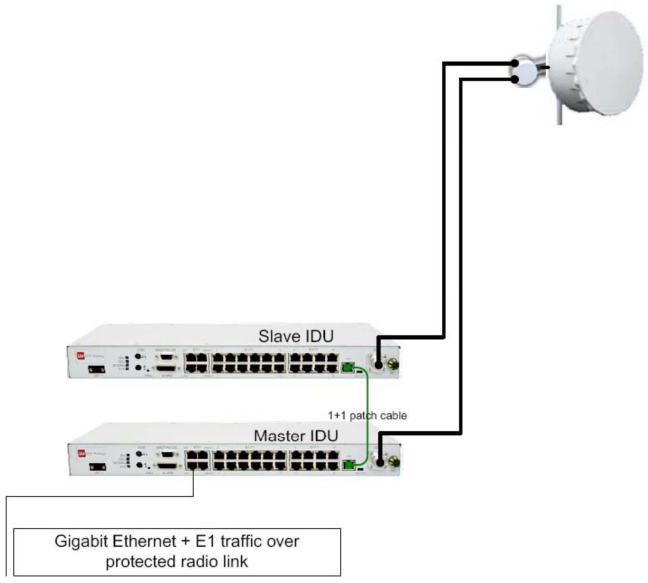

Figura 3.45 Configuración del SAF CFIP PhoeniX (1+1) HSB

Los radios SAF nos brindan una gran variedad de par de frecuencias en la banda de 7 GHz, que pueden ser usados para la transmisión y recepción del enlace. En esta banda y usando estos radios tenemos una separación del dúplex de frecuencias de 154 MHz, y el ancho de banda para cada frecuencia es de 28MHz, la información sobre el dúplex de frecuencias utilizables, se resume en la tabla 3.5:

	Channel no.	Type High		Type Low	
		Tx Freq. (MHz)	Rx Freq. (MHz)	Tx Freq. (MHz)	Rx Freq. (MHz)
Band A	1	7296	7142	7142	7296
	2	7324	7170	7170	7324
Band B	3	7352	7198	7198	7352

	4	7380	7226	7226	7380
Band C	5	7380	7226	7226	7380
	6	7408	7254	7254	7408

Tabla 3.5. Rango de Frecuencias especificadas por la ODU

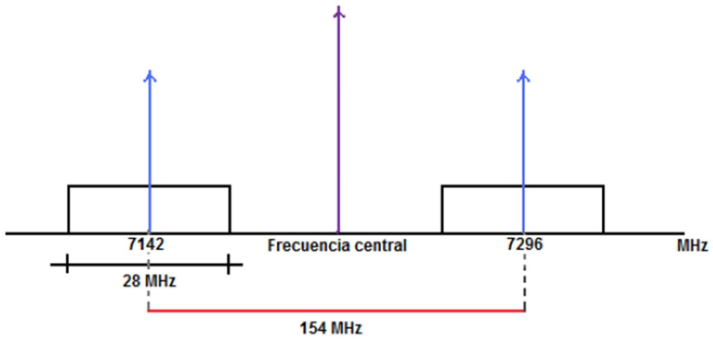

Figura 3.46 Grafico de frecuencias de transmisión y recepción del equipo

3.1.2.4.1.4 Interfaces/ Administración

- La unidad CFIP PhoeniX IDU ofrece Ethernet, E1, energía, EOW, alarma, serial, 1+1, conectores ODU y un tornillo de puesta a tierra.

- 4 Puertos Gigabit Ethernet para usuarios y la administración de tráfico.

- El trafico Ethernet soporta QoS y 4 colas de prioridad, esencial para el uso de ACM.

- El trafico de usuario y NMS puede ser tratado como un único flujo de datos o separados por etiquetado, usando diferentes etiquetas para VLANs.
- El conector RS-232, para el acceso terminal.

- Conector RJ-45 1+1 permite interconectar dos CFIP PhoeniX CDI para la configuración de 1+1.

- Web, Telnet y SNMP están disponibles como interfaces NMS en la unidad.

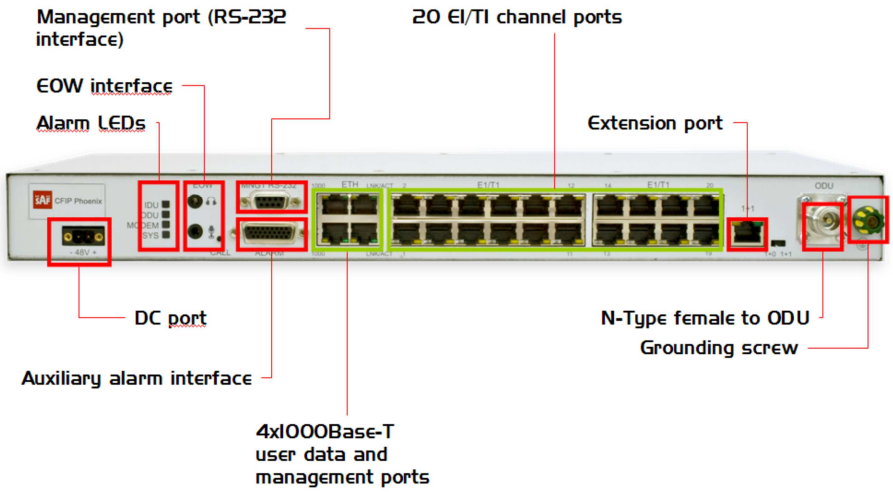

Figura 3.47. CFIP Phoenix IDU connectors

3.1.2.4.1.5. CFIP PhoeniX ODU Parámetros

•CFIP PhoeniX proporciona excelentes parámetros de radio (Ganancia del Sistema), debido al uso de APSK y modulaciones QAM y eficiente a la vez que consumen poca energía Tx /Rx en el sistema.

•Umbral de RSL en BER 10-6, 56MHz, 256 QAM, 366Mbps: -62 dBm.

• La ganancia del sistema esta garantizada con una potencia máxima Tx/Rx, y la sensibilidad es de 74 dB.
•CFIP proporcionan la capacidad para reemplazar un radio típico de 34Mbps PDH al sistema de366Mbpsconservando el tamaño de la antena/ distancia.
•ACM (Adaptive Codingy modulación), ACM abre montón de nuevas posibilidades dependiendo de la estrategia de red de los diseñadores.

•ATPC (Automatic Transmitter Power Control), para incrementar el despliegue de la capacidad.

•Muy alta flexibilidad permite configurar el sistema para diferentes anchos de banda, esquemas de modulación y configuraciones de capacidad.

3.1.2.4.2. ANTENAS-CARACTERISTICAS [4]

Se ha considerado para el diseño las antenas parabólicas COMHAT, las cuales están disponibles con un diámetro de 30, 60, 90, 120, 180, 240 y 320 cm, y son utilizadas con todas las frecuencias comerciales.

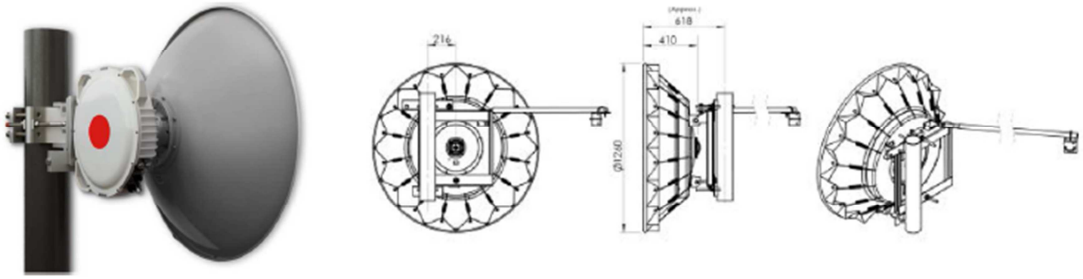

Figura 3.48 Antena COMHAT

Las antenas y los montajes se hacen en un diseño fácil de usar y adaptar en condiciones severas. COMHAT proporciona antenas para la instalación independiente, así como aplicaciones personalizadas integradas para radioenlaces. Se anexa el datasheet de las antenas.

3.1.3. ASPECTOS A CONSIDERARSE EN EL DISEÑO

Para empezar el planteamiento, es indispensable considerar aspectos como:

[4] http://www.ultratelecom.kiev.ua/catalog/%287GHz,1.2m%2920041227154950251901-HAA0712_00-PA3.pdf

3.1.3.1 SERVICIOS A PRESTARSE

La red a diseñarse, esta dimensionada para soportar varios servicios como: VoIP, Video Conferencia, Video Vigilancia IP, la integración del Servicio Troncalizado actual, así mismo el envío de datos como emails, archivos u otros adicionales que se necesiten y que se quieran implementar.

3.1.3.1.1. Video Conferencia [5]

Es una tecnologia que falicita la comunicación de manera bidireccional, de video, audio y datos, de esta manera los participantes en dicha comunicación tendran una comunicación simulatanea en *real time,* es decir; podremos comunicarnos con cualesquier parte del mundo sin la necesidad de trasladarnos, gracias a los equipos que permiten realizar una conexión.

La señal antes de ser transmitida, debe pasar por diferentes procesos de tratamiento (uso de codecs), y una vez digitalizada, esta se debera transmitir por los medios mas convenientes, ya sea via terrestre o satelital.

La video conferencia nos brinda mucho beneficios y aplicaciones como: educación a distancia, investigación, vinculación, y todo en cuanto se refiera a reuniones, congresos, cursos, conferencias, etc.

3.1.3.1.1.1. CONSIDERACIÓNES IMPORTANTES DE LA TECNOLOGIA [6]

Las comunicaciones de video presentan un adicional de ancho de banda debido a los encabezados aproximado de un 20% en Ethernet/MPLS. Si el tráfico de video está

[5] http://www.videoconferencia.es/polycom.html

compartiendo red de transporte con datos, se pueden aplicar políticas de calidad de servicio para mejorar la experiencia en las sesiones. Esta configuración se realiza en los equipos terminales y el multipunto.

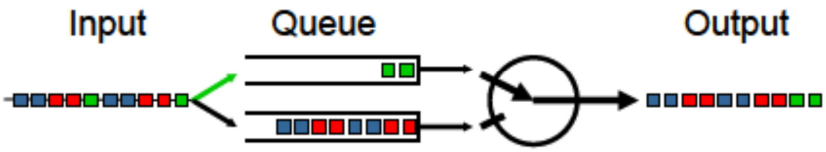

Figura 3.49 Encabezado adicional en Ethernet/MPLS.

Así mismo, utilizando el sistema de Administración, Control y Monitoreo, Polycom CMA, se puede restringir el uso del ancho de banda por equipo, por sitio o por enlace de sitio. Los sistemas Polycom tienen algoritmo predictivo llamado Lost Packet Recovery el cual permite recuperar la imagen que se pierde cuando existe una pérdida de paquetes igual o menor al 5%.

Por último, existen parámetros en una red de transporte determinantes de la calidad de las comunicaciones en tiempo real, adicionales al ancho de banda como son: la pérdida de paquetes, el round trip delay, latencia y Jitter. La tabla 3.6 presenta los valores límite para tener un buen desempeño en el servicio de video:

Parámetros	**Valor**
Packet Loss	< 0.1%
Packet Latency	<= 100 ms
Packet Jitter	< 40 ms

Tabla 3.6. Parámetros y valores Packet(loss, latency, jitter).

3.1.3.1.1.2. COMPRESION DE VIDEO (H.264 HIGH PROFILE)

Polycom posee soporte a la nueva tecnología avanzada de compresión de video basada en estándares H.264 High Profile, que reduce los requisitos de ancho de banda para telepresencia de alta definición (HD) y video conferencia de definición estándar (SD) hasta en un 50 por ciento, lo cual representa considerables ahorros de coste de ancho de banda para los clientes.

El soporte de Polycom para H.264 High Profile proporciona un despliegue avanzado de video en cualquier ancho de banda, incluyendo calidad de video HD de movimiento completo desde sólo 512 Kbps y video de movimiento completo con calidad de DVD desde sólo 128 Kbps.

3.1.3.1.1.3. CARACTERISTICAS DE LOS EQUIPOS

MULTIPUNTO RMX 1500

La plataforma de conferencias de medios en tiempo real RMX 1500 entrega conferencia de video y audio de alto desempeño a PYMES, grandes empresas u organizaciones que exija lo máximo en facilidad, calidad y confiabilidad de sus comunicaciones.

Figura 3.50. Multipunto RMX 1500

El RMX 1500 permite que las organizaciones aprovechen sus inversiones en conferencias, actuales y futuras. Al optimizar sus recursos, sin importar el tipo de llamada, la plataforma de conferencias RMX 1500 siempre opera en máxima eficiencia

en todos los ambientes. El RMX 1500 también facilita un desempeño superior e integración de servicios de conferencia IP (H.323 y SIP), PSTN y ISDN.

Fácil de configurar, fácil de usar y una poderosa herramienta de colaboración, la plataforma de conferencias de medios en tiempo real RMX 1500, ofrece conferencias multipunto, intuitivas, de alta calidad, a los usuarios finales, así como una flexibilidad y control sin paralelo a los administradores. Sus sencillas interfaces de usuario y de administrador dan lugar a experiencias de comunicación en persona consistentes, sin los obstáculos de tecnología complicada, lo que incrementa la productividad y acelera la velocidad de la adopción de las conferencias.

Soporte para conferencias en demanda y AdHoc, Personalización de las salas de conferencias, layouts, colores, duración de sesiones, Calendarización, Encripción de llamadas y transcoding así como LPR integrado.

POLYCOM QDX 6000™

Figura 3.51. Polycom QDX 6000

Para organizaciones que buscan incrementar significativamente la productividad y la calidad de la comunicación, el sistema de video conferencia de alta resolución Polycom QDX 6000 combina un desempeño sin precedente en anchos de banda bajos con una configuración sencilla y facilidad de uso.

QDX 6000 permite a las organizaciones implementar video conferencia sin recursos dedicados de TI y con un mínimo impacto en la red. Al ofrecer experiencias de junta más realistas y poderosas capacidades para compartir contenidos, QDX 6000 provee una óptima relación precio - desempeño en aplicaciones de video que no son de alta definición (HD).

Video conferencia de alta resolución, fácil de instalar y usar. Al aprovechar un potente códec, cámara con calidad de estudio, audio con calidad de CD y múltiples entradas y salidas de video, el QDX 6000 es compatible con todos los sistemas estándar de video conferencia, multipuntos, productos para firewall y mas.

Con encriptación AES de alta seguridad para comunicaciones en video y audio e interfaces intuitivas, los usuarios pueden llamar a otros con seguridad y entrar en una video conferencia en segundos. Contenidos y otros medios se comparten mediante una sencilla interface point-and-click, mientras la tecnología Polycom Lost Packet Recovery™, provee experiencias de conferencia suaves y sin interrupciones, incluso en redes congestionadas.

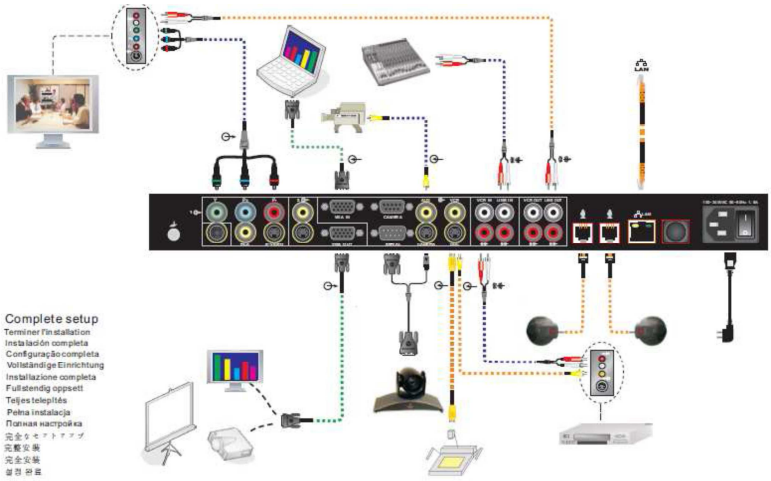

Figura 3.52. Cobertura del QDX 6000

3.1.3.1.2. VideoVigilancia IP [7]

Videovigilancia IP es una tecnología de vigilancia visual que combina los beneficios analógicos de los tradicionales CCTV (*Circuito Cerrado de Televisión*) con las ventajas digitales de las redes de comunicación **IP** permitiendo la supervisión local y/o remota de imágenes y audio. Su despliegue resulta sencillo, puesto que aprovecha la red informática empresarial, es decir, el mismo cableado que se emplea para la comunicación de datos, acceso a Internet o correo electrónico. Entre los avances que se tienen están la alta resolución de imagen que ofrecen las cámaras megapixel (1,x megapíxeles…), la inclusión de sistemas de inteligencia para el tratamiento de video, etc. A la mejora de la resolución le acompañan elevadas tasas de compresión para evitar altos consumos de ancho de banda y espacio de almacenamiento, con estándares como H.264, que simplifican significativamente el almacenamiento en los NVR (*Network Video Recorders*) o servidores de vídeo respecto a otros formatos como vídeo Motion JPEG, MPEG-4.

3.1.3.1.2.1. Consideración para el servicio de Video Vigilancia IP

Para diseñar un sistema de video vigilancia, es necesario determinar el tipo de cámaras a utilizar (cámaras IP), la ubicación general, que en este caso sería en las bodegas de los destacamentos… y la disposición física interna dentro de cada uno de estas para obtener una mayor cobertura del área. Hay que señalar que cada destacamento tiene 3 bodegas y es requerimiento cubrir estas zonas con el monitoreo constante de cámaras de seguridad.

Entre los tipos de cámaras que nos pueden brindar una solución para el requerimiento podríamos tener fijas y móviles, con visión nocturna, que tenga la aplicación para transmitir voz, y sensores de movimiento. Para el caso puntual de la tesis referente a este servicio, el requerimiento es monitorear las bodegas de cada uno de los destacamentos, para lo cual se utilizarían cámaras fijas con monitoreo nocturno, transmisión de voz y resolución HD, esta consideración se toma en base seguridad que representa este

[7] http://es.wikipedia.org/wiki/V%C3%ADdeovigilancia_IP

servicio y al consumo de ancho de banda. Para el monitoreo de todas estas cámaras de deberá disponer de un software libre administrador.

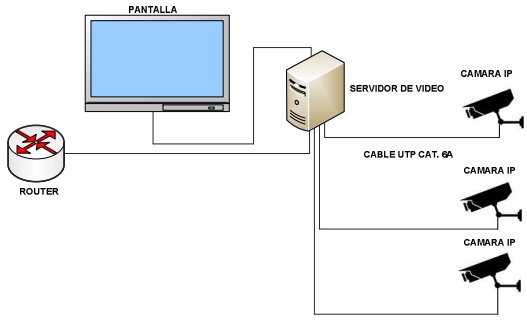

Figura 3.53. Esquema de cámaras IP

En la figura 3.53 se muestra el diagrama, con el que funcionara el sistema de video vigilancia. De preferencia para el cableado se considera el cable UTP cat. 6 ya que es un estándar para Gigabit Ethernet, y también es compatible con versiones anteriores, y otros protocolos de red. Además de las cámaras utilizadas con conexión por cable UTP, también existe la posibilidad de usar cámaras inalámbricas, la cual nos facilita trabajos de montaje. Esta posibilidad no se contempla en el estudio de la tesis, se deja libre esta consideración; sin embargo el dimensionamiento y cálculo de ancho de banda se considera con cámaras IP fijas, con visión nocturna, transmisión de voz y resolución HD.

3.1.3.1.2.2. Numero de Bodegas por Destacamento

DESTACAMENTOS	NUMEROS DE BODEGAS
III ZONA MILITAR	3
CALDERON	3
DAVALOS	3
PATUCA	3
MACHALA	3
SANTA ROSA	3
PASAJE	3

ARENILLAS	3
LOJA	3
MACARA	3

Tabla 3.7 Numero de Bodegas por Destacamento

3.1.3.1.2.3. Hardware y Software para la Gestión de Video

Los requisitos mínimos que deberá cumplir una estación remota de video vigilancia será:

Requerimiento	Servidor de Video	Estación Remota
Sistema Operativo	Windows	Windows XP SP2
Resolución de Pantalla	1280-1024 pixeles	128-1024 pixeles
Definición de Color Procesador	32 bits Intel Core 2 duo	32 bits Intel Core 2 duo
Velocidad	2.6 GHz o superior	1.6 GHz o superior
Memoria RAM	2 GB o superior	2 GB o superior
Disco Duro	250 GB	250 GB
NIC (Network Interface Card)	10/100 Mbps	10/100 Mbps
DVD	Lector, quemador de DVDs de hasta 18X de velocidad	Lector, quemador de DVDs de hasta 18X de velocidad

Tabla 3.8 Características del servidor de Video

Hay que tener presente que el video grabado por las cámaras se deberá de guardar en un disco duro principal en este caso en el administrador. El cual podrá especificar qué tiempo deberá guardarse esta información, ya que luego de ese tiempo se podrá descartarla.

3.1.3.1.2.4. Funcionamiento de las Cámaras IP [8]

Las cámaras IP tienen su conexión a una red LAN de una instalación de internet u oficina, se le adiciona una dirección IP interna a través de un Router. Estas cámaras envían información a través de un servicio de banda ancha, es posible acceder a la cámara y observar la misma, ingresando a una web del sistema y colocando la dirección de la cámara que se desea visualizar. Una vez que se ha accedido a la cámara y dependiendo de las características de esta será posible tomar fotografías, grabar videos, sonidos y todo lo que esté al alcance en cuanto a monitoreo y características de las cámaras.

Una cámara de alta tecnológica puede enviar de manera simultánea imágenes a 10 clientes, en caso de que las imágenes se hayan enviado a un servidor web externo al lugar de los clientes directamente, se podría manejar un número ilimitado de usuarios.

3.1.3.1.2.5. Acceso a una Cámara IP

Para tener acceso a las cámaras se realiza a través de un software administrador, o vía web browser, a través software administrador es posible establecer niveles de seguridad sobre los accesos como:

Administrador: Para poder configurar el sistema, a este usuario se debe proteger mediante una contraseña ya que a través de este usuario se puede configurar todo el sistema.

Usuario: se pide una contraseña, para poder ver las imágenes, manejar las cámaras, etc.

Demo: no pide ninguna tipo de identificación y es de acceso libre.

[8] bibdigital.epn.edu.ec/bitstream/15000/2162/1/CD-2919.pdf

3.1.3.1.2.6. Administración del Video

La administración en video vigilancia trata sobre la visualización, grabación, reproducción y almacenamiento, por lo que es muy importante. Mediante una interfaz web incorporada de las cámaras de red y codificadores de video, es posible realizar la visualización y grabación de una forma básica de una o pocas cámaras.

En caso de que el sistema conste de varias cámaras, es necesario utilizar un sistema de gestión de red, el cual dependerá también del sistemas operativo a usar (Windows, Linux, etc.), existen aspectos a considerar en el momento de elección de plataforma de hardware ya sea como: Una PC basada en servidor, o Uno basado en una grabadora de video en red.

Y en cuanto al software, como características del sistema (instalación y configuración), gestión de eventos, video inteligente, administración, seguridad, etc.

Plataforma de Hardware

Existen dos tipos de plataformas: de servidor de PC, y NVR.

Plataforma de Servidor de PC

Esta plataforma incluye servidores de PC, equipos de almacenamiento, ya que dependiendo si se desea un rendimiento superior, se puede escoger estos equipos. Al tratarse de plataformas abiertas, existen las posibilidades de incrementar firewall, protección contra virus, software de gestión de video, y algoritmos de video inteligentes. Esta plataforma se amplia, o actualiza para nuevas necesidades, y al ser un plataforma abierta, es posible la integración con sistemas de control de acceso de una forma más sencilla, así el usuario podrá gestionar video y controles, a través de una interfaz de usuario y un programa.

Plataforma NVR

Se trata de un grabador de video en red, el cual es un hardware con funcionalidades que ya se encuentran instaladas, NVR esta patentado y diseñado específicamente para gestión de video, se encarga de grabar, analizar, y reproducir el video en red, no permite que otras aplicaciones estén conectadas a este.

NVR, puede trabajar con SO Windows, Linux, o un patentado, y está diseñado para ofrecer un rendimiento óptimo para un conjunto de cámaras, normalmente es menos escalable que un sistema basado en PC, por lo que es más conveniente en sistemas con números de cámaras que estén dentro del límite del diseño del NVR.

3.1.3.1.2.7. Grabación de Video

La grabación de video se puede realizar de forma manual, de forma continua, y por activación ya sea por movimiento, o por programación, para que se ejecuten en determinadas horas de día. Una vez que se ha seleccionado el modo de grabación, se selecciona el formato para las diferentes calidades de la imagen, ya que dependerá mucho de esto el ancho de banda a utilizar, y el espacio de almacenamiento necesario.

Compresión de Video H.264 O Mpeg-4 Part 10/Avc

Es el estándar MPEG más actual para la codificación de video, puesto que no compromete la calidad de la imagen, y reduce el tamaño de un archivo de video digital más de un 80% comparando con el formato Motion JPEG, y hasta un 50% en comparación con el estándar con el estándar MPEG-4. De esta manera reduce el espacio de almacenamiento y el ancho de banda a utilizar.

Se espera que H.264 acelere la adopción de cámaras megapíxel, ya que estas resultan más eficientes en cuanto a compresión, para reducir el tamaño de los archivos, sín que la imagen se vea afectada.

Frecuencia de Bits Variable y Constante

En H.264 es posible determinar si la frecuencia de bits puede ser variable o contaste: VBR (variable bit rate), se puede mantener un perfil definido de calidad de imagen, independiente de la cantidad de movimiento en la zona, al existir mayor cantidad de movimiento el ancho de banda requerido será mayor. Ideal para aplicaciones de video vigilancia de alta calidad; CBR (Constant bit rate), aquí en cambio el usuario se define una frecuencia de bits, en caso de que exista mayor cantidad de movimiento en la zona vigilada, y la frecuencia supere a la frecuencia en bits establecida por el usuario, la calidad de la imagen será inferior.

3.1.3.1.2.8. Protocolos de Transporte de Datos de Video en la Red

Entre los protocolos de control de transmisión TCP y el protocolo de datagramas de usuario UDP, estos se basan en IP, para enviar datos, y actúan como portadores para muchos otros protocolos como http (Hyper Text Transfer Protocol), a continuación vemos algunos de los protocolos y su uso.

TCP (Transmission control protocol) provee de un canal de trasmisión fiable basado en la conexión, garantiza que los datos enviados se reciban en el otro extremo, se encarga de negociar un proceso, para que grandes bloques de datos se dividan en paquetes más pequeños. Puede existir retrasos significativos, ya que utiliza retransmisión, pero esto se usa cuando la fiabilidad de la comunicación predomina sobre la latencia del transporte.

UDP (User datagram protocol) es un protocolo sin conexión, y no garantiza la entrega de datos a su destino, es la aplicación la que se deberá encargar de los mecanismos de control y comprobación de errores, no tiene retardos de transmisión, ya que no retransmite datos perdidos.

FTP (Protocolo de transferencia de ficheros) usa TCP puerto 21, para transferir archivos a través de internet/intranets, transferencia de imágenes o video, desde un codificador de video/cámara de red a un servidor FTP o a un aplicación respectiva.

SMTP (Protocolo simple de transferencia de correo) usa TCP puerto 25, para el envío de mensajes de correo electrónico, en cuanto a video en red, un codificador de video/cámara de red puede enviar imágenes o notificaciones de alarma usando su cliente de correo electrónico integrado.

HTTP (Protocolo de transferencia de hipertexto) usa TCP puerto 80, normalmente se usa para navegar por la red, en cuanto a video en red, es el más común para transferir video de un codificador de video/cámara de red, aquí el dispositivo de video en red, funciona básicamente como un servidor web, poniendo el video a disposición del usuario o del servidor de aplicaciones que lo soliciten.

HTTPS (Protocolo de transferencia de hipertexto sobre capa de sockets seguros) Usa TCP puerto 443, brinda seguridad en el acceso a páginas web con tecnología de cifrado, para la transmisión segura de video procedente de codificadores de video/cámara de red.

RTP (Real Time Protocol) usa protocolos UDP/TCP, usa el formato de paquete estandarizado para la entrega de audio y video a través de internet, comúnmente se utiliza en video conferencia y transmisión multimedia. Un modo habitual de transmitir video en red basado en H.264/MPEG y de sincronizar audio y video, los paquetes se vuelven a unir en el orden correcto, ya que la numeración y datación de paquetes se la realiza en forma secuencial, se usar unidifusión o multidifusión para la transmisión.

RSTP (Protocolo de transmisión en tiempo real) usa protocolos TCP puerto 554, se usa para configurar y controlar sesiones multimedia a través de RTP.

Frames por segundo (FPS) es el número de fotogramas por segundo que envía el sistema, para ver video en internet, el mínimo es de 15FPS por cada cámara. En un sistema de monitoreo, se tiene un determinado número de FPS, este se divide entre las cámaras instaladas.

Si un sistema dispone de 30FPS, al tener dos cámaras, cada una tendrá 15FPS, al tener tres cámaras, cada una tendrá 10FPS, etc. Esto quiere decir que mientras más cámaras activas, menor el FPS, menor velocidad de visualización, el video se vería pausado y lento.

3.1.3.1.2.9. REQUISITOS DE ANCHO DE BANDA

Un conjunto de video vigilancia que conste de 8 a 10 cámaras se le considera pequeño, por lo que se puede usar un Switch básico de 100Megabits, sin muchas limitaciones del ancho de banda, las consideraciones a tomar en cuenta para que la red no se sobrecargue serán estas reglas generales:

Las cámaras que ofrecen alta calidad en sus imágenes pueden utilizar de 2 a 3 MHz de ancho de banda. Ya en sistemas más grandes se tomaría en cuenta el uso de Switch con redes troncales de mayor capacidad.

Calculo MPEG-4

Velocidad binaria aprox /8(bits en un bite)x3600s igual a KB por hora/1000 =MB/hora: MB x hora, y x horas de funcionamiento al día/1000 =GB/día

Es importante reconocer que dependiendo de la cantidad de movimiento, puede influir en el tamaño de almacenamiento.

Cámara	Resolución	Velocidad binaria aprox. (Kbps)	Imágenes por segundo	MB/hora	Horas de funcionamiento	GB/día
No. 1	CIF	170	5	76.5	8	0.6
No. 2	CIF	400	15	180	8	1.4
No. 3	4CIF	880	15	396	12	5
Capacidad total para las 3 cámaras y 30 días de almacenamiento = 204 GB						

Tabla 3.9 Almacenamiento de MPEG-4

CIF es el tamaño de la resolución.

Resoluciones NTSC y PAL.

En Norteamérica y Japón se usa comúnmente el estándar NTSC, mientras que en Europa, áfrica y países de áfrica se usa la norma PAL, estos son estándares en la industria de la televisión, NTSC tiene una resolución de 480 líneas, y utiliza una actualización de campos de 60 campos entrelazados por segundo, es decir, 30 imágenes completas por segundo. PAL en cambio actualiza 50 campos entrelazados por segundo, o 25 imágenes completas por segundo.

En la tabla 3.10 se muestra tipos de resoluciones de imágenes para cámaras IP.

RESOLUCIÓN	FORMATO DE VISUALIZACIÓN (digital)	DEFINICIÓN (pixeles)
NTSC	4 CIF	704 x 480
	2 CIF	704 x 240
	CIF	352 x 240
	QCIF	176 x 120
PAL	4 CIF	704 x 576
	2 CIF	704 x 288
	CIF	352 x 288
	QCIF	176 x 144
VGA	QVGA(SIF)	320 x 240
	VGA	640 x 480
	SVGA	800 x 600
	XVGA	1024 x 768
	4x VGA	1180 x 960
MEGAPIXEL	SXGA	1280 x 1024
	SXGA + (EXGA)	1400 x 1050
	UXGA	1600 x 1200
	WUXGA	1920 x 1200
	QXGA	2048 x 1536
	WQXGA	2560 x 1600
	QSXGA	2560 x 2048
HDTV	HDTV 720P	1280 x 720
	HDTV 1080	1920 x 1080

Tabla 3.10 Resoluciones de imágenes para camaras IP

Cámara AXIS 216MFD

Figura 3.54 Cámara AXIS 216MFD

La AXIS 216MFD es una cámara de red de gran rendimiento con resolución de megapíxeles diseñada para la video vigilancia profesional en ubicaciones tales como tiendas, colegios, bancos y edificios de la administración

La cámara de red AXIS 216MFD incorpora un sensor de 1,3 megapíxeles que ofrece imágenes claras y nítidas, lo que la hace perfecta para la identificación de objetos y personas. El objetivo de alta calidad utiliza un control de iris de tipo DC para mejorar la profundidad de campo y proteger el sensor en escenas con iluminación intensa. La resolución de megapíxeles permite supervisar con gran detalle áreas importantes como accesos o recepciones.

La cámara de red AXIS 216MFD ofrece una solución discreta, compacta y rentable con una protección eficaz contra manipulaciones indebidas. El cristal domo se fija desde el interior y la carcasa se asegura a la pared o techo mediante tornillos de montaje a prueba de manipulaciones.

La cámara de red AXIS 216MFD se instala rápida y fácilmente en la pared, techos duros o falsos techos. Permite un ajuste versátil mediante los movimientos horizontales, verticales y de giro del objetivo de óptica variable hasta obtener cualquier ángulo de cámara. Las cubiertas transparentes ahumadas y el kit de montaje en falso techo son opciones para hacer más discreta la cámara de red AXIS 216MFD.

La compatibilidad con Alimentación a través de Ethernet (PoE) permite a la cámara recibir datos y alimentación eléctrica a través de un único cable Ethernet, lo cual hace que la instalación sea más sencilla y económica. Si se conecta a un sistema de

alimentación interrumpida (SAI), puede seguir funcionando aunque se produzca un fallo eléctrico.

3.1.3.1.3 VoIP

"Voz sobre Protocolo de Internet, también llamado Voz sobre IP, VoIP (por sus siglas en inglés, Voice over IP), es un grupo de recursos que hacen posible que la señal de voz viaje a través de un sistema de comunicación empleando un protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional como las redes PSTN (Red Telefónica Pública Conmutada).

Los Protocolos que se usan para enviar las señales de voz sobre la red IP se conocen como protocolos de Voz sobre IP o protocolos IP. **El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet**, como por ejemplo las redes de área local (LAN)."[9]

3.1.3.1.3.1. CONSIDERACIONES PARA VoIP[10]

Para realizar una comunicación de VoIP, es necesario tener en cuenta los diferentes estándares, que ayudan a llevar a cabo dicha comunicación, entre los que tenemos:

Direccionamiento para el direccionamiento se utiliza RAS (registration, admission and status), este protocolo a través del gatekeeper, permite que una estación H.323 localice a otra estación H.323. Y el DNS (domain name service), que se trata de un servicio de resolución de nombres en direcciones IP, tiene el mismo propósito de RAS pero mediante un servidor DNS

Señalización en cuanto a señalización para iniciar llamadas tenemos Q.931. Para el control, señalización, registro y admisión, paquetizacion/sincronización del flujo de voz

[9] http://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet

[10] http://dspace.epn.edu.ec/bitstream/15000/8712/1/T10902ANEXOS.pdf

tenemos H.225. Y el protocolo que especifica la apertura y cierre de canal para el flujo de datos el protocolo H.245

Compresión de Voz para la compresión de voz podemos usar G.711 y G.723

CÓDEC	TASA	LT(bytes)	Tt(ms)	N	total (bytes)	BW(Kbps)
G.729	8Kbps	10	10	3	108	28,8
				6	138	18,4
G.723	6.4Kbps	24	30	1	102	27,2
				2	126	16,8
	5.3Kbps	20	30	1	98	26,13
				2	118	15,73
G.711	64Kbps	1	0,125	240	318	84,8
				480	558	74,4
G.726	32kbps	1	0,25	120	198	52,8
				240	318	42,4

Tabla 3.11. Códec para cálculo ancho de banda en VoIP [11]

3.1.3.1.3.2. Transmisión de Voz

Para la transmisión de voz podemos usar:

UDP: La transmisión se realiza sobre paquetes UDP, este no ofrece integridad en los datos, se aprovecha más el ancho de banda en TCP.

RTP: (Real Time Protocol)**:** se encarga de la temporización, marcando los paquetes UDP, contiene la información necesaria para que la entrega en recepción sea correcta.

RTCP:(Real Time Control Protocol)**:** Se usa para detectar situaciones de congestión de la red y de acuerdo a esto tomar acciones necesarias para corregirlas.

Los elementos disponibles que nos permiten construir aplicación de VoIP son:

• Teléfonos IP
• Adaptadores para PC
• Hubs Telefónicos
• Gateways (pasarelas RTC / IP)
• Gatekeeper
• Unidades de audio conferencia múltiple (MCU Voz)
• Servicios de Directorio

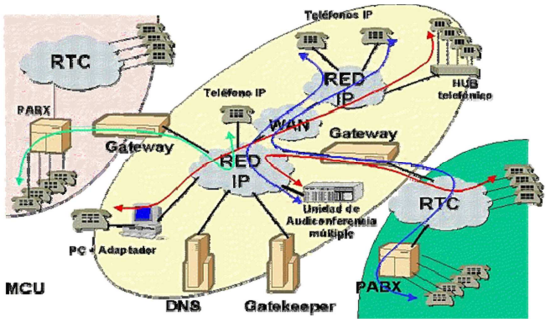

Figura 3.55. Elementos de una red VoIP [12]

En la figura anterior se observa diferentes elementos, que se pueden definir de la siguiente manera:

Gatekeeper este elemento de red que puede ser opcional, al usarse en una red, todos los elementos de la red, deben hacer uso del este, se encarga de gestionar y controlar los recursos de la red, con la finalidad de que no existan saturaciones en la red.

Gateway este elemento de red, nos ayuda a enlazar la red de VoIP con la red telefónica RDSI, este elemento consta de interfaces LAN y otras como FXO (para conexión a extensiones de centrales o RDSI), FXS (centrales o teléfonos analógicos), E&M(conexiones especificas a centrales), BRI para acceso básico RDSI(2B+D) y PRI para el acceso primario RDSI(30B+D).

Estos elementos pueden estar físicamente separados, o en su caso puede estar en una misma plataforma, así CISCO ha implementado funciones de Gateway en un Router.

Un aspecto importante que se tiene que tener en consideración, son los retardos en la transmisión, ya que estos retardos en la voz no son muy tolerantes, al tratarse de una retardo de 300 ms, la conversación ya no resulta ser fluida. Se usa el protocolo RSVP, el cual fragmenta los paquetes grandes en este caso dando prioridad a los paquetes de voz, cuando existen congestiones en el Router. RSVP ayuda al tráfico multimedia, pero no garantiza una calidad de servicio.

3.1.3.1.3.3. Protocolos de Control de VoIP

En el protocolo H.323 existen aspectos que impiden que su aplicación sea universal, tales como ausencia de una interfaz red a red, y un mecanismo de control de congestión. Existen protocolos como MGCP (control de compuertas para medios) y SIP (protocolo de Inicio de Sesión), y mejorado a estos MeGaCo, el cual se encarga del control y el señalización para las conexiones de VoIP.

3.1.3.1.3.4. EQUIPO MATRIZ [13]

Servidor Cisco Call Manager: Esta plataforma Media Convergence Server funciona bajo el sistema operativo Windows 2000 Server, sobre el cual trabaja el software de telefonía Cisco Call Manager. Es un sistema de poderosas soluciones de clase empresarial, incluyendo telefonía IP, comunicaciones unificadas, video y conferencia IP. Este dispositivo se encarga del procesamiento de llamadas, basado en software.

Dependiendo del número de usuarios, tenemos varias opciones en hardware, ya que se puede manejar (200, 1000, 2500, 7500) usuarios.

Las características principales son:

[13] http://hdl.handle.net/123456789/32

Señalización SCCO, H.323, MGCP.
Ruteo automático de llamadas (ARS).
Traducción del número de llamada a dirección IP.
Gestión de directorio.
Database.
Administración de usuario.
Integración con LDAP Directory.

Cisco Unity: Es el producto voicemail de Cisco que permite a los empleados acceder y administrar la voz, fax y correos electrónicos desde cualquier dispositivo de escritorio.

Dependiendo de la plataforma de hardware Unity puede soportar 500 usuarios por servidor. Unity Connection es orientado para medianas y grandes empresas y Unity Express para pequeñas empresas o sucursales.

Cisco 6506: El Cisco 6506 es un conmutador de altas prestaciones con las siguientes características:

48 puertos Ethernet a 10/100 Mbps.
8 puertos gigabit.
24 Gbps de conmutación "non-blocking".
Fuente de alimentación redundante.

Figura 3.56. CISCO 6506 [14]

Router Cisco 3845: Este equipo proporciona enrutamiento de alto rendimiento, seguridad, voz, telefonía IP, voicemail y video. Estos equipos son óptimos para satisfacer las necesidades de empresas en telefonía IP, voicemail, operadora automática y funciones de convergencia.

Posee puertos de switches FastEthernet y Gigabit Ethernet, VLAN, tecnología inalámbrica y PoE. Posee 2 puertos autosensing 10/100/1000 y una ranura SFP. Asegura la escalabilidad ya que soporta 24 troncales T1/E1, 88 puertos FXS o 56 puertos FXO que pueden operarse de manera simultánea con el tráfico normal de datos.

Figura 3.57. Router CISCO 3845[15]

3.1.3.1.3.5. EQUIPOS TERMINALES

Router Cisco 2800 Series: La serie Cisco 2800 brinda servicios integrados de datos, voz, video y fax dedicado para pequeñas empresas. Estos serán utilizados dentro de las sucursales existentes como Gateway. Algunas características de este Router son:

- Seguridad: cifrado incorporado, NAC, IPS en línea, túneles VPN y firewall de alto rendimiento.
- Satisfacer necesidades de telefonía IP, voicemail, operadora automática.
- PoE: Fuente de alimentación en línea para teléfonos IP.
- Integra procesamiento de llamadas: soporta 96 teléfonos IP Cisco.
- Integra Voice Mail: Soporta 250 mailboxes usando Cisco Unity Express sistema de mensaje de voz.

Posee una arquitectura escalable que permite conectar 12 T1/E1 trunks, 58puertos FXS o 36 puertos FXO. Esto nos servirá para la conexión de la línea E1al Router de cada sucursal y si son pocas líneas se utilizará los puertos FXO.

TARJETA FXO: Cisco high-density Analog and Digital Extentión Module for Voice and Fax, este módulo permite conectar el Router Cisco 2800 a la red PSTN y a equipos de telefonía existentes como por ejemplo una PBX, teléfonos analógicos a fax analógicos.

CISCO CATALYST EXPRESS 500 Series: Equipos aptos para negocios de hasta 250 usuarios. Brinda prioridad al tráfico crítico, provee de conversaciones de voz claras, tráfico de video no afecta a las aplicaciones en la red y posee red inalámbrica segura.

ADAPTADORES CISCO ATA 186: Los adaptadores ATA servirán para conectar las máquinas de fax a la infraestructura de red de telefonía IP. Soporta dos salidas FXS y un solo puerto LAN.

TELEFONO IP Linksys SPA942[16]

Figura 3.58 Linksys SPA942

El teléfono VoIP SPA942 es ideal para residencias o negocios que estén usando un servicio telefónico IP, un IP PBX o un Centrex IP con despliegue a gran escala.

Las características principales de este teléfono es que tiene dos líneas activas, puertos Ethernet de doble Switch, soporte PoE 802.3af, una pantalla gráfica de alta resolución, altavoz y un puerto para audífonos de 2.5 mm. Mediante la actualización del software se

[16] http://www.inphonex.es/productos/linksys-spa942.php

puede actualizar a un teléfono de cuatro líneas, cada línea puede ser configurada de manera independiente para usarlas como un único número(o extensión), o para un número compartido que este asignado a múltiples teléfonos.

SOFTPHONES: es un software que simula un teléfono convencional por computadora. Permitiendo realizar llamadas a otros teléfonos o a otros softphones. Normalmente, un Softphone es parte de un entorno Voz sobre IP y puede estar basado en el estándar SIP/H.323 o ser privativo.

Figura 3.59. Teléfono IP SOFTPHONE

SERIES - CENTRAL IP CP-1000: Utilizado para las estaciones

Figura 3.60. Central IP CP-1000

La central IP CP-1000 es ideal para las empresas que quieren ampliar y mejorar su sistema telefónico, y/o reducir costos de llamadas nacionales e internacionales. Este modelo es recomendado para empresas de hasta 100 extensiones.

3.1.3.1.4 SISTEMA TRONCALIZADO IP [17]

3.1.3.1.4.1. CONSIDERACIONES PARA SISTEMAS TRONCALIZADO.

Es necesario modernizar el sistema troncalizado de las Fuerzas Armadas (III Zona Militar), a una tecnología con plataforma IP, de esta manera se podría aprovechar al máximo, ya que mediante esta se tiene diferentes aplicaciones, ventajas, beneficios, de esta manera resulta escalable y flexible.

Una de las alternativas que presentan para este cambio de tecnología es un sistema APCO P25 IP, el cual tiene la capacidad de brindar voz y datos a los troncalizados, usando tecnología digital, mediante la actualización de tecnología y software, es posible aprovechar de una mejor manera los sistemas y sus repetidoras.

Normalmente se usa para seguridad pública, dependiendo del crecimiento, esta solución es escalable, ya que es modular, y nos puede brindar desde pequeñas hasta grandes capacidades, considera un ancho de banda de canal de 12,5Khz, optimizando de esta manera el uso de las frecuencias.

3.1.3.1.4.2. CARACTERÍSTICAS DEL APCO P25 (SISTEMA TRONCALIZADO)

Las características principales que ofrece este sistema son:

Eficiencia en el uso del espectro

Interoperabilidad

Estándares orientados a los usuarios

Migración futura

Funcionalidades avanzadas

[17] http://www3.espe.edu.ec:8700/bitstream/21000/2634/1/T-ESPE-029866.pdf

Se trata de un estándar digital y ofrece la opción de encriptación.

Existen 25kHz todavía que puede ser utilizada por las radios analógicas y dividido en dos 12,5 kHz canales digitales según sea necesario.

Topología

Los sistemas troncalizados, se basan en una arquitectura centralizada, donde los repetidores se deben comunicar hacia el sitio maestro, para cubrir determinada área de servicio se basa o es similar a la arquitectura celular, basada en celdas, las que dependerán de la topografía del terreno, condiciones atmosféricas, etc., es decir de factores que intervengan con la propagación de la señal.

Tráfico

P25 brinda a los usuarios la ventaja de integrar voz y datos dentro de una misma infraestructura, los canales que manejan el tráfico generado, pueden ser configurados de manera indistinta para transmitir voz, datos. También se tiene un canal dedicado en cada sitio de repetición, que es el encargado del control.

Conectividad

Desde el sitio maestro es desde donde se realiza la administración y la gestión del sistemas, además se podrá monitorear los grupos de usuarios, mensajes generales entre usuarios, establecer enlaces de comunicación entre diferentes grupos, etc.,

Frecuencias

Es posible reutilizar las frecuencias que están en uso, y en caso de requerir mayor número de sitios, se asignarán nuevos bloques de frecuencias, de manera que estos no causen problemas de intermodulación o interferencia, con el resto de equipos.

Servicios de Datos

El sistema permite a los usuarios enviar y recibir datos, mientras se movilizan dentro de la zona de servicio, y estos sean de confianza, ya que cuenta con técnicas de corrección de errores, de esta manera los mensajes dañados son fácilmente recuperables, es posible alcanzar hasta 9600bps de velocidad sobre canales de 12,5Khz. En caso de requerir capacidades adicionales es posible que se asignen hasta 3 canales de manera simultánea, para soportar la comunicación.

Diseño

Para el diseño de la red acceso del sistema troncalizado, se toma en cuenta varios parámetros necesarios para el cálculo de la capacidad de la red de acceso, se están considerando un total de 600 usuarios para este servicio.

3.1.3.1.4.3. ANÁLISIS DE LA TECNOLOGÍA DEL SISTEMA APCO P25

Descripción del Sistema

ASTRO®25es un sistema de comunicaciones de radio digital, que permite establecer comunicaciones entre amplias zonas geográficas, un usuario puede establecer una comunicación con otro usuario que se encuentre dentro de la zona de servicio del sistema.

Este sistema requiere de redes de computadoras, de LAN/WAN de altas velocidades, bases de datos, y software de administración del sistema. A continuación muestra un diagrama simplificado de un típico sistema ASTRO®25.

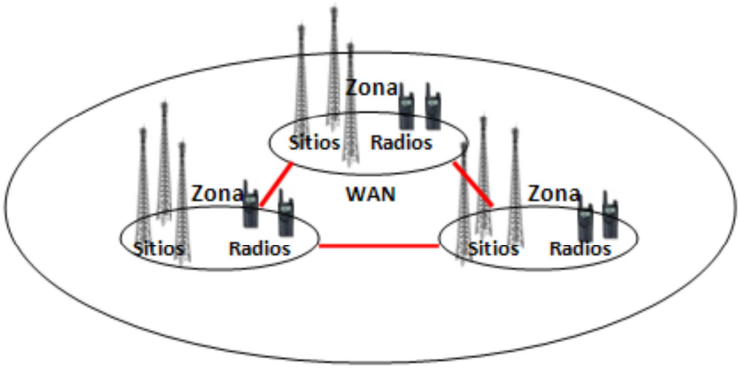

Figura. 3.61. Diagrama de zonas ASTRO®25

Un sistema ASTRO®25, tiene los siguientes bloques:

Nivel de Sistema – compuesto por múltiples zonas
Nivel de Zona – compuesto de múltiples sitios
Nivel de Sitio – sitios ASTRO®25 y equipamiento redes
Nivel de Usuario – radios portátiles y móviles

En este sistema, el procesamiento de llamadas se distribuye entre zonas del sistemas, cada una de las zonas posee una LAN(red de área local), estas LAN se interconectan para formar una red WAN de transporte de área ancha (alta velocidad), y a través de esta, que la información de procesamiento de llamadas, configuraciones, son transmitidas por el sistema. Cada una de las zonas es responsable de administrar sus propios elementos (infraestructura física, administración y procesamiento de llamadas, etc.)

3.1.3.1.4.4. Componentes del sistema ASTRO®25

Se trata de un sistema complejo, ya que está formado por componentes de hardware y software individuales, que en conjunto forman todo la red, los componentes que conforman el sistema están distribuidos de la siguiente manera, equipamiento nivel de

sistema, equipamiento nivel de zona, equipamiento nivel de sitio, equipamiento a nivel de usuario.

Sitio Maestro

Es en donde se encuentra el núcleo de procesamiento computacional de cada una de las zonas, este consta de un controlador, base de datos, terminales de administración, un switch WAN, un switch LAN, routers y otros elementos. Uno de los sitios maestros, es designado como el sitio maestro del sistema, adicional a los servidores de zona, este sitio posee los servidores de sistema: UCS(servidor de configuración de usuarios) y SSS(servidor estadístico del sistema), y estos se utilizan uno por cada sistema, en la figura 3.62, se muestra un diagrama de un sitio maestro.

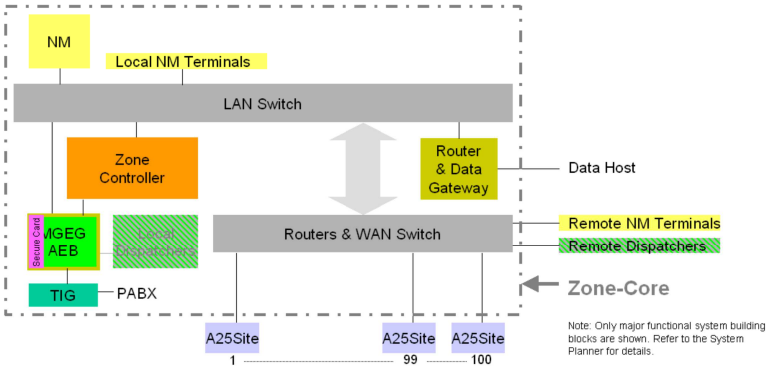

Figura. 3.62. Diagrama Sitio maestro

Sitios de Repetición

Los sitios de repetición se basan en la tecnología Quantar, un sistema de antenas, un LAN Switch, un Router, y un controlador de sitio redundante (a través de estos es posible dar soporte de tráfico, control y administración de voz, datos en la red).

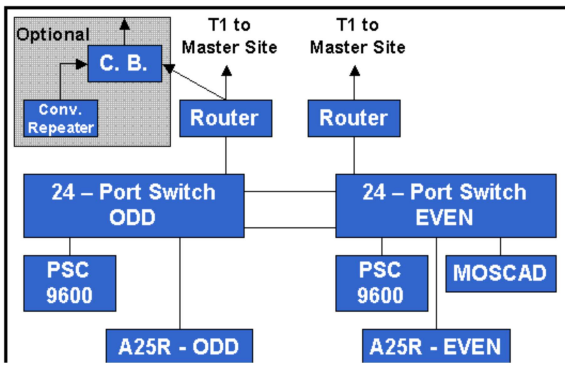

Figura. 3.63. Diagrama Sitios de Repetición

La visión de estos sistemas (ASTRO®25), es tener la capacidad de poder integrarse con otros subsistemas, que conformen un avanzado sistemas de comunicaciones, integrando voz y datos, de distintos anchos de banda e independientes de la plataforma RF que se utilice. La plataforma ASTRO25, nombre comercial de Motorola para el protocolo APCO25.

Se instala un controlador de sitios redundante (APCO25), en los sitios de repetición, también un Switch/Router para la comunicación con el sitio maestro. Los repetidores existentes QUANTAR de la plataforma SmartZone pueden ser fácilmente transformados para operar en la plataforma ASTRO®25, ya que las nuevas repetidoras pertenecen a la familia GTR-8000.

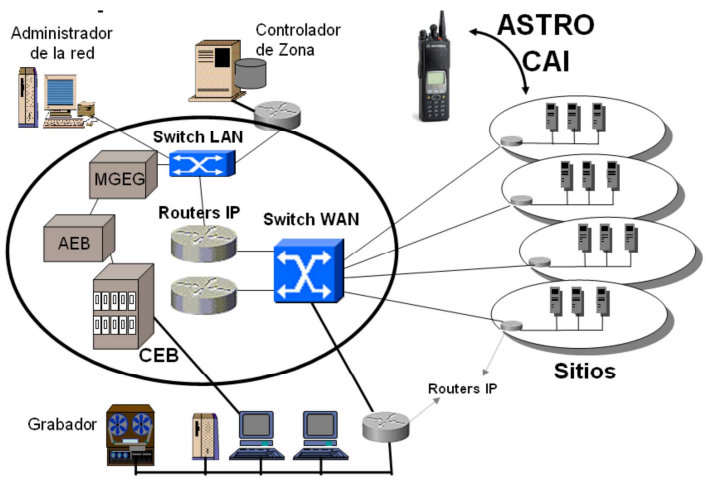

Figura. 3.64. Arquitectura ASTRO 25

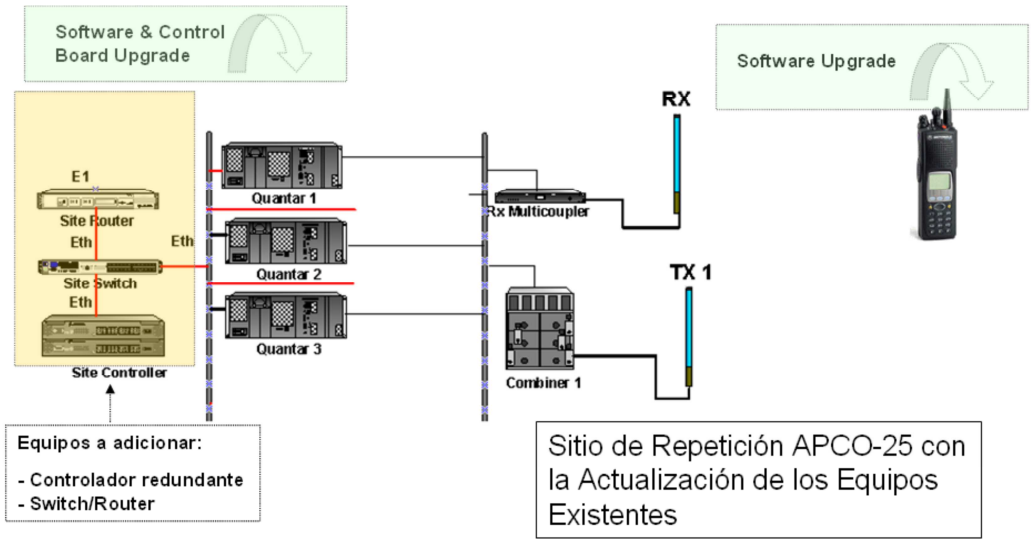

Figura. 3.65. Actualización de Sitios de Repetición Existentes

3.1.3.1.4.5. VENTAJAS DE APCO P25

Entra las ventajas que brinda este sistema, tenemos: Interoperabilidad, estándar orientado a los usuarios, posibles migraciones futuras, uso eficiente del espectro, compatibilidad, la integración de voz y datos.

Para proteger la comunicación digital, se cuenta con la capacidad de Encripción (opcional), también la opción de reintroducción (OTRA over the air re-keying) de datos digitales sobre la red de radio, permitiendo cambiar la llaves de encripcion de manera remota por el encargado de los sistemas de radio.

3.2 DESARROLLO DEL DISEÑO TÉCNICO

Para cumplir con el objetivo del establecimiento de la Red MPLS el diseño técnico se basará en los siguientes puntos específicos:

3.2.1 UBICACIÓN GEOGRÁFICA

La Red está diseñada sobre el sistema de las Fuerzas Armadas Terrestres del Ecuador Región Sur. Están bien definidas las zonas en donde se encuentran los destacamentos Militares en cada Provincia (Azuay, Loja, El Oro, Morona Santiago), cada uno tiene su identificación según los códigos que se manejan internamente y con los cuales constan y se pueden ubicar en la red. Debido a que MPLS presenta muy buenas características referentes a la escalabilidad, es una arquitectura que no tendrá mayores problemas al momento de afrontar el crecimiento interno y externo de los destacamentos de la red.

La figura 3.66 nos presenta un modelo de conexión entre cada uno de los nodos de la red, este esquema se ilustra para el análisis de manera conveniente y cómoda, ya que las rutas establecidas por las ubicaciones geográficas reales de los Nodos se cruzan en el espacio y harían dificultoso el análisis de la topología de Red.

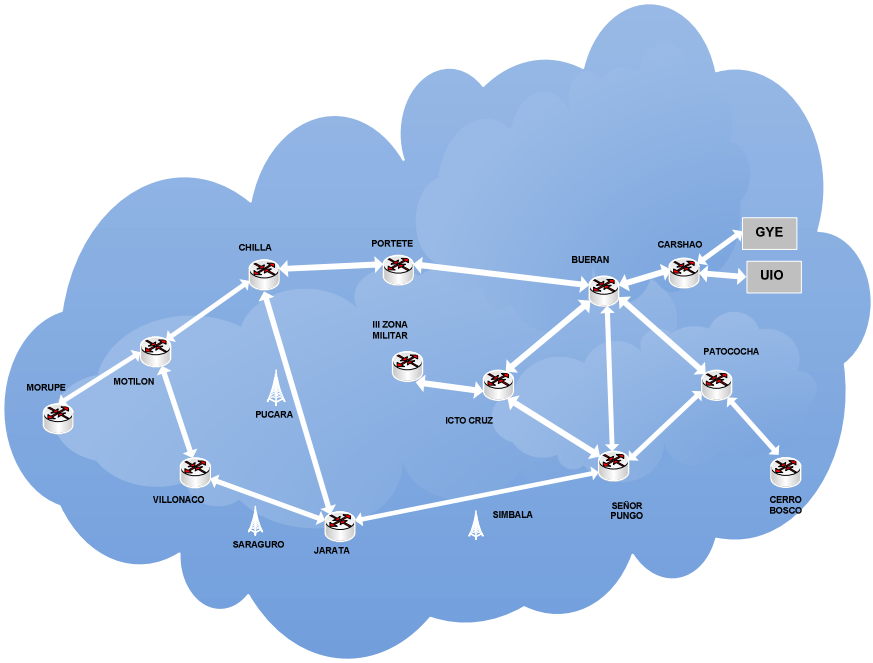

Figura 3.66. Red Militar Terrestre

3.2.2. ESTUDIO Y ANÁLISIS DE TRÁFICO

Para el análisis del tráfico, vamos a tomar en consideración, el ancho de banda que cada uno de los servicios requiere para su correcto desempeño, de esta manera, vamos a realizar cálculos que nos indiquen los valores de ancho de banda que necesitamos para cada servicio en nuestra red, ya que como servicios tenemos: video vigilancia IP, VoIP, videoconferencia, y sistema de radio troncalizados IP.

3.2.2.1. VIDEO VIGILANCIA

Calculo de Ancho de banda y espacio de disco.

La fórmula para calcular el consumo de ancho de banda es:

$$AB = Tamaño\_de\_la\_imagen * cuadros\_por\_segundo * Canales$$

Por ejemplo, una cámara H.264 en tiempo real (10fps) a compresión normal y tamaño normal consume tanto como:

$$AB = 8Kb * 25cps * 1 = 160Kbps$$

Cuanto espacio en disco duro ocupa una grabación.

Primero tenemos que calcular el ancho de banda como lo indicamos en la ecuación de anterior. Esto nos daría los Bytes (o Kbytes) por segundo. Ahora debemos multiplicar este valor por la cantidad de segundos que queremos almacenar, más un margen de 10% de sobrecarga debido al sistema de archivos. Por ejemplo una jornada de 8hs de grabación continúa necesitaría (si usamos el ancho de banda calculado anteriormente):

$$Tamaño\_disco\_duro = 160Kbps * 60seg * 60\,\min * 8H$$
$$Tamaño\_disco\_duro = 7756800Kbytes$$
$$Tamaño\_disco\_duro = 7756,8Mbytes$$
$$Tamaño\_disco\_duro = 7,76Gbytes * 1,10 = 8,5Gbytes$$

Es de mucha importancia de determinar cuál es el mínimo necesario de cuadros por segundo a transmitir y el tamaño y nivel de compresión de la imagen, ya que se consumen demasiados recursos que pueden no ser necesarios en función del objetivo a cubrir por la cámara.

SOFTWARE PARA CALCULAR EL CONSUMO DE ANCHO DE BANDA Y ESPACIO EN DISCO (IP VIDEO SYSTEM DESING TOOL)

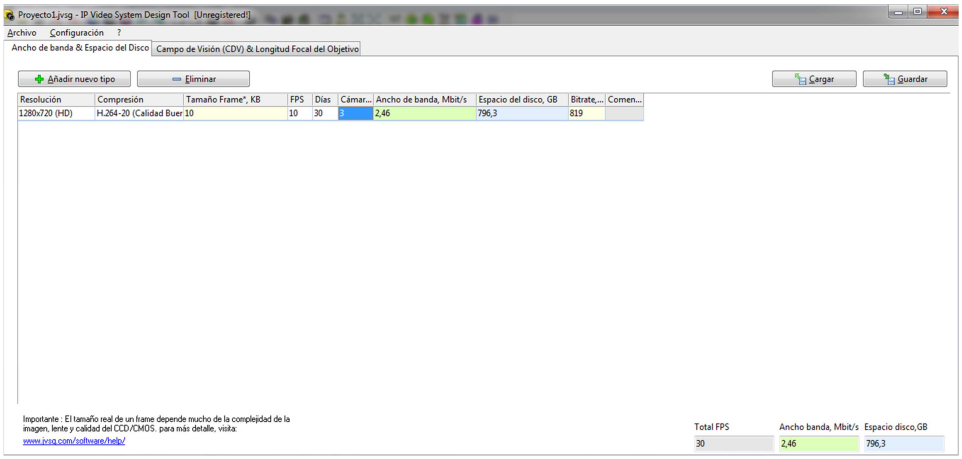

Figura 3.67. Calculadora Ancho de Banda Video Vigilancia [20]

[20] http://www.idris.com.ar/BWCalc/

3.2.2.2. VOZ SOBRE IP (VoIP)

Cálculos para VoIP

El cálculo se dimensiona para cubrir la demanda de 600 usuarios aproximadamente, con un escenario de 5 llamadas/hora, con una duración de 2 minutos cada llamada en la hora pico, y con una probabilidad de bloqueo del 1%.

La intensidad de tráfico se calcula mediante la siguiente fórmula **[formula 1]**:

$$A(Erlangs) = \frac{M * L * H}{3600}$$

Dónde:

M: número de usuarios

L: número de llamadas en la hora pico

H: duración de la llamada en segundos

$$A(Erlangs) = \frac{600 * 5 * (3 * 60)}{3600}$$

$$A(Erlangs) = 150E$$

Con estos datos podemos determinar el número de circuitos necesarios para soportar el tráfico obtenido, mediante la calculadora de Erlang-B**[19]**.

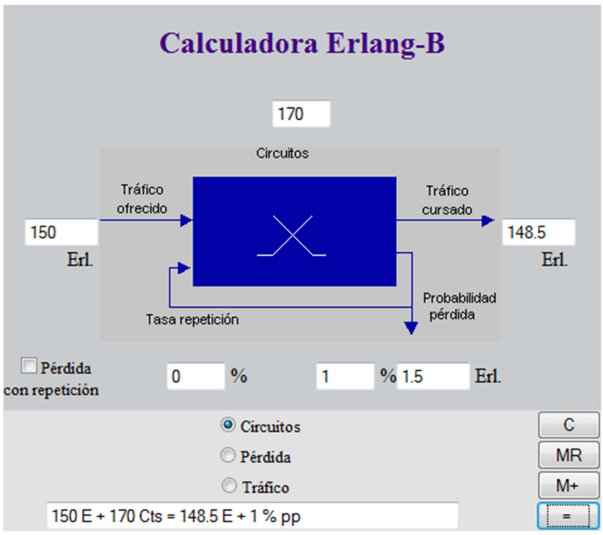

Figura 3.68. Calculadora Erlang B

[19] http://personal.telefonica.terra.es/web/vr/erlang/cerlangb.htm

Lo que resulta en 170 circuitos, lo que nos sirve para calcular el Ancho de Banda Total necesario para el soporte del servicio en estudio.

El códec a usar es el G. 723.1 de 5,3Kbps (Tabla 3.11), hay que considerar que todos los paquetes de VoIP contienen las propias muestras de voz y las cabeceras RTP, UDP e IP, así como los bytes de cabecera de capa 2, en este caso de Ethernet, por lo que la velocidad es mayor de 5,3 Kbps.

Para UDP se tiene el tamaño de encabezado de 8 bytes, en cuanto a IP el tamaño del encabezado en la mayoría de los casos de es de 20 bytes, pero podría crecer hasta 60 bytes con el campo de opciones (esto no es usual en VoIP por lo que tomaremos 20 bytes como tamaño IP).

Para RTP tiene tamaño variable también, aunque siempre que no haya mezcla de audio, esto es una conferencia, el tamaño será de 12 bytes.

La voz corre sobre RTP, que corre sobre UDP, que corre sobre IP, estos protocolos están siempre sobre una comunicación de VoIP.

Tamaño de la cabecera:

H(header): (RTP+UDP+IP)=40bytes + encabezado Ethernet (38) +encabezado MPLS(4)
Lt*N=20 Longitud de trama (Tabla 3.11)
Tt*N=30Tiempo de Trama (Tabla 3.11)

$$BW = \frac{(H + Lt * N)}{Tt * N} * 8$$

$$BW = \frac{((40 + 38 + 4) + 20)}{30} * 8$$

$$BW = 27,2Kbps$$

Se obtiene un ancho de banda de 27,2 Kbps. Existen factores a tener en cuenta en el cálculo como es la supresión de silencio, que se basa en la actividad de la voz. El factor

de la actividad de la voz suele considerárselo en el orden de un 35 %, aunque un valor de un 50% parece ser un valor más real acorde a mediciones reales.

Por lo tanto aplicando supresión de silencio de 50% (27,2 kbps*0.005) se obtiene= 13,6 Kbps.

Usando la calculadora de Ancho de Banda de VoIP: **[2020]**

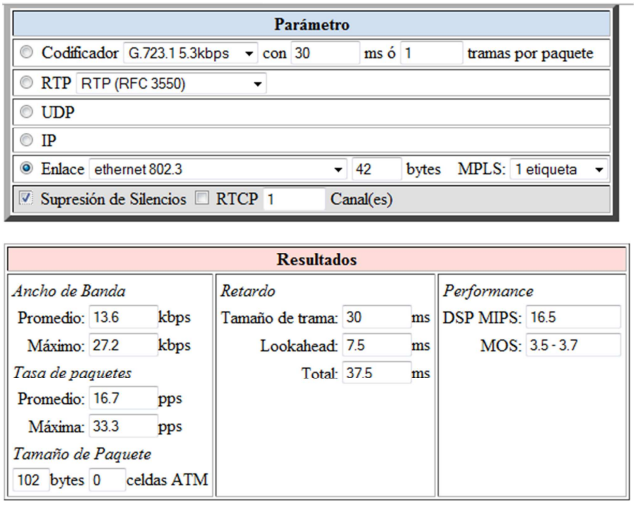

Figura 3.69. Calculadora del ancho de banda VoIP [20]

Usando la calculadora de ancho de banda VoIP se comprueba los datos obtenidos mediante las formulas. La calculadora visualiza según la velocidad del códec utilizado, un ancho de banda de 13,6 Kbps considerando supresión de silencio de 50%.

Por lo tanto, el ancho de banda total para este servicio, tomando las consideraciones necesarias será de:

$$BW = 170 * 13,6 = 2312 Kbps$$
$$BW = 170 * 13,6 = 2,312 Mbps$$

[20] http://www.idris.com.ar/BWCalc/

3.2.2.3. VIDEO CONFERENCIA

La mayoría de los equipos permiten, llamadas multipunto de 3 +1 participantes sin necesidad de una unidad multipunto externa. El ancho de banda requerido en este equipo central será de la suma de cada conexión realizada:

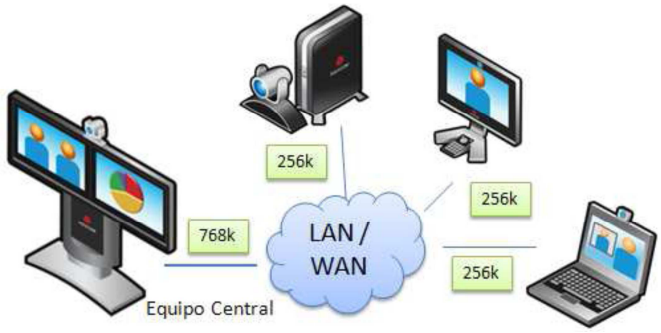

Figura 3.70. Consideración de ancho de banda

Cuando se requiere realizar llamadas multipunto de más de 4 participantes, es necesario contar con una unidad multipunto externa. Cada equipo realiza una marcación a este dispositivo por lo que el ancho de banda se distribuye como se indica la figura 3.71:

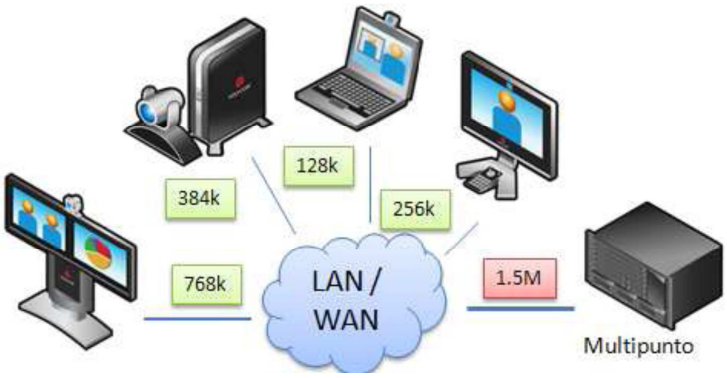

Figura 3.71. Consideración de ancho de banda multipunto

Las llamadas punto a punto entre los equipos terminales de video se harán a través de los enlaces que los unan, mientras que las llamadas multipunto se harán entre el equipo final

y la infraestructura centralizada de Polycom. El Ancho de Banda que esta tecnología requiere por sitio para HD es de 512Kbps y tomando en consideración los 5 sitios que necesita cubrir el Servicio, nos da un total de 2,5 Mbps, tal y como nos indica la figura 3.72:

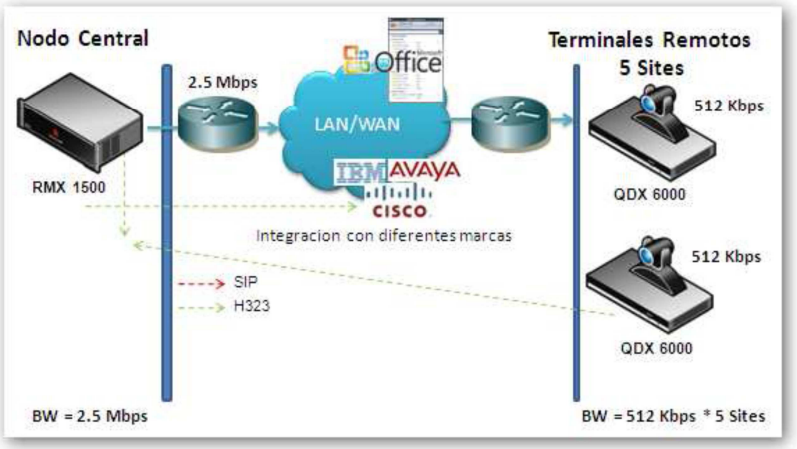

Figura 3.72. Consideración de Ancho de Banda para Video Conferencia

3.2.2.4. SISTEMA TRONCALIZADO IP

Cálculo de Canales

Para el cálculo de los canales necesarios para la red de acceso del sistema troncalizado nos basamos en la fórmula de Erlang B:

$$A(Erlangs) = \frac{M * L * H}{3600}$$

Dónde:

M: número de usuarios

L: número de llamadas en la hora pico

H: duración de la llamada (seg)

De acuerdo a la información obtenida, se estima un total de 600 usuarios (fijos, móviles y portátiles), se toma en consideración cada uno de los sitios con sus respectivos usuarios, por ejemplo, en un sitio con 100 móviles, la duración media de la llamada de

20 seg, y un promedio de llamadas en la hora pico de 3, de acuerdo a esto y a la fórmula de Erlang B:

$$A(Erlangs) = \frac{100 * 3 * 20}{3600} = 1{,}666Erlangs$$

Y para determinar el número de canales, nos ayudamos de la calculadora de Erlang B:

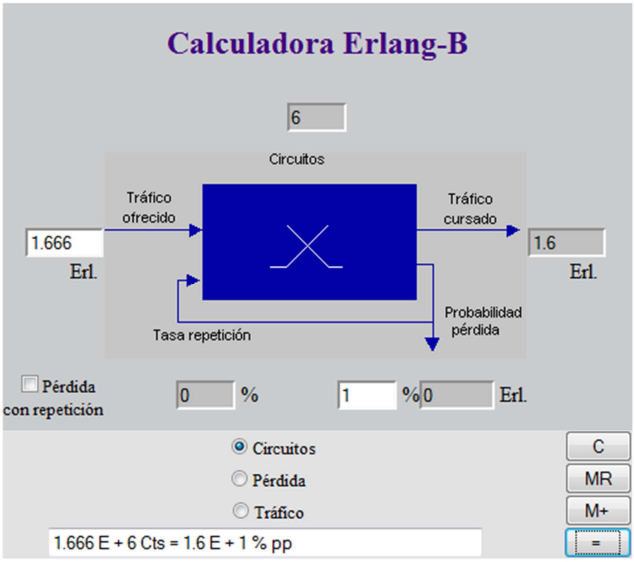

Figura 3.73. Calculadora Erlang B [19]

De acuerdo a estos datos, realizamos el cálculo para cada una de los sitios y obtenemos la tabla 3.14:

SITIO	Nro. EQUIPOS	ERLANGS	CANALES
Icto Cruz	100	1,66666667	6
Portete	90	1,5	6
Chilla	80	1,33333333	5
Morupe	90	1,5	6
Motilon	80	1,33333333	5

[19] http://personal.telefonica.terra.es/web/vr/erlang/cerlangb.htm

Villonaco	80	1,33333333	5
Cerro Bosco	80	1,33333333	5
Total	600	10	38

Tabla 3.14. Resultados de aplicación de fórmulas y Calculadora Erlang B.

Luego del cálculo se obtiene un total de 38 canales, como se sabe que un E1(2Mbps) tiene 32 canales(se usan solo 30), con 2E1, tendríamos suficientes canales para cubrir estas necesidades.

Un radio trunking, utiliza un canal de comunicación, en el caso de tener 100 radios, y a través de cálculos (Erlang B), estos utilizarían 6 canales de comunicación (más 2 de control), esto quiere decir que en este sitio pueden funcionar 6 radios de manera simultánea.

Se toma en consideración los requerimientos de la Institución, en cuanto al índice de crecimiento y en base a ello, se toma en cuenta como el número máximo de canales (28 canales), por cada uno de los sitios (destacamentos), además se sabe que radio utiliza 9.6kbps de ancho de banda.

Por lo tanto el ancho de banda para el sitio en ejemplo (100 radios), seria de: En este caso se considera, el máximo número de canales (28 canales) de acuerdo al crecimiento impuesto, no se utiliza el número de canales obtenidos con el cálculo para 100 usuarios.

$$BW = 9.6Kbps * 28 = 268.8Kbps$$

Y el ancho total, para los 7 sitios en cuestión, resultaría:

$$BW = 268.8Kbps *= 1.881Mbps$$

3.2.3. DIMENSIONAMIENTO DEL BACK BONE

Para el dimensionamiento vamos a tomar en cuenta el número de usuarios para cada servicio, para el dimensionamiento de la parte de video vigilancia se toma en consideración lo siguiente.

Servicio	Numero de host	Red y Broadcast	Nro. de direcciones totales
Video vigilancia	40	+ 2 (red y broadcast) + 1(Ethernet)	43

Tabla 3.15. Información para el dimensionamiento video vigilancia.

Como se necesita 43 direcciones en total, tenemos que con 2^6 = 64 Direcciones (62 direcciones asignables), por lo tanto tenemos 6 bits de host, y la máscara de red seria: 255.255.255.192 /26

Entonces tendríamos:

	Host		
Network	Desde	hasta	Broadcast
192.168.1.0	192.168.1.1	192.168.1.63	192.168.1.64

Tabla 3.16. Direcciones IP video vigilancia.

Para el servicio de video conferencia tenemos lo siguiente:

Servicio	Numero de host	Red y Broadcast	direcciones totales
Video conferencia	10	+ 2 (red y broadcast) + 1(Ethernet)	13

Tabla 3.17. Información para el dimensionamiento video conferencia.

Como se necesita 13 direcciones en total, tenemos que con 2^4 = 16 Direcciones (14 direcciones asignables), por lo tanto tenemos 4 bits de host, y la máscara de red seria: 255.255.255.240 /28

Entonces tendríamos:

	Host		
Network	Desde	hasta	broadcast
192.168.2.0	192.168.2.1	192.168.1.14	192.168.1.15

Tabla 3.18. Direcciones IP video vigilancia.

Y para el servicio de VoIP tenemos los siguientes datos:

Servicio	Numero de host	Red y Broadcast	Nro. de direcciones totales
VoIP	600	+ 2 (red y broadcast) + 1(Ethernet)	602

Tabla 3.19. Información para el dimensionamiento VoIP.

Como se necesita 602 direcciones en total, tenemos que con 2^{10} = 1024 Direcciones (1022 direcciones asignables), por lo tanto tenemos 10 bits de host, y la máscara de red seria: 255.255.252.0 /22

Entonces tendríamos:

	host		
Network	Desde	hasta	broadcast
192.168.4.0	192.168.4.1	192.168.7.254	192.168.7.255

Tabla 3.20. Direcciones IP video vigilancia.

3.2.4. DEFINICIÓN Y ELECCIÓN DEL PROTOCOLO DE ENRUTAMIENTO DEL BACK BONE

Tipos de Enrutamiento

Los protocolos de enrutamiento nos brindan diferentes mecanismos para crear y mantener las tablas de enrutamiento de en cada uno de los routers pertenecientes a la red, de esta manera se establecen las rutas para llegar a los host, en un mismo router existe la posibilidad de tener distintos protocolos de encaminamiento.
Las manera que los router aprenden sobre las redes remotas, lo pueden hacer de manera dinámica, o de usando estáticas.

En algunos casos se prefieren el uso de rutas estáticas, debido a que la cantidad de procesamiento es menor, y no sobrecargar los routers como el enrutamiento dinámico, durante el envío de paquetes los routers aprenden sobre las redes remotas, y mantienen esta información.

Se utilizan las tablas de enrutamiento para encontrar la mejor coincidencia entre la dirección IP destino, y una dirección de red en la tabla de enrutamiento, además de determinar la interfaz por la que se enviara el paquete. Para enviarse el paquete es necesario que se encapsule en una trama de enlace de datos apropiada para la infertaz.

En el ruteo existen dos tipos de protocolos, los protocolos enrutados y los protocolos de enrutamiento que determinan las rutas que siguen los protocolos enrutados hacia los destinos, como RIP, IGRP, EIGRP , OSPF y BGP

Entre los diferentes tipos de enrutamiento, se va a considerar principalmente el enrutamiento estático.

Enrutamiento Estático.

Las tablas de enrutamiento estático nos presentan los inconvenientes, al momento de su configuración se las debe realizar de forma manual en cada uno de routers, con toda la

información que se contenga. Una de las ventajas principales que tenemos es que las rutas estáticas no cambian, por lo tanto son más estables que las dinámicas.

Para este estudio, se considera de cierta manera un enrutamiento estático, a los tuéneles creados para enviar información de cada uno de los servicios, en este caso estos túneles se les conoce como VRFs.

VRF (*Virtual Routing and Forwarding*) es una tecnología que nos permite múltiples tablas de rutas separadas, las cuales pueden estar en el mismo router, todas las tablas pueden ser independientes. La implementación de esta tecnología se puede realizar en un dispositivo de red, por distintas FIB(tablas de rutas), una por cada una de las VRF.

De acuerdo a los requerimientos del proyecto, vamos a crear una VRF, para cada uno de los servicios, como en el servicio de VoIP, en este todos los usuarios de la red tienen el acceso a este servicio, en la figura 3.74 se muestra el diagrama de la red, y de la VRF para este servicio.

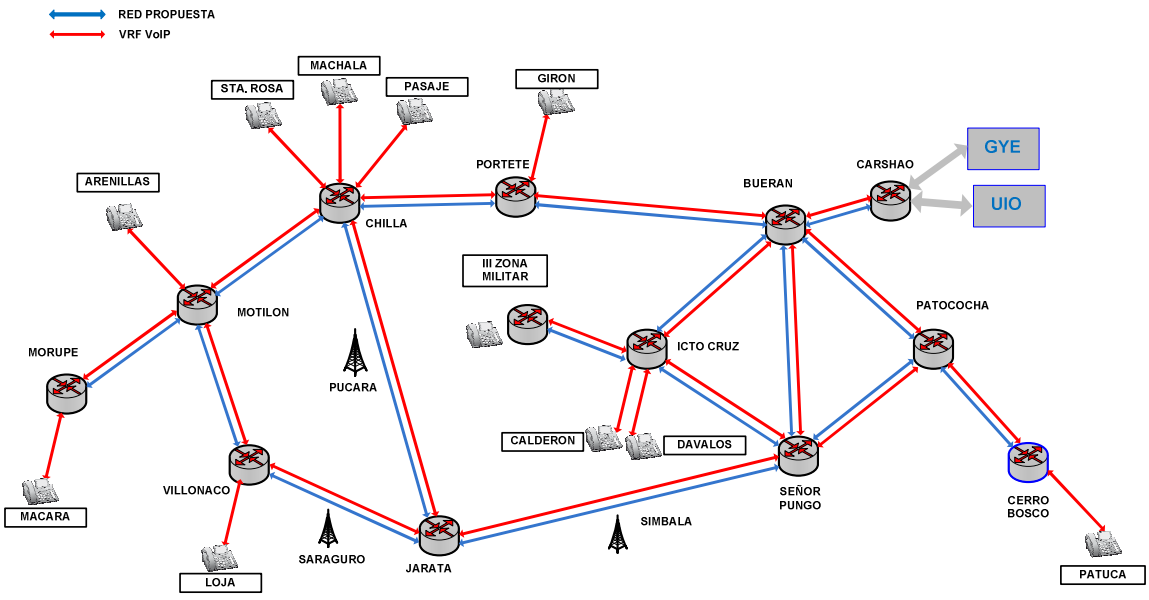

Figura 3.74 VRF para el servicio de VoIP.

De acuerdo a los requerimientos, para el servicio de video conferencia, se solicitó que solamente los destacamentos de: Loja, Machala, Patuca, Calderón, Dávalos, tengan

acceso a este servicio, la III Zona Militar, es la parte central para este servicio, se ilustra en la figura 3.75.

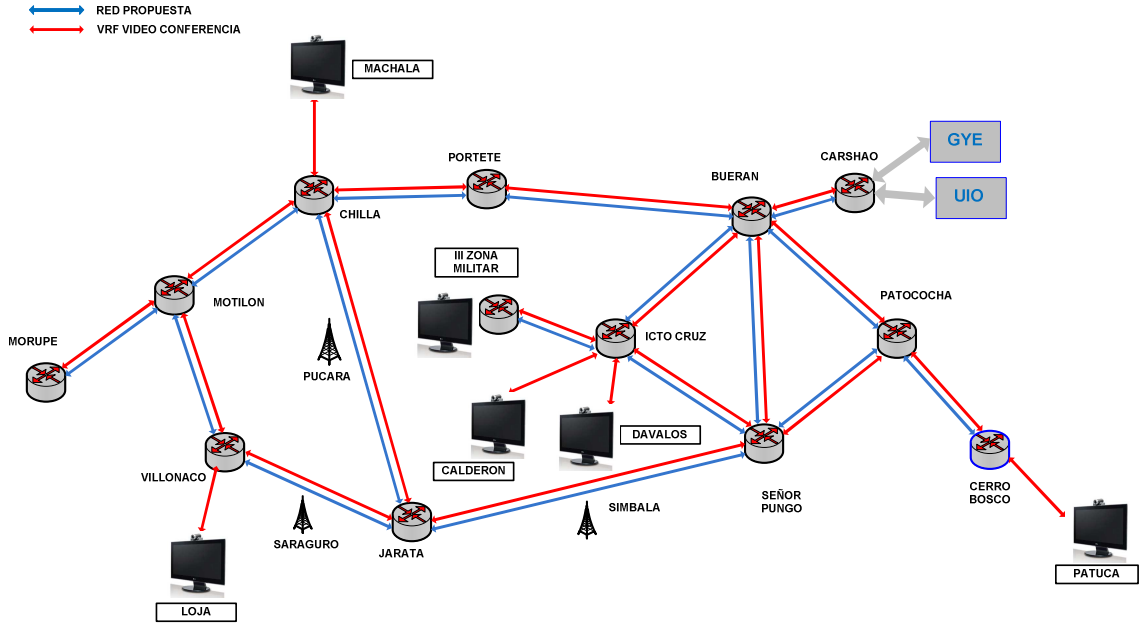

Figura 3.75. VRF para el servicio de Video Conferencia.

Para el servicio de video vigilancia, se tomaron en cuenta todos los destacamentos con sus respectivas bodegas, y teniendo como central la III Zona Militar, desde este destacamento es posible acceder hacia todas las cámaras IP presentes en la red, como se muestra en la figura 3. 76.

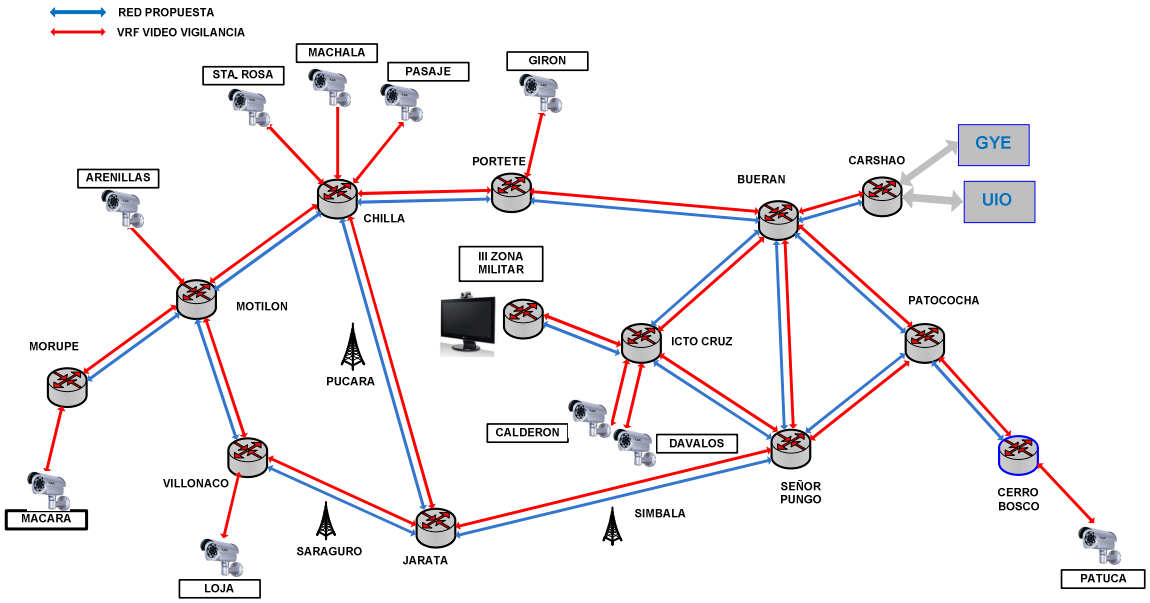

Figura 3.76. VRF para el servicio de Video Conferencia.

3.2.5. CALIDAD DE SERVICO

El administrador de la red, puede activar la calidad de servicio QoS en las interfaces WAN del router, en los túneles y las interfaces VPN IPSec. Las políticas se aplican al tráfico saliente.

Generación de la política de QoS

Para asignar los anchos de banda a los distintos tipos de tráfico que pasan a través de la interfaz seleccionada, en nuestro caso tenemos un valor total de 100 Mbps. Por ejemplo, si especifica 5%, se asigna un ancho de banda de 5Mbps. El valor del porcentaje total para cualesquier tipo de tráfico no debe superar el 75%, a excepción del best effort.

Las consideraciones necesarias que se tienen para los tipos de tráfico no deben superar los siguientes porcentajes.

Voz: El valor que se considera es del 15 por ciento del ancho de banda.
Video vigilancia: El valor que se considera es del 25 por ciento del ancho de banda.

Video Conferencia: El valor que se considera es del 30 por ciento del ancho de banda.

Además del ancho de banda necesario para los servicios a brindar, se utiliza también para la señalización de llamadas, la que se encarga de la señalización necesaria para controlar el tráfico de voz. El valor por defecto es el 5 por ciento del ancho de banda.

Enrutamiento: tráfico generado por éste y otros routers para administrar el enrutamiento de paquetes. El valor por defecto es el 5 por ciento del ancho de banda.

Administración: Telnet, SSH y otros tráficos generados para administrar el router. El valor por defecto es el 5 por ciento del ancho de banda.

Transaccional: por ejemplo, el tráfico generado para aplicaciones comerciales o actualizaciones de base de datos. El valor por defecto es el 5 por ciento del ancho de banda.

Best Effort: ancho de banda restante para otro tráfico, como el tráfico de correo electrónico. El valor por defecto es el 47 por ciento del ancho de banda. El valor de Mejor esfuerzo se actualiza dinámicamente según el porcentaje total para los otros tipos de tráfico.

CAPITULO 3-BIBLIOGRAFÍA

[1] **"***CFIP PhoeniX ODU "*, septiembre 2011
www.technicalbase.com.ar/PDFs/WirelessNetworking/CFQ_productline_esp.pdf

[2] "*Customized Microwave Solutions* **"**
https://www.saftehnika.com/upload/File/Siebel/201005013_SAF_CFIP_CFQ_brochure_Esp.pdf

[3] LOZADA, Diego y VEGA, Marcia *" Diseño de una Red de alta capacidad para el Enlace Quito – Lago Agrio utilizando radios SDH para el transporte de datos"*
http://dspace.epn.edu.ec/bitstream/15000/10359/2/T12006_paper.pdf

[4] "*COMHAT TECHNICAL DATA ANTENNA*", octubre 2011
http://www.ultratelecom.kiev.ua/catalog/%287GHz,1.2m%2920041227154950251901-HAA0712_00-PA3.pdf

[5] **"***Polycom VideoConfenrencing"*, octubre 2011
http://www.videoconferencia.es/polycom.html

[6] *"Polycom® QDX 6000",* noviembre 2011
http://latinamerica.polycom.com/products/telepresence_video/video_conference_systems/room_systems/qdx6000.html

[7] WIKIPEDIA, *"Videovigilancia IP"*, noviembre 2011
http://es.wikipedia.org/wiki/V%C3%ADdeovigilancia_IP

[8] SACA, Angel, *"Diseño del Sistema de Vigilanciacon cámaras IP para el EdificioMatriz de Petroecuador",* Escuela Politecnica Nacional, marzo 2010
bibdigital.epn.edu.ec/bitstream/15000/2162/1/CD-2919.pdf

[9] WIKIPEDIA, **"***Voz sobre Protocolo de Internet"*, diciembre 2011
http://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet

[10] "*Protocolos utilizados para las redes de Nueva Generación"*
http://dspace.epn.edu.ec/bitstream/15000/8712/1/T10902ANEXOS.pdf

[11] OCHOA, Edgar, Material de la asignatura "*Comunicaciones III*", Universidad Politécnica Salesiana, 5 año.

[13] RAMOS, Henry, *"VoIP Corporación Nacional de Telecomunicaciones CNT S.A Diseño"*, Tesis Universidad Politecnica Salesiana, Cuenca, septiembre 2009
http://hdl.handle.net/123456789/32

[14] "*Router Cisco 3800"*, diciembre 2011
http://www.router-switch.com/Cisco-Price-cisco-routers-cisco-router-3800-

[15] "*Teléfono IP Linksys SPA942"*, diciembre 2011
http://www.inphonex.es/productos/linksys-spa942.php

[17] DUQUE, Darío "*Estudio para la migración del sistema troncalizado de la fuerza terrestre del Ecuador de una plataforma smartzone a una plataforma APCO P25 IP"*, ESPE / 2010
http://www3.espe.edu.ec:8700/bitstream/21000/2634/1/T-ESPE-029866.pdf

[18] SOFTWARE, **"***IP Video System Design Tool"*, diciembre 2011
http://www.jvsg.com/es/

[19] SOFTWARE, **"***Calculadora Erlgan-B"*, diciembre 2011
http://personal.telefonica.terra.es/web/vr/erlang/cerlangb.htm

CAPITULO 4

4.1 ANÁLISIS ECONÓMICO

4.1.1 INTRODUCCIÓN

El análisis económico del proyecto, está conformado por una técnica matemática financiera, que nos ayuda a determinar, que tan factible es la realización del proyecto, es decir, nos ayuda a tomar una decisión acerca de los beneficios o perdidas que se obtiene con la inversión que se realizara en el mismo.

Es necesario que en todo proyecto se realice el análisis económico, de esta manera podemos determinar la rentabilidad y la factibilidad del mismo, para determinar estos datos es necesario tomar en consideración los costos de inversión, y también la relación costo beneficio, los cuales nos darán una visión más clara acerca de la inversión que se pretende realizar.

Se tiene los siguientes términos como: VAN, TIR.

4.1.2. VAN (VALOR ACTUAL NETO) [1]

El valor actual neto, es la diferencia entre el valor actual de los ingresos esperados de una inversión y el valor actual neto que la misma ocasione, es una rentabilidad mínima pretendida por el inversor, por debajo de la cual estará dispuesto a efectuar su inversión.

Este método toma en consideración el valor tiempo de dinero, los ingresos que se esperan en el futuro, como también los egresos, deben ser actualizados a la fecha del inicio del proyecto.

La tasa de interés la determinaran las personas que evalúan el proyecto, conjuntamente con los inversionistas o dueños de dicha inversión.

4.1.3. TIR (TASA INTERNA DE RETORNO)[1]

[1] http://dspace.ups.edu.ec/bitstream/123456789/828/5/CAPITULO%205.pdf

La tasa interna de retorno iguala la suma de ingresos actualizados, con la suma de egresos actualizados, o también se considera que es la tasa de interés que hace cero al VAN del proyecto. A partir de esta tasa podemos obtener un criterio de rentabilidad y no de ingreso monetario neto.

4.1.4. RELACIÓN COSTO / BENEFICIO [1]

Esta relación nos muestra la rentabilidad en términos relativos y la interpretación del resultado se expresa en centavos ganados por cada dólar de inversión en el proyecto.
La relación se puede calcular al dividir la sumatoria de los valores del VAN y el año de la inversión al año cero (inversión total inicial).

$$\frac{B}{C} = \frac{\sum_1^N VAN_n}{Inversion\_Inicial}$$

Ecuación 1. Relación costo beneficio/costo

Donde:

B/C Relación Beneficio/Costo

VAN Valor Actual Neto

N Duración del proyecto en años.

Esta relación es indispensable para la decisión de proyectos, ya que nos indica la cantidad de dólares que se está obteniendo o perdiendo por cada uno de los dólares invertidos, mientras este valor sea mayo a 1, quiere decir que económicamente el proyecto es factible.
Las siguientes condiciones, nos ayudan mediante los términos vistos anteriormente a determinar las factibilidades de los proyectos:

4.1.4. PARA ACEPTAR UN PROYECTO [1]

Para que un proyecto sea aceptado debe cumplir con los siguientes resultados:

---

[1]http://dspace.ups.edu.ec/bitstream/123456789/828/5/CAPITULO%205.pdf

VAN > 0.

TIR > Tasa de actualización inferior, pero dentro de los valores de interpolación

B/C >1

Con estos resultados podemos interpretar que con el valor del VAN es mayor a cero, los beneficios superan los costos, que mediante el TIR, la tasa interna de rendimiento es superior a la tasa bancaria, y mediante la relación B/C, que los beneficios que el proyecto generara son superiores a los costos de implementación.

4.1.5. PARA RECHAZAR UN PROYECTO [1]

Las condiciones para que un proyecto sea descartado o rechazado son las siguientes:

VAN < 0

TIR<Tasa de descuento

B/C < 1

En este caso, los beneficios son inferiores a los costos, la tasa interna de rendimiento es inferior a la tasa bancaria, siendo rechazado definitivamente el proyecto.

4.1.6. PARA POSTERGAR UN PROYECTO [1]

Se posterga un proyecto cuando te obtiene los siguientes resultados.

VAN = 0

TIR = Tasa de descuento

B/C = 1

Para este caso tenemos un equilibrio entre los beneficios y los costos de los proyectos, por lo tanto se pueden realizar algunas variables, que tengan que ver con la inversión, ya sea cambio de tecnología, etc., con la finalidad de obtener mejores resultados.

4.2 ANÁLISIS ECONÓMICO DEL PROYECTO

[1] http://dspace.ups.edu.ec/bitstream/123456789/828/5/CAPITULO%205.pdf

Para realizar el análisis económico del proyecto, se toma en consideración en primera instancia la cotización de los radioenlaces.

COSTOS DE ENLACES SAF CFIP PHOENIX 1+1		
CANTIDAD	**DESCRIPCIÓN**	**SUBTOTAL**
1	ENLACE III ZONA MILITAR - ICTO CRUZ	$ 27.357,12
1	ENLACE ICTO CRUZ – BUERAN	$ 28.603,68
1	ENLACE BUERAN – PATOCOCHA	$ 29.850,24
1	ENLACE BUERAN – CARSHAO	$ 28.611,97
1	ENLACE PATOCOCHA – CERROBOSCO	$ 28.611,97
1	ENLACE BUERAN – PORTETE	$ 31.613,69
1	ENLACE PORTETE – CHILLA	$ 34.176,96
1	ENLACE CHILLA – MOTILON	$ 34.176,96
1	ENLACE MOTILON – VILLONACO	$ 34.176,96
1	ENLACE MOTILON – MORUPE	$ 31.613,69
TOTAL DÓLARES		$ 308.793,23

Tabla 4.1 Costos de los Enlaces

En la siguiente tabla se muestra es costo de los enlaces redundantes de la red.

COSTOS DE ENLACES RED REDUNDANTE SAF CFIP PHOENIX 1+1		
CANTIDAD	**DESCRIPCIÓN**	**SUBTOTAL**
1	ENLACE SEÑOR PUNGO– BUERAN	$ 27.357,12
1	ENLACE SIMBALA– JARATA	$ 28.603,68
1	ENLACE SARAGURO – VILLONACO	$ 29.850,24
1	ENLACE SEÑOR PUNTO - ICTO CRUZ	$ 28.611,97
1	ENLACE SEÑOR PUNGO–SIMBALA	$ 28.611,97
1	ENLACE SEÑOR PUNGO– PATOCOCHA	$ 31.613,69
1	ENLACE PUCARA – JARATA	$ 34.176,96
1	ENLACE PUCARA – CHILLA	$ 34.176,96
1	ENLACE JARATA – SARAGURO	$ 34.176,96
TOTAL DÓLARES		$ 277.179,55

Tabla 4.2 Costos de los Enlaces Redundantes

Los ROUTERS CISCO 2800, se instalaran en cada uno de los nodos, que se encargan del enrutamiento y el tráfico.

COSTOS EQUIPOS ROUTER CISCO 2800			
CANTIDAD	**DESCRIPCIÓN**	**SERIE**	**SUBTOTAL**
1	III ZONA MILITAR	2811	$ 998,00
1	ICTO CRUZ	2811	$ 998,00
1	BUERAN	2811	$ 998,00
1	CARSHAO	2811	$ 998,00
1	CERROBOSCO	2811	$ 998,00
1	PORTETE	2811	$ 998,00
1	CHILLA	2811	$ 998,00
1	MOTILON	2811	$ 998,00
1	VILLONACO	2811	$ 998,00
1	MORUPE	2811	$ 998,00
TOTAL DÓLARES			$ 9.980,00

Tabla 4.3 Costos Routers Cisco 2800

Los SWITCHS de concentración solamente se instalaran en los siguientes nodos.

COSTOS EQUIPOS SWITCH DE CONCENTRACIÓN			
CANTIDAD	**DESCRIPCIÓN**	**SERIE**	**SUBTOTAL**
1	BUERAN	2811	$ 998,00
1	CARSHAO	2811	$ 998,00
1	MOTILON	2811	$ 998,00
TOTAL DÓLARES			$ 2.994,00

Tabla 4.4 Costos Switches Cisco 2800

Los ROUTERS CISCO en cada uno de los destacamentos, que nos servirán como equipos terminales.

COSTOS EQUIPOS DESTACAMENTOS ROUTER			
CANTIDAD	**DESCRIPCIÓN**	**SERIE**	**SUBTOTAL**
1	III ZONA MILITAR	881	$ 337,00
1	CALDERÓN	881	$ 337,00
1	DÁVALOS	881	$ 337,00
1	PATUCA	881	$ 337,00
1	MACHALA	881	$ 337,00
1	SANTA ROSA	881	$ 337,00
1	PASAJE	881	$ 337,00
1	ARENILLAS	881	$ 337,00
1	LOJA	881	$ 337,00
1	MACARA	881	$ 337,00
TOTAL DÓLARES			$ 3.370,00

Tabla 4.5 Costos Routers Serie 881

Solución de Videoconferencia Multipunto (5 salas).

COSTOS EQUIPOS VIDEOCONFERENCIA 5 SALAS – POLYCOM			
CANTIDAD	**DESCRIPCIÓN**	**P. Unit.**	**SUBTOTAL**
1	RMX 1500 Base System, loaded with 10SD, 15 CIF resource licenses, upgradable with SW licence to 25 CIF or/and HD support, equipped with MPMx-Q(Maintenance contract required)	$ 17.164,21	$ 17.164,21
1	Premier one year RMX 1500 Base System, loaded with 10SD, 15 CIF resource licenses, upgradable with license to 25 CIF or/and HD support, equipped with MPMx-Q	$ 3.133,68	$ 3.133,68
1	RMX 1500/2000/4000 encryption license pack - restricted by destination countries	$ 0,00	$ 0,00
1	RMX 1500 HD CP software license option (Maintenance contract required). Available only on RMX1500 MPMx-Q configurations	$ 6.440,00	$ 6.440,00
1	Premier One Year RMX1500 HD CP Software License Option	$ 1.363,16	$ 1.363,16
EQUIPOS DHX 6000 para CUENCA(2), PATUCA, LOJA, MACHALA			
5	QDX 6000 codec, EagleEye QDX with 3m cable, 2 QDX mics with 25´ cables, H.239, PPCIP, Spanish Remote, Cable bundle (6´ Component, 12´ LAN, 6´ combo-S-video. RCA composite& dual audio, 1.5m VGA monitor),Power Cords: 10' NA, 2.5 Eur, 1 yr Prem Srvc	$ 4.925,26	$ 24.626,32
5	EagleEye HD, EagleEye View and EagleEye QDX Camera wall/panel/shelf mounting bracket	$ 130,53	$ 652,63
	SERVICIOS DE INSTALACIÓN		

5	Instalación, configuración y pruebas	$ 400,00	$ 2.000,00
	Capacitación sobre el manejo de la solución (4 personas)	**Subtotal**	**$ 55.380,00**
		12% IVA	**$ 6.645,60**
		TOTAL	**$ 62.025,60**

Tabla 4.6 Costos Equipos Videoconferencia 5 Salas Polycom

Cámaras para video vigilancia.

COSTOS EQUIPOS VIDEO VIGILANCIA			
CANTIDAD	**DESCRIPCIÓN**	**SUBTOTAL**	**TOTAL**
33	Cámaras Axis 216MFD	$ 337,00	$ 11.121,00

Tabla 4.7 Cámaras Video Vigilancia

Sumando todos los valores de las cotizaciones tenemos el costo total de inversión:

COSTO TOTAL DE LA INVERSIÓN
$ 675.463,38

Tabla 4.8 Costos Total de Inversión

La III Zona Militar al contar con su propia red, y sus propios servicios, se ahorraría, el pago a otras empresas, de esta manera se considera, los siguientes precios de servicios, como un ahorro.

AHORROS POR COSTO DE INVERSIÓN						
SERVICIOS						
VOIP	$300	$290	$280	$270	$260	$250
VIDEOCONFERENCIA	$250	$240	$230	$220	$210	$200
VIDEO VIGILANCIA	$500	$490	$480	$470	$460	$450
VALOR TOTAL AÑO (MENSUAL X 12)	**$12600**	**$12240**	**$11880**	**$11520**	**$11160**	**$10800**

TABLA 4.9 Ahorros por Costos de Inversión

La vida útil de la tecnología de comunicación se considera para un tiempo de 10 años, por lo que se considera que la depreciación anual será de:

DEPRECIACIÓN ANUAL	$ 67.546,34

Tabla 4.10 Depreciación Anual

Como egresos se consideran los gastos de operación, en este caso se toman en cuenta los equipos de backup, los cuales son indispensables al momento de fallas de los equipos y caídas de la tecnología en general, que se pueden dar por varios factores.

COSTOS DE OPERACIÓN						
Equipos de backup	$ 16.290	$ 16.290	$ 16290	$ 16290	$ 16290	$ 16290

Tabla 4.11 Costos de Operación

A partir de esto calculamos el flujo neto efectivo (ingresos – egresos)

FLUJO NETO EFECTIVO	-$ 3.690,00	-$ 4.050,00	-$ 4.410,00	-$ 4.770,00	-$ 5.130,00	-$ 5.490,00

Tabla 4.12 Flujo Neto Efectivo

Procedemos a calcular el VP(VALOR PRESENTE): tomando en cuenta la tasa de rendimiento deseada en este caso del 14%, y aplicando la fórmula:

$$VP = \frac{VR}{(1+i)^n}$$

Donde:

"VR" consideramos el flujo neto efectivo de cada año.
"i" la tasa de rendimiento deseada, y "n" el año en que se estamos calculando.

VALOR PRESENTE	-3236,84	-3116,34	-2976,62	-2824,22	-2664,36	-2501,17

Tabla 4.13 Valor Presente

Para el cálculo del valor residual, se toma en cuenta la inversión total, y a este le restamos el valor de la depreciación acumulada (el valor de la depreciación multiplicado por el número de años en este caso 6).

VALOR RESIDUAL	$ 270.185,35

Tabla 4.14valor Residual

Y por último calculamos VPN (Valor Presente Neto), que nos resulta la suma de las VPs de cada año, restado el costo de inversión y sumado el valor residual.

VALOR PRESENTE NETO	-$ 422.597,59

Tabla 4.15 Valor Presente

En este caso el valor obtenido es menor a cero, lo que nos dice que el proyecto no es factible a primera instancia, se ha analizado y considerado que se trata de una empresa pública, y no pretende vender su servicios, son para usos particulares, de esta manera el proyecto resulta viable tomando en cuenta los beneficios ya que se trata de seguridad nacional.

4.3. CONCLUSIONES

La Red PDH del sistema Militar existente tiene ya 10 años de haberse implementado y ya tiene antecedentes de haber presentado fallas y caídas de enlaces. La misma necesita ya de un mantenimiento y actualización-UpGrade del Release de los Radios, esto como medida preventiva y correctiva. Por el mismo tiempo de funcionamiento de las Microondas se ha perdido estabilidad en la conexión, haciendo que los tiempos de respuesta sean demasiado largos en caso de caída de servicio; es decir, al momento de caerse un Nodo de la Red, el personal de Soporte Técnico Militar se moviliza al sitio en cuestión, lo que implica un tiempo de traslado, más un tiempo de detección del problema y más un tiempo de solución.

La necesidad de la III Zona Militar es la de implementar nuevos servicios (Video Vigilancia, Videoconferencia, VoIP, etc) sobre su red existente, generando exclusividad de tráfico, gestión de red y seguridad. El inconveniente que se tiene en este caso es que la tecnología de su red (PDH, Jerarquía Digital Plesiocrona) no soporta el transporte de este tipo de trafico porque la misma se basa en conmutación de circuitos, básicamente telefónicos, pero con sus respectivas limitaciones como por ejemplo: no es posible identificar una señal de orden inferior dentro de un flujo de orden superior, siendo necesario demultiplexar la señal completamente, esto se debe a que cada nivel jerárquico tiene su proceso de justificación y temporización. Otra limitación de estos sistemas es la

insuficiente capacidad de gestión de red a nivel de tramas, debido a que es muy complejo seguir un canal de tráfico a través de la red.

Para la actualización de la Red Militar se ha optado por una tecnología de Radio Enlaces de gran capacidad (SDH, Jerarquía Digital Síncrona), puesto que con la misma se obtiene una infraestructura de comunicaciones única, proporcionando completa centralización de todas las funciones de administración y control de la red. Como solución al requerimiento y al alcance del proyecto se ha seleccionado a la Marca de Microondas SAF en su serie "CFIP PhoeniX ", puesto que la misma proporciona desde un STM-1 (155,52 Mbps) de capacidad, esta serie de SAF es escalable hasta 366 Mbps nominales dependiendo de la Modulación, Banda de Frecuencia y de su respectiva Actualización – Release Licenciada. Esta serie se constituye en un elemento perfecto para cualquier red inalámbrica moderna futura, incluyendo proveedores de servicio móvil, fijo, datos, clientes empresariales, y redes gubernamentales como es el caso de la Red Militar.

SDH es un sistema de transporte digital sincrónico diseñado para proveer una infraestructura más sencilla, económica y flexible para redes de telecomunicaciones, emplea una infraestructura de comunicaciones única, conectando todas las sucursales y oficinas de la empresa y reduciendo los costes globales de las comunicaciones. A esta reducción de costes contribuye el tener tanto un único medio de transmisión como una tarifa plana, independiente del consumo.

Para el estudio ingenieril de la Red de Redundancia fue necesario realizar inspecciones y levantamientos de información en Sitio, puesto que los puntos de interconexión de la Red a proponer son críticos, debido a su situación geográfica distante. Cabe recalcar que fue imposible hacer uso de los datos obtenidos con herramientas virtuales tales como Google Earth, Google Maps, Radio Mobille, etc, porque no son reales y confiables, presentando muchas inconsistencias.

Con el diseño propuesto en este proyecto se establece una nueva Topología de red, en la cual es posible garantizar la disponibilidad del servicio, y en caso de pérdida de

conexión los tiempos de respuesta de backup van a estar dentro de un margen de tolerancia mínimo. Esta nueva topología de Red diseñada es capaz de soportar la tecnología MPLS y sus aplicaciones (VRFs, Virtual Routing Forwarding), dando paso a que se implementen varios servicios (convergencia).

La tecnología Ethernet no garantiza parámetros como, disponibilidad, reordenamiento de tramas, duplicación de tramas, tiempo de vida de la trama entre otros, en su lugar la tecnología MPLS que conmuta paquetes que se encuentran los niveles de capa 2 y 3 del modelo OSI, mejora funcionalidades de capa 2 Ethernet, sin sacrificar sus prestaciones.

EoMPL (Ethernet Over MPLS) proporciona calidad de servicio, anchos de banda reservados, ingeniería de tráfico, etc. MPLS tiene la capacidad de transportar diferentes tipos de tráfico, ya sea tráfico de voz, paquetes IP, etc., y dar prioridades a cada uno de estos.

Una de las mayores ventajas de la tecnología MPLS, es el uso de etiquetas que agrega a los encabezados de los paquetes, las mismas que tienen significado local en los conmutadores, de esta manera la conmutación de paquetes es más rápida. Luego de que MPLS distribuye sus etiquetas, necesita establecer las trayectorias de conmutación o LSP, que son similares a un túnel, y tienen un solo sentido de emisor a receptor.

El administrador de una red MPLS es quien determina que los datos entren o salgan del LSP, razón por la que MPLS es bastante segura, y los datos que se transmiten a los dispositivos, solo son distinguidos por el módulo MPLS y no por capas superiores.

Para evitar la congestión de la red, MPLS tiene las características de ingeniería tráfico, y DiffServ permite priorizar el tráfico de acuerdo al servicio, de esta manera asegurando la calidad de servicio. Para evitar un mal desempeño en aplicaciones de real time (sensible a retardos), se debe tener la precaución de elegir un esquema de colas adecuado, entre los cuales podemos tener CQB, RED o WRED.

El análisis económico realizado muestra que el valor presente neto es negativo, en primera instancia este resultado demostraría que el proyecto no es viable, pero tomando en consideración que está empresa es pública, no vende servicios y sus fines están relacionados exclusivamente con el transporte secreto de información, destinada a la seguridad nacional, la inversión a realizar en la implementación del diseño se ve justificada en su totalidad. No existe razón alguna para que las Fuerzas Militares carezcan de una red que reúna todas las características de capacidad, calidad de servicio y seguridad.

4.4. RECOMENDACIONES

Desde el punto de vista técnico es recomendable y factible la aplicación de la tecnología MPLS en las redes del Ecuador, debido a que la gran mayoría de redes funcionan sobre núcleos constituidos en ATM. En el presente proyecto se estudió la interoperabilidad de estas dos tecnologías, donde la conmutación se realiza mediante la asignación de etiquetas locales en los equipos y el transporte se lo realiza a través del núcleo ATM.

La implementación de una red basada en MPLS es bastante costosa, por los equipos que se deben conseguir o por el software que se debe adquirir para realizar actualizaciones en los nodos. Desde este de vista, no es muy recomendable la implementación total de redes basadas en el protocolo MPLS debido a la fuerte inversión que se debe realizar. Cabe mencionar que actualmente las redes que existen en el país, dan abasto al crecimiento de la demanda de usuarios y están dimensionadas para soportar grandes capacidades, por lo que no sería necesario a corto plazo este tipo de implementación.

Dado los avances tecnológicos actuales y al auge de tecnologías como ATM, MPLS sería un complemento ideal para un mejor desarrollo de las redes de área metropolitana y extendida. La idea en un principio abarcaría implementar MPLS en áreas de mayor congestión de tráfico para lograr una mejor distribución y administración del mismo.

Dado las grandes posibilidades que presenta MPLS, en cuanto a sus aplicaciones, se torna muy necesario en el ambiente laboral tener conocimientos de esta tecnología, por

eso es muy necesario incluir un tópico relacionado en el pensum académico para complementar los conocimientos que se adquieren y estar actualizados en el medio tecnológico.

Cuando se tiene una red de proveedor de servicios funcionando, es recomendable realizar una medición de tráfico por cada sitio de la VPN, para realizar las correcciones necesarias tales como: la capacidad del canal contratado, la actualización del hardware o software del equipo que se usa en la VPN. Se puede recomendar que los enlaces sean sobredimensionados sobre para garantizar el cumplimiento de los SLAs, con la desventaja de que se incurre en gastos adicionales.

4.5 ANEXOS 1

ESTUDIO RADIOELÉCTRICO RED EXISTENTE
ENLACE ICTO CRUZ-III ZONA MILITAR

	ICTO CRUZ	III ZONA MILITAR
Elevación (m)	2832.78	2554.24
Latitud	02 55 51.59 S	02 53 27.46 S
Longitud	078 59 51.70 W	079 00 04.15 W
Azimuth Verdadero (°)	355.04	175.04
Ángulo Vertical (°)	-3.68	3.65
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	12.00	6.00
Ganancia de Antena (dBi)	30.20	30.20
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.30	4.30
Pérdida en Línea de TX (dB)	1.50	1.50
Pérdida en Conectores (dB)	1.00	1.00
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	4.44	
Pérdidas de Espacio Libre (dB)	122.92	
Pérdidas de Absorción Atmosférica (dB)	0.04	
Pérdidas Netas del Enlace (dB)	67.58	67.58
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	57.70	57.70
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-37.58	-37.58
Margen de Desv. - Térmico (dB)	39.42	39.42
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	63.94	
Fade occurrence factor (Po)	9.35E-09	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	100.00000	100.00000
(sec)	4.28e-06	4.28e-06
Fuera de Servicio Anual por Multitrayecto (%)	100.00000	100.00000
(sec)	1.93e-05	1.93e-05
(% - sec)	100.00000 - 0.00	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	39.42	
Intensidad de Lluvia (mm/hr)	2327.48	
Atenuación por Lluvia (dB)	39.42	
Fuera de Servicio Anual por Lluvia (%-sec)	100.00000 - 0.00	
Total Anual (%-seg)	100.00000 - 0.00	

Dom, Ene 22 2012
ICTO CRUZ - III ZONA MILITAR (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE ICTO CRUZ-BUERAN

	ICTO CRUZ	BUERAN
Elevación (m)	2832.83	3793.43
Latitud	02 55 51.59 S	02 35 58.30 S
Longitud	078 59 51.70 W	078 55 43.60 W
Azimuth Verdadero (°)	11.81	191.81
Ángulo Vertical (°)	1.36	-1.61
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	20.00	28.00
Ganancia de Antena (dBi)	37.46	37.46
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	37.45	
Pérdidas de Espacio Libre (dB)	141.44	
Pérdidas de Absorción Atmosférica (dB)	0.37	
Pérdidas Netas del Enlace (dB)	72.04	72.04
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	64.88	64.88
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-42.04	-42.04
Margen de Desv. - Térmico (dB)	34.96	34.96
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	25.86	
Fade occurrence factor (Po)	6.91E-05	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	99.99999	99.99999
(sec)	0.36	0.36
Fuera de Servicio Anual por Multitrayecto (%)	99.99999	99.99999
(sec)	1.62	1.62
(% - sec)	99.99999 - 3.23	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	34.96	
Atenuación por Lluvia (dB)	34.96	
Fuera de Servicio Anual por Lluvia (%-sec)	99.99993 - 23.33	
Total Anual (%-seg)	99.99992 - 26.56	

Lun, Ene 23 2012
ICTO CRUZ - BUERAN (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE BUERAN-CARSHAO

	BUERAN	CARSHAO
Elevación (m)	3793.44	3991.59
Latitud	02 35 46.31 S	02 26 11.22 S
Longitud	078 55 35.84 W	078 56 56.03 W
Azimuth Verdadero (°)	352.02	172.02
Ángulo Vertical (°)	0.58	-0.70
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	20.00	20.00
Ganancia de Antena (dBi)	37.46	37.46
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	17.84	
Pérdidas de Espacio Libre (dB)	135.00	
Pérdidas de Absorción Atmosférica (dB)	0.18	
Pérdidas Netas del Enlace (dB)	68.40	68.40
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	63.38	63.38
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-38.40	-38.40
Margen de Desv. - Térmico (dB)	38.60	38.60
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	11.11	
Fade occurrence factor (Po)	1.46E-05	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	100.00000	100.00000
(sec)	0.02	0.02
Fuera de Servicio Anual por Multitrayecto (%)	100.00000	100.00000
(sec)	0.09	0.09
(% - sec)	100.00000 - 0.17	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	38.60	
Intensidad de Lluvia (mm/hr)	340.32	
Atenuación por Lluvia (dB)	38.60	
Fuera de Servicio Anual por Lluvia (%-sec)	99.99999 - 3.86	
Total Anual (%-seg)	99.99999 - 4.03	

Lun, Ene 23 2012
BUERAN - CARSHAO (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE BUERAN-PATOCOCHA

	BUERAN	PATOCOCHA
Elevación (m)	3793.44	3569.16
Latitud	02 35 58.30 S	03 01 07.00 S
Longitud	078 55 43.60 W	078 39 52.00 W
Azimuth Verdadero (°)	147.62	327.61
Ángulo Vertical (°)	-0.42	0.05
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	20.00	20.00
Ganancia de Antena (dBi)	45.50	45.50
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	54.88	
Pérdidas de Espacio Libre (dB)	144.76	
Pérdidas de Absorción Atmosférica (dB)	0.55	
Pérdidas Netas del Enlace (dB)	62.45	62.45
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	71.42	71.42
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-32.45	-32.45
Margen de Desv. - Térmico (dB)	44.55	44.55
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	4.09	
Fade occurrence factor (Po)	2.81E-03	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	99.99949	99.99949
(sec)	13.33	13.33
Fuera de Servicio Anual por Multitrayecto (%)	99.99981	99.99981
(sec)	60.00	60.00
(% - sec)	99.99962 - 120.01	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	52.41	
Margen de Desv. - Plano por Lluvia (dB)	44.55	
Atenuación por Lluvia (dB)	44.55	
Fuera de Servicio Anual por Lluvia (%-sec)	100.00000 - 0.74	
Total Anual (%-seg)	99.99962 - 120.75	

Lun, Ene 23 2012
BUERAN - PATOCOCHA (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE PATOCOCHA-CERRO BOSCO

	CERRO BOSCO	PATOCOCHA
Elevación (m)	2371.93	3569.17
Latitud	03 00 02.00 S	03 01 07.00 S
Longitud	078 30 35.00 W	078 39 52.00 W
Azimuth Verdadero (°)	263.38	83.38
Ángulo Vertical (°)	3.90	-4.01
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	26.00	26.00
Ganancia de Antena (dBi)	41.00	41.00
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	17.32	
Pérdidas de Espacio Libre (dB)	134.74	
Pérdidas de Absorción Atmosférica (dB)	0.17	
Pérdidas Netas del Enlace (dB)	61.06	61.06
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	66.92	66.92
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-31.06	-31.06
Margen de Desv. - Térmico (dB)	45.94	45.94
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	69.03	
Fade occurrence factor (Po)	1.13E-06	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	100.00000	100.00000
(sec)	1.92e-03	1.92e-03
Fuera de Servicio Anual por Multitrayecto (%)	100.00000	100.00000
(sec)	8.65e-03	8.65e-03
(% - sec)	100.00000 - 0.02	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	52.41	
Margen de Desv. - Plano por Lluvia (dB)	45.94	
Atenuación por Lluvia (dB)	45.94	
Fuera de Servicio Anual por Lluvia (%-sec)	100.00000 - 0.00	
Total Anual (%-seg)	100.00000 - 0.02	

Lun, Ene 23 2012
PATOCOCHA-CERRO BOSCO (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE BUERAN-PORTETE

	BUERAN	PORTETE
Elevación (m)	3793.44	3196.06
Latitud	02 35 46.31 S	03 07 44.50 S
Longitud	078 55 35.83 W	079 04 35.82 W
Azimuth Verdadero (°)	195.80	15.81
Ángulo Vertical (°)	-0.77	0.35
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	28.00	28.00
Ganancia de Antena (dBi)	45.50	45.50
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	61.23	
Pérdidas de Espacio Libre (dB)	145.71	
Pérdidas de Absorción Atmosférica (dB)	0.61	
Pérdidas Netas del Enlace (dB)	63.47	63.47
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	71.42	71.42
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-33.47	-33.47
Margen de Desv. - Térmico (dB)	43.53	43.53
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	9.76	
Fade occurrence factor (Po)	1.46E-03	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	99.99959	99.99959
(sec)	10.83	10.83
Fuera de Servicio Anual por Multitrayecto (%)	99.99985	99.99985
(sec)	48.72	48.72
(% - sec)	99.99969 - 97.44	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	43.53	
Intensidad de Lluvia (mm/hr)	304.99	
Atenuación por Lluvia (dB)	43.53	
Fuera de Servicio Anual por Lluvia (%-sec)	99.99997 - 10.18	
Total Anual (%-seg)	99.99966 - 107.62	

Lun, Ene 23 2012
BUERAN - PORTETE (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE PORTETE-CHILLA

	CHILLA	PORTETE
Elevación (m)	3509.43	3196.06
Latitud	03 29 58.57 S	03 07 56.49 S
Longitud	079 37 53.93 W	079 04 43.61 W
Azimuth Verdadero (°)	56.55	236.52
Ángulo Vertical (°)	-0.49	-3.39e-03
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	28.00	26.00
Ganancia de Antena (dBi)	45.50	45.50
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	73.65	
Pérdidas de Espacio Libre (dB)	147.31	
Pérdidas de Absorción Atmosférica (dB)	0.74	
Pérdidas Netas del Enlace (dB)	65.20	65.20
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	71.42	71.42
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-35.20	-35.20
Margen de Desv. - Térmico (dB)	41.80	41.80
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	4.28	
Fade occurrence factor (Po)	7.69E-03	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	99.99768	99.99768
(sec)	61.04	61.04
Fuera de Servicio Anual por Multitrayecto (%)	99.99913	99.99913
(sec)	274.68	274.68
(% - sec)	99.99826 - 549.36	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	41.80	
Intensidad de Lluvia (mm/hr)	291.64	
Atenuación por Lluvia (dB)	41.80	
Fuera de Servicio Anual por Lluvia (%-sec)	99.99995 - 14.69	
Total Anual (%-seg)	99.99821 - 564.05	

Lun, Ene 23 2012
CHILLA - PORTETE (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE CHILLA-MOTILON

	CHILLA	MOTILON
Elevación (m)	3509.44	2635.17
Latitud	03 29 58.57 S	04 04 58.89 S
Longitud	079 37 53.93 W	079 56 29.44 W
Azimuth Verdadero (°)	208.07	28.09
Ángulo Vertical (°)	-0.93	0.44
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	26.00	28.00
Ganancia de Antena (dBi)	45.50	45.50
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	73.12	
Pérdidas de Espacio Libre (dB)	147.25	
Pérdidas de Absorción Atmosférica (dB)	0.73	
Pérdidas Netas del Enlace (dB)	65.13	65.13
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	71.42	71.42
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-35.13	-35.13
Margen de Desv. - Térmico (dB)	41.87	41.87
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	11.93	
Fade occurrence factor (Po)	2.14E-03	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	99.99913	99.99913
(sec)	22.85	22.85
Fuera de Servicio Anual por Multitrayecto (%)	99.99967	99.99967
(sec)	102.84	102.84
(% - sec)	99.99935 - 205.68	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	41.87	
Intensidad de Lluvia (mm/hr)	292.14	
Atenuación por Lluvia (dB)	41.87	
Fuera de Servicio Anual por Lluvia (%-sec)	99.99995 - 14.49	
Total Anual (%-seg)	99.99930 - 220.17	

Lun, Ene 23 2012
CHILLA - MOTILON (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE MOTILON-VILLONACO

	VILLONACO	MOTILON
Elevación (m)	2895.67	2635.17
Latitud	03 59 18.19 S	04 04 58.89 S
Longitud	079 16 06.78 W	079 56 29.44 W
Azimuth Verdadero (°)	262.00	82.05
Ángulo Vertical (°)	-0.45	-0.06
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	28.00	26.00
Ganancia de Antena (dBi)	45.50	45.50
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	75.46	
Pérdidas de Espacio Libre (dB)	147.52	
Pérdidas de Absorción Atmosférica (dB)	0.75	
Pérdidas Netas del Enlace (dB)	65.43	65.43
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	71.42	71.42
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-35.43	-35.43
Margen de Desv. - Térmico (dB)	41.57	41.57
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	3.48	
Fade occurrence factor (Po)	1.06E-02	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	99.99686	99.99686
(sec)	82.61	82.61
Fuera de Servicio Anual por Multitrayecto (%)	99.99882	99.99882
(sec)	371.77	371.77
(% - sec)	99.99764 - 743.53	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	41.57	
Intensidad de Lluvia (mm/hr)	289.98	
Atenuación por Lluvia (dB)	41.57	
Fuera de Servicio Anual por Lluvia (%-sec)	99.99995 - 15.38	
Total Anual (%-seg)	99.99759 - 758.91	

Lun, Ene 23 2012
VILLONACO - MOTILON (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE MOTILON-MORUPE

	MORUPE	MOTILON
Elevación (m)	2644.16	2635.17
Latitud	04 22 14.90 S	04 04 58.89 S
Longitud	079 43 07.40 W	079 56 29.44 W
Azimuth Verdadero (°)	322.14	142.15
Ángulo Vertical (°)	-0.15	-0.12
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	28.00	24.00
Ganancia de Antena (dBi)	43.50	43.50
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	40.30	
Pérdidas de Espacio Libre (dB)	142.08	
Pérdidas de Absorción Atmosférica (dB)	0.40	
Pérdidas Netas del Enlace (dB)	63.63	63.63
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	69.42	69.42
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-33.63	-33.63
Margen de Desv. - Térmico (dB)	43.37	43.37
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	0.32	
Fade occurrence factor (Po)	6.10E-03	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	99.99957	99.99957
(sec)	11.21	11.21
Fuera de Servicio Anual por Multitrayecto (%)	99.99984	99.99984
(sec)	50.45	50.45
(% - sec)	99.99968 - 100.90	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	43.37	
Intensidad de Lluvia (mm/hr)	318.62	
Atenuación por Lluvia (dB)	43.37	
Fuera de Servicio Anual por Lluvia (%-sec)	99.99998 - 7.00	
Total Anual (%-seg)	99.99966 - 107.90	

Lun, Ene 23 2012
MOTILON-MORUPE (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

RED REDUNDANTE
ENLACE BUERAN-SEÑOR PUNGO

	BUERAN	SEÑOR PUNGO
Elevación (m)	3793.44	3139.48
Latitud	02 35 58.30 S	02 48 19.60 S
Longitud	078 55 43.60 W	078 49 19.00 W
Azimuth Verdadero (°)	152.45	332.45
Ángulo Vertical (°)	-1.55	1.37
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	28.00	28.00
Ganancia de Antena (dBi)	43.50	43.50
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	25.68	
Pérdidas de Espacio Libre (dB)	138.16	
Pérdidas de Absorción Atmosférica (dB)	0.26	
Pérdidas Netas del Enlace (dB)	59.57	59.57
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	69.42	69.42
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-29.57	-29.57
Margen de Desv. - Térmico (dB)	47.43	47.43
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	25.46	
Fade occurrence factor (Po)	1.82E-05	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	100.00000	100.00000
(sec)	0.04	0.04
Fuera de Servicio Anual por Multitrayecto (%)	100.00000	100.00000
(sec)	0.19	0.19
(% - sec)	100.00000 - 0.38	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	47.43	
Intensidad de Lluvia (mm/hr)	375.97	
Atenuación por Lluvia (dB)	47.43	
Fuera de Servicio Anual por Lluvia (%-sec)	100.00000 - 1.45	
Total Anual (%-seg)	99.99999 - 1.83	

Lun, Ene 23 2012
BUERAN-SEÑOR PUNGO (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE SEÑOR PUNGO-ICTO CRUZ

	ICTO CRUZ	SEÑOR PUNGO
Elevación (m)	2832.73	3139.48
Latitud	02 55 51.60 S	02 48 19.60 S
Longitud	078 59 51.70 W	078 49 19.00 W
Azimuth Verdadero (°)	54.61	234.60
Ángulo Vertical (°)	0.65	-0.81
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	28.00	28.00
Ganancia de Antena (dBi)	43.50	43.50
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	23.97	
Pérdidas de Espacio Libre (dB)	137.56	
Pérdidas de Absorción Atmosférica (dB)	0.24	
Pérdidas Netas del Enlace (dB)	58.95	58.95
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	69.42	69.42
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-28.95	-28.95
Margen de Desv. - Térmico (dB)	48.05	48.05
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	12.80	
Fade occurrence factor (Po)	3.53E-05	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	100.00000	100.00000
(sec)	0.06	0.06
Fuera de Servicio Anual por Multitrayecto (%)	100.00000	100.00000
(sec)	0.26	0.26
(% - sec)	100.00000 - 0.53	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	48.05	
Intensidad de Lluvia (mm/hr)	389.82	
Atenuación por Lluvia (dB)	48.05	
Fuera de Servicio Anual por Lluvia (%-sec)	100.00000 - 0.99	
Total Anual (%-seg)	100.00000 - 1.52	

Lun, Ene 23 2012
ICTO CRUZ-SEÑOR PUNGO (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE SEÑOR PUNGO-SIMBALA

	SEÑOR PUNGO	SIMBALA
Elevación (m)	3139.51	3147.56
Latitud	02 48 19.60 S	03 08 12.90 S
Longitud	078 49 19.00 W	079 05 09.90 W
Azimuth Verdadero (°)	218.69	38.71
Ángulo Vertical (°)	-0.13	-0.19
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	28.00	45.00
Ganancia de Antena (dBi)	43.50	43.50
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	46.97	
Pérdidas de Espacio Libre (dB)	143.40	
Pérdidas de Absorción Atmosférica (dB)	0.47	
Pérdidas Netas del Enlace (dB)	65.02	65.02
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	69.42	69.42
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-35.02	-35.02
Margen de Desv. - Térmico (dB)	41.98	41.98
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	0.53	
Fade occurrence factor (Po)	8.60E-03	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	99.99918	99.99918
(sec)	21.58	21.58
Fuera de Servicio Anual por Multitrayecto (%)	99.99969	99.99969
(sec)	97.13	97.13
(% - sec)	99.99938 - 194.26	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	41.98	
Intensidad de Lluvia (mm/hr)	304.93	
Atenuación por Lluvia (dB)	41.98	
Fuera de Servicio Anual por Lluvia (%-sec)	99.99997 - 10.20	
Total Anual (%-seg)	99.99935 - 204.46	

Lun, Ene 23 2012
SEÑOR PUNGO-SIMBALA (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE SEÑOR PUNGO- PATOCOCHA

	SEÑOR PUNGO	PATOCOCHA
Elevación (m)	3139.47	3569.17
Latitud	02 48 19.60 S	03 01 07.00 S
Longitud	078 49 19.00 W	078 39 52.00 W
Azimuth Verdadero (°)	143.40	323.39
Ángulo Vertical (°)	0.74	-0.93
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	26.00	24.00
Ganancia de Antena (dBi)	41.00	41.00
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	29.36	
Pérdidas de Espacio Libre (dB)	139.32	
Pérdidas de Absorción Atmosférica (dB)	0.29	
Pérdidas Netas del Enlace (dB)	65.77	65.77
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	66.92	66.92
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-35.77	-35.77
Margen de Desv. - Térmico (dB)	41.23	41.23
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	14.56	
Fade occurrence factor (Po)	6.19E-05	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	99.99999	99.99999
(sec)	0.16	0.16
Fuera de Servicio Anual por Multitrayecto (%)	100.00000	100.00000
(sec)	0.72	0.72
(% - sec)	100.00000 - 1.43	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	41.23	
Intensidad de Lluvia (mm/hr)	321.60	
Atenuación por Lluvia (dB)	41.23	
Fuera de Servicio Anual por Lluvia (%-sec)	99.99998 - 6.45	
Total Anual (%-seg)	99.99997 - 7.89	

Lun, Ene 23 2012
SEÑOR PUNGO- PATOCOCHA (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE SIMBALA-JARATA

	JARATA	SIMBALA
Elevación (m)	3420.03	3147.57
Latitud	03 18 52.60 S	03 08 12.90 S
Longitud	079 07 52.70 W	079 05 09.90 W
Azimuth Verdadero (°)	14.35	194.35
Ángulo Vertical (°)	-0.84	0.70
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	28.00	28.00
Ganancia de Antena (dBi)	41.00	41.00
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	20.28	
Pérdidas de Espacio Libre (dB)	136.11	
Pérdidas de Absorción Atmosférica (dB)	0.20	
Pérdidas Netas del Enlace (dB)	62.46	62.46
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	66.92	66.92
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-32.46	-32.46
Margen de Desv. - Térmico (dB)	44.54	44.54
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	13.43	
Fade occurrence factor (Po)	1.81E-05	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	100.00000	100.00000
(sec)	0.02	0.02
Fuera de Servicio Anual por Multitrayecto (%)	100.00000	100.00000
(sec)	0.11	0.11
(% - sec)	100.00000 - 0.22	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	44.54	
Intensidad de Lluvia (mm/hr)	376.25	
Atenuación por Lluvia (dB)	44.54	
Fuera de Servicio Anual por Lluvia (%-sec)	100.00000 - 1.44	
Total Anual (%-seg)	99.99999 - 1.66	

Lun, Ene 23 2012
JARATA-SIMBALA (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE SARAGURO-VILLONACO

	VILLONACO	SARAGURO
Elevación (m)	2895.74	3282.77
Latitud	03 59 18.19 S	03 38 30.30 S
Longitud	079 16 06.78 W	079 15 34.20 W
Azimuth Verdadero (°)	1.50	181.50
Ángulo Vertical (°)	0.45	-0.71
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	50.00	50.00
Ganancia de Antena (dBi)	43.50	43.50
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	38.34	
Pérdidas de Espacio Libre (dB)	141.64	
Pérdidas de Absorción Atmosférica (dB)	0.38	
Pérdidas Netas del Enlace (dB)	63.18	63.18
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	69.42	69.42
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-33.18	-33.18
Margen de Desv. - Térmico (dB)	43.82	43.82
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	10.09	
Fade occurrence factor (Po)	2.60E-04	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	99.99997	99.99997
(sec)	0.89	0.89
Fuera de Servicio Anual por Multitrayecto (%)	99.99999	99.99999
(sec)	4.01	4.01
(% - sec)	99.99997 - 8.03	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	43.82	
Intensidad de Lluvia (mm/hr)	323.50	
Atenuación por Lluvia (dB)	43.82	
Fuera de Servicio Anual por Lluvia (%-sec)	99.99998 - 6.13	
Total Anual (%-seg)	99.99996 - 14.15	

Lun, Ene 23 2012
VILLONACO-SARAGURO (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE JARATA-SARAGURO

	SARAGURO	JARATA
Elevación (m)	3282.76	3420.02
Latitud	03 38 30.30 S	03 18 52.60 S
Longitud	079 15 34.20 W	079 07 52.70 W
Azimuth Verdadero (°)	21.50	201.49
Ángulo Vertical (°)	0.07	-0.33
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	28.00	28.00
Ganancia de Antena (dBi)	43.50	43.50
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	38.88	
Pérdidas de Espacio Libre (dB)	141.76	
Pérdidas de Absorción Atmosférica (dB)	0.39	
Pérdidas Netas del Enlace (dB)	63.30	63.30
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	69.42	69.42
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-33.30	-33.30
Margen de Desv. - Térmico (dB)	43.70	43.70
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	3.53	
Fade occurrence factor (Po)	9.56E-04	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	99.99991	99.99991
(sec)	2.49	2.49
Fuera de Servicio Anual por Multitrayecto (%)	99.99996	99.99996
(sec)	11.18	11.18
(% - sec)	99.99993 - 22.37	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	43.70	
Intensidad de Lluvia (mm/hr)	322.12	
Atenuación por Lluvia (dB)	43.70	
Fuera de Servicio Anual por Lluvia (%-sec)	99.99998 - 6.36	
Total Anual (%-seg)	99.99991 - 28.73	

Lun, Ene 23 2012
SARAGURO-JARATA (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE JARATA-PUCARA

	JARATA	PUCARA
Elevación (m)	3420.03	3534.38
Latitud	03 18 52.60 S	03 12 39.20 S
Longitud	079 07 52.70 W	079 30 14.50 W
Azimuth Verdadero (°)	285.47	105.49
Ángulo Vertical (°)	7.27e-03	-0.30
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	28.00	28.00
Ganancia de Antena (dBi)	43.50	43.50
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	42.98	
Pérdidas de Espacio Libre (dB)	142.63	
Pérdidas de Absorción Atmosférica (dB)	0.43	
Pérdidas Netas del Enlace (dB)	64.21	64.21
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	69.42	69.42
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-34.21	-34.21
Margen de Desv. - Térmico (dB)	42.79	42.79
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	2.66	
Fade occurrence factor (Po)	1.85E-03	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	99.99980	99.99980
(sec)	5.32	5.32
Fuera de Servicio Anual por Multitrayecto (%)	99.99992	99.99992
(sec)	23.94	23.94
(% - sec)	99.99985 - 47.87	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	42.79	
Intensidad de Lluvia (mm/hr)	312.65	
Atenuación por Lluvia (dB)	42.79	
Fuera de Servicio Anual por Lluvia (%-sec)	99.99997 - 8.25	
Total Anual (%-seg)	99.99982 - 56.12	

Lun, Ene 23 2012
JARATA-PUCARA (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ENLACE PUCARA-CHILLA

	PUCARA	CHILLA
Elevación (m)	3534.38	3509.60
Latitud	03 12 39.20 S	03 29 58.59 S
Longitud	079 30 14.50 W	079 37 53.93 W
Azimuth Verdadero (°)	203.95	23.96
Ángulo Vertical (°)	-0.16	-0.08
Modelo de Antena	PARABOLICA	PARABOLICA
Altura de Antena (m)	28.00	28.00
Ganancia de Antena (dBi)	43.50	43.50
Tipo de Línea de TX	RG-213	RG-213
Longitud de Línea de TX (m)	35.00	35.00
Pérdida Unitaria en Línea de TX (dB /100 m)	4.50	4.50
Pérdida en Línea de TX (dB)	1.57	1.57
Pérdida en Conectores (dB)	1.00	1.00
Pérdidas Misceláneas (dB)	1.50	1.50
Otras Pérdidas TX (dB)	0.00	0.00
Otras Pérdidas RX (dB)	0.00	0.00
Frecuencia (MHz)	7500.00	
Polarización	Vertical	
Longitud de la Trayectoria (km)	34.93	
Pérdidas de Espacio Libre (dB)	140.83	
Pérdidas de Absorción Atmosférica (dB)	0.35	
Pérdidas Netas del Enlace (dB)	62.33	62.33
Modelo de Radio	SAF 7 GHz	SAF 7 GHz
Potencia de Transmisión (w)	1.00	1.00
Potencia de Transmisión (dBm)	30.00	30.00
PIRE (dBm)	69.42	69.42
Designador de Emisor	CFIP 100Mbps	CFIP 100Mbps
Criterio de Umbral de Recepción	BER 10-6	BER 10-6
Nivel de Umbral (dBm)	-77.00	-77.00
Señal Recibida (dBm)	-32.33	-32.33
Margen de Desv. - Térmico (dB)	44.67	44.67
Factor Geoclimático	2.50E-07	
Inclinación del Trayecto (mr)	0.71	
Fade occurrence factor (Po)	2.55E-03	
Temperatura Anual Promedio (°C)	27.00	
Fuera de Servicio del Peor Mes por Multitrayecto (%)	99.99985	99.99985
(sec)	3.98	3.98
Fuera de Servicio Anual por Multitrayecto (%)	99.99994	99.99994
(sec)	17.91	17.91
(% - sec)	99.99989 - 35.83	
Región de Precipitación	ITU Region N	
0.01% Intensidad de Lluvia (mm/hr)	95.00	
Margen de Desv. - Plano por Lluvia (dB)	44.67	
Intensidad de Lluvia (mm/hr)	333.27	
Atenuación por Lluvia (dB)	44.67	
Fuera de Servicio Anual por Lluvia (%-sec)	99.99999 - 4.68	
Total Anual (%-seg)	99.99987 - 40.51	

Lun, Ene 23 2012
PUCARA-CHILLA (SAF CFIP 100 Mbps).pl4
Reliability Method - Rec. ITU-R P.530-7/8
Precipitación - ITU-R P530-7

ANEXOS 2

CFIP PhoeniX IDU

Modem	
Channel Bandwidths	7, 14, 28, 40, 56 MHz
Modulations	QPSK, 16APSK, 32APSK, 64QAM, 128QAM, 256QAM
Capacity	9 - 366 Mbps
Supported ODUs	CFIP ODU*; CFQ ODU (SB, WB*)
Applications	
Configuration	1+0, 1+1*
Protection switching*	Hot Stand-by (hitless, errorless; Active Tx <50ms), Space/Frequency diversity
Ports	
Ethernet	4x1000Base-T, RJ-45
E1/T1	20 E1/T1, RJ-45
Serial port for configuration	RS-232, DB-9 connector
Alarm port	4 digital inputs, 4 relay outputs (26 pin hi-density D-SUB)
ODU port	N-Type Female
EOW port	3.5mm headset and mic, 64 Kbps
Extension/protection port	RJ-45
Management features	
Management port	Ethernet with VLAN support or serial (RS-232)
Monitoring	via Telnet, WEB GUI, NMS, SNMP Manager, Serial interface
SNMP	Yes, SNMP traps, MIB, SNMP v1/v2c
EMS	Web based, HTTP
Ethernet	
QoS/CoS	64 level DiffServ (DSCP) or 8 level 802.1p mapped in 4 prioritization queues with VLAN support
Max frame size	9728 bytes
Flow Control	Yes
802.1q VLAN support	Up to 4093 concurrent traffic VLANs
Mechanical & Electrical	
Temperature Range / Humidity	-5°C to +45°C / 5% to 95%
Dimensions: HxWxD, mm / weight, kg	1U (45x430x240) / 3.1
Max. power consumption	20-30W
IDU-ODU connection	Belden 9914/RG-8 cable (300 m), RG213 cable (200 m), N-Type connectors
DC port	-40.5V to -57V DC (conforms to ETSI EN 300 132-2)

CFIP ODU RSL at 10^{-6} (dBm) and Total Payload Capacity (Mbps)**											
Modulation	FEC	Channel bandwidth (MHz)									
		7		14		28		40*		56*	
		RSL dBm	Bit rate Mbps	RSL dBm	Bit rate Mbps	RSL dBm	Bit rate Mbps	RSL dBm	Bit rate Mbps	RSL dBm	Bit rate Mbps
QPSK	Strong	-93	8.7	-91	17	-88	34	-87	48	-85	71
	Weak	-91	10.4	-88	21	-85	43	-83	60	-81	89
16APSK	Strong	-87	17.3	-84	34	-82	69	-80	97	-77	143
	Weak	-84	20.5	-81	42	-79	84	-77	119	-74	176
32APSK	Strong	-84	21.6	-81	43	-79	86	-78	121	-76	179
	Weak	-80	25.8	-78	52	-76	104	-74	146	-73	216
64QAM	Strong	-81	28.8	-79	57	-76	115	-75	162	-73	239
	Weak	-77	32.4	-76	65	-73	131	-71	185	-69	273
128QAM	Strong	—		-76	69	-73	138	-72	194	-70	286
	Weak	—		-73	76	-70	153	-68	216	-67	319
256QAM	Strong	—		-73	80	-70	161	-68	226	-66	334
	Weak	—		-69	88	-66	176	-65	248	-62	366

CFIP ODU Tx Power					
Modulation	Standard/High Tx Power, dBm				
	7*, 8* GHz	10*, 11*, 13, 15 GHz	18*, 23, 26* GHz	24* GHz	38* GHz
QPSK	+19 / +27	+19 / +25	+19	+5	+17
16APSK	+18 / +26	+18 / +24	+18	+4	+16
32APSK	+17 / +25	+17 / +23	+17	+3	+15
64QAM	+15 / +23	+15 / +21	+15	+1	+13
128QAM	+14 / +22	+14 / +20	+14	0	+12
256QAM	+12 / +20	+12 / +17	+12	-2	+10

Modem	
Channel Bandwidth (MHz)	7 – 28; (7 - 56)*
Modulation	QPSK – 256QAM
Capacity (Mbps)	8 - 366
Supported ODUs	CFIP ODU*; CFQ ODU (SB, WB*)
Applications	
Configuration	1+0, 1+1*
Protection switching*	Hot stand-by (hitless, errorless; Active Tx <50ms), Space/Frequency diversity
Ports	
Ethernet	4x1000Base-T RJ-45
E1/T1	20 E1/T1 RJ-45
Serial port for configuration	RS-232, DB-9 connector
Alarm port	4 digital inputs, 4 relay outputs (26 pin hi-density D-SUB)
ODU port	N-Type Female
EOW port	3.5mm headset and mic, 64 Kbps
Extension/protection port	RJ-45
Management features	
Management port	Ethernet with VLAN support or serial (RS-232)
Monitoring	via Telnet, WEB GUI, NMS, SNMP Manager, Serial interface
SNMP	Yes, SNMP traps, MIB, SNMP v1/v2c
EMS	Web based, HTTP

ANEXOS 3

CABLE COAXIAL PARA BAJADA DE ANTENA RG-213 NORMAS MIL C-17F, CALIDAD EXTRA

Características técnicas y tabla comparativa:

Tipo	**Ohm**	**Factor Veloc**	**Tensión Máx RMS**	**pF por metro**	**Atenuación en dB por cada 100 mts**							**Diámetro en mm**
					10 Mhz	50 Mhz	100 mhz	200 Mhz	400 Mhz	800 Mhz	1 Ghz	
RG-58	50	0,66	1900	93	4,6	9,1	13,1	19,4	28,4	42,7	49,0	5
RG-213	50	0,66	5000	101	1,8	4,5	6,7	9,9	14,3	21,3	24,3	10,3

BIBLIOGRAFÍA

BARBERÁ, José, "*MPLS: Una arquitectura de backbone para la Internet del siglo XXI*"
http://www.rediris.es/rediris/boletin/53/enfoque1.html

D'SOUSA, Carmen, "*Tecnología Frame Relay*", mayo 2011
http://www.monografias.com/trabajos11/frame/frame.shtml

ISDN, "*Red digital de servicios integrados*", mayo 2011
http://www.frm.utn.edu.ar/comunicaciones/isdn.html

ISDN, "*Red digital de servicios integrados*", mayo 2011
http://personales.mundivia.es/jtoledo/angel/SE.HTM

OCHOA, Edgar, Material de la asignatura "*Comunicaciones III*", Universidad Politécnica Salesiana, 5 año.

PÉREZ, Jorge, y otros, "*Comparación entre IPV4 - IPV6*" , junio 2011
http://www.ilustrados.com/documentos/eb-Comparacion%20IP4%20y%20IPV6.pdf

"*Redes X.25*", mayo 2011
http://www.angelfire.com/wi/ociosonet/5.html

"*Redes ATM*", mayo 2011
http://www.angelfire.com/wi/ociosonet/29.html

SOTO, Miguel, "Protocolo *TCP/IP*", mayo 2011
http://usuarios.multimania.es/janjo/janjo1.html

TRAVERSO, Damián, "*Tecnologías en las Redes de Acceso*", junio 2011
http://www.monografias.com/trabajos13/tecnacc/tecnacc.shtml

VALERA, Isabel, "*Tecnología DSL*", junio 2011
http://www.monografias.com/trabajos5/tecdsl/tecdsl.shtml

VELÁSQUEZ, Ana y SAINEA, Fabio **"***Cabecera IPv6"*, junio 2011
http://www.dei.uc.edu.py/tai2003/ipv6/cabecera.htm

WIKIPEDIA**,** IP, "*Protocolo de Internet*", junio 2011
http://es.wikipedia.org/wiki/Internet_Protocol

WIKIPEDIA**,** "*Cabecera IP*", junio 2011
http://es.wikipedia.org/wiki/Cabecera_IP

WIKIPEDIA**,** "*Dirección IP*", junio 2011
http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP

WIKIPEDIA**,** IPv6, "*Protocolo de Internet Versión 6*", junio 2011
http://es.wikipedia.org/wiki/IPv6

WIKIPEDIA, ATM, "*Modo de Transferencia Asíncrona*", mayo 2011
http://es.wikipedia.org/wiki/Asynchronous_Transfer_Mode

WIKIPEDIA, SDH, "*Jerarquía Digital Síncrona*", mayo 2011
http://es.wikipedia.org/wiki/Jerarqu%C3%ADa_digital_s%C3%ADncrona

WIKIPEDIA,TDMA, "*Multiplexación por División de Tiempo,* mayo 2011
http://es.wikipedia.org/wiki/Acceso_m%C3%BAltiple_por_divisi%C3%B3n_de_tiempo

WIKIPEDIA, "*Norma X.25*", mayo 2011
http://es.wikipedia.org/wiki/Norma_X.25

WIKIPEDIA, "*Jerarquía Digital Plesiocrona*", mayo 2011
http://es.wikipedia.org/wiki/Jerarqu%C3%ADa_Digital_Plesi%C3%B3crona

ALLER, Conchi y otros, "*Redes Metro Ethernet*", julio 2011
http://www.coit.es/publicaciones/bit/bit149/64-66.pdf

CARREON, Roberto, *"Redes Privadas Virtuales"*, julio 2011
http://www.monografias.com/trabajos11/repri/repri.shtml

FLORES, Ricardo y GONZÁLEZ, Santiago, *"Protocolo múltiple por conmutación de etiquetas (MPLS): fundamentos y aplicaciones"*, Tesis Universidad Politécnica Salesiana, Cuenca, nov-2006
http://dspace.ups.edu.ec/bitstream/123456789/209/3/Capitulo%202.pdf

HEVIA, Mariano, *"Virtual Private Networks (VPN)"*, julio 2011
http://www.monografias.com/trabajos12/monvpn/monvpn.shtml

LIMA, Servio, *"Las redes de Área Metropolitana basadas en Ethernet en el Ecuador"*, julio 2011
http://www.docstoc.com/docs/25917668/LAS-REDES-DE-AREA-METROPOLITANA-BASADAS- EN-ETHERNET-EN

MAYA, Marcela y otros, *"Metro Ethernet"*, julio 2011
http://www.monografias.com/trabajos17/metro-ethernet/metro-ethernet.shtml

"*METRO ETHERNET Y MPLS"*, Escuela Politécnica Nacional
http://dspace.epn.edu.ec/bitstream/15000/8678/5/capitulo_2.pdf

SILVESTRE, Kelvin, *"Estudio de las ventajas e implementación de servicios IP VPN, sobre una infraestructura MPLS en la Región Centroamericana"*, Tesis Universidad de San Carlos de Guatemala, nov - 2008

http://biblioteca.usac.edu.gt/tesis/08/08_0221_EO.pdf

"*Tendencia en Tecnologías Ethernet Metropolitanas"*, julio 2011
http://sistemas.itlp.edu.mx/ponencias/3.pdf

WIKIPEDIA, *"CHAP",* agosto 2011
http://es.wikipedia.org/wiki/CHAP

WIKIPEDIA**,** "*Redes Privadas Virtuales"*, julio 2011
http://es.wikipedia.org/wiki/Red_privada_virtual

WIKIPEDIA**,** "*Redes Metro Ethernet*", julio 2011
http://es.wikipedia.org/wiki/Metro_Ethernet

WIKIPEDIA, *"RSA"*, agosto 2011
http://es.wikipedia.org/wiki/RSA

WIKIPEDIA, *"Multiprotocol Label Switching",* Agosto 2011
http://es.wikipedia.org/wiki/Multiprotocol_Label_Switching

"*CFIP PhoeniX ODU "*, septiembre 2011
www.technicalbase.com.ar/PDFs/WirelessNetworking/CFQ_productline_esp.pdf

"*Customized Microwave Solutions* **"**
https://www.saftehnika.com/upload/File/Siebel/201005013_SAF_CFIP_CFQ_brochure_Esp.pdf

"*COMHAT TECHNICAL DATA ANTENNA*", octubre 2011
http://www.ultratelecom.kiev.ua/catalog/%287GHz,1.2m%29200412271549502 51901-HAA0712_00-PA3.pdf

DUQUE, Darío, *"Estudio para la migración del sistema troncalizado de la fuerza terrestre del Ecuador de una plataforma smartzone a una plataforma APCO P25 IP"*, ESPE / 2010
http://www3.espe.edu.ec:8700/bitstream/21000/2634/1/T-ESPE-029866.pdf

LOZADA, Diego y VEGA, Marcia *" Diseño de una Red de alta capacidad para el Enlace Quito – Lago Agrio utilizando radios SDH para el transporte de datos"*
http://dspace.epn.edu.ec/bitstream/15000/10359/2/T12006_paper.pdf

"*Polycom VideoConfenrencing",* octubre 2011
http://www.videoconferencia.es/polycom.html

"Polycom® QDX 6000", noviembre 2011
http://latinamerica.polycom.com/products/telepresence_video/video_conference_systems/room_systems/qdx6000.html

"*Protocolos utilizados para las redes de Nueva Generación"*
http://dspace.epn.edu.ec/bitstream/15000/8712/1/T10902ANEXOS.pdf

RAMOS, Henry, *"VoIP Corporación Nacional de Telecomunicaciones CNT S.A Diseño"*, Tesis Universidad Politecnica Salesiana, Cuenca, septiembre 2009
http://hdl.handle.net/123456789/32

"*Router Cisco 3800"*, diciembre 2011
http://www.router-switch.com/Cisco-Price-cisco-routers-cisco-router-3800-

SACA, Angel, *"Diseño del Sistema de Vigilanciacon cámaras IP para el EdificioMatriz de Petroecuador"*, Escuela Politecnica Nacional, marzo 2010
bibdigital.epn.edu.ec/bitstream/15000/2162/1/CD-2919.pdf

SOFTWARE, *"IP Video System Design Tool"*, diciembre 2011

http://www.jvsg.com/es/

SOFTWARE, *"Calculadora Erlgan-B"*, diciembre 2011

http://personal.telefonica.terra.es/web/vr/erlang/cerlangb.htm

SOFTWARE, *"Calculadora ancho de banda VoIP"*, diciembre 2011

http://www.idris.com.ar/BWCalc/

"Teléfono IP Linksys SPA942", diciembre 2011

http://www.inphonex.es/productos/linksys-spa942.php

WIKIPEDIA, *"Voz sobre Protocolo de Internet",* diciembre 2011

http://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet

WIKIPEDIA, *"Videovigilancia IP"*, noviembre 2011

http://es.wikipedia.org/wiki/V%C3%ADdeovigilancia_IP

ACRÓNIMOS

AAL	ATM Adaptation Layer
ABR	Available Bit Rate
ADSL	Asymmetric Digital Subscriber Line
ARP	Address Resolution Protocol
ARS	Ruteo automático de llamadas
ASDM	Adaptive Security Device Manager
ATM	Modo De Transferencia Asíncrono
AU	Unidad Administrativa
Bc	Committed Burst
Be	Excess Burst
BRI	Acceso Básico
C	Contenedor
CBR	Constant Bit Rate
CCTV	Circuito Cerrado de Televisión
CE	Customer Equipment
CHAP	Challenge Handshake Authentication Protocol
CIR	Commited Information Rate
CLP	Cell Loss Priority
CoS	Clases De Servicios Ethernet
CR-LDP	Constraint-based Routed Label Distribution Protocol
CS	Convergence Sublayer
DCE	Data Circuit Terminating Equipment
DHCPv6	Dynamic Host Configuration Protocol
DLL	Data Link Layer
DNS	Domain Name Service
DTE	Data Terminal Equipment
E-LAN	Multipunto a Multipunto
E-Line	Punto a Punto
EoMPLS	Ethernet Over MPLS

EVC	Ethernet Virtual Connection
FEC	Forwarding Equivalence Class
FPS	Frames por segundo
FTP	Protocolo de transferencia de ficheros
GFC	Generic Flow Control
GRE	Generic Routing Encapsulation
HD	High Definition
HDSL	High-bit-rate DSL
HDSL2 o SHDSL	High Bit-rate DSL 2
HTTP	Hypertext Transfer Protocol
HTTPS	Protocolo de transferencia de hipertexto sobre capa de sockets seguros
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol v6
IDSL	ISDN Digital Subscriber Line
IGMP	Internet Group Management Protocol
IGP	Internal Gateway Protocol
IHL	Internet Header Length
IntServ	Servicios Integrados
IP	Protocolo De Internet
IPsec	Internet Protocol Security
IPv4	Protocolo De Internet Version 4
IPv6	Protocolo De Internet Version 6
ISP	Proveedores De Internet
L2FP	Fowarding Protocol
LDP	Label Distribution Protocol
LDP	Label Distribution Protocol
LER	Label Edge Router
LIB	Label Information Base
LIFO	Last In, First Out
LLC	Link Logical Control

LSC	Label Switch Controlled
LSP	Label Switched Path
LSP	Label Switched Path
LSR	Label Switched Router
Lt	Longitud de Trama
MCR	Minimum Cell Rate
MEF	Metro Ethernet Forum
MEN	Metro Ethernet Network
MGCP	control de compuertas para medios
MPLS	Multiprotocol Label Switching
MSOH	Multiplexacion SOH
NM	Network manager
NNI	Network Network Interface
NVR	Network Video Recorders
OPTIS	Overlapped Phase Trellis-Code Interlocked Spectrum
OSI	Open System Interconnection
OSPF	Open Shortest Path First
OSPF	Open Shortest Path First
PAD	Relleno De Longitud Variable
PCM	Pulse Code Modulation
PCR	Peak Cell Rate
PCR	Peak Cell Rate
PDH	Jerarquía digital plesiócrona
PDU	Unidad de Protocolo de Datos
PE	Router de Borde de Red del Proveedor
ISP	Proveedor de Servicios
PHS	Per-hop behaviors
PPP	Point to Point Protocol
PPTP	Point to Point Tunneling Protocol
PPTP	Tunneling Protocol
PRI	Acceso Primario

PS	Physical Section
PSTN	Red Telefónica Pública Conmutada
PT	Payload Type
PTR	Puntero
PVC	Permanent Virtual Channel
PVC	Circuitos Virtuales Privados
PVC	Permanent Virtual Circuit
QoS	Calidad de Servicio
QPSK	Quadrature Phase Shift Keying
RADSL	Rate-Adaptive DSL
RARP	Reverse Address Resolution Protocol
RD	Identificador De Rutas
RDSI-ISDN	Red Digital De Servicios Integrados
RIP	Routing Information Protocol
RSA	Rivest, Shamir y Alemán
RSOH	Regeneracion SOH
RSTP	Protocolo de transmisión en tiempo real
RSVP-TE	Resource Reservation Protocol - Traffic Engineering
RT	Ruta Objetivo
RTCP	Real Time Control Protocol
RTP	Real Time Protocol
RTP	Real Time Protocol
rt-VBR	Real Time Variable Bit Rate
SAI	Sistema de Alimentación Interrumpida
SAR	Segmentation and Reassembly
SAR	Segmentation and Reassembly Sublayer
SCR	Sustained Cell Rate
SDH	Jerarquía Digital Síncrona
SDSL	Symmetric Digital Subscriber Line
SIP	Protocolo de Inicio de Sesión
SLA	Acuerdos de un Nivel de Servicio

SMTP	Protocolo simple de transferencia de correo
SOH	Tara de Seccion
SONET	Synchronous Optical Network
STM	Modulo de Transporte Síncrono
SVC	Switched Virtual Circuit
SVC	Switched Virtual Channel
TCP	Transmission control protocol
TCP	Protocolo De Control De Transmisión
TDM	Multiplexación Por División De Tiempo
TOS	Type of Service
ToS	Type of service
Tt	Tiempo de Trama
TTL	Time To Live
UBR	Unspecified Bit Rate
UBR	Unspecified Bit Rate
UDP	User datagram protocol
UDP	User Datagram Protocol
UDSL	Línea de Abonados Digital Pequeña
UNI	User Network Interfaz
UNI	User Network Interface
VBR	Variable Bit Traffic
VC	Circuitos Virtuales
VC	Contenedor Virtual
VC	Virtual Chanel
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VDSL	Very high rate DSL
Ver	Versión
VLAN	Redes de Área Local Virtual
VoIP	Voz sobre IP
VPC	Virtual Path Connection

VPI	Virtual Path Identifier
VPN	Virtual private network
VRF	Virtual Routing and Forwarding
VRF	VPN routing forwarding
WAN	Redes De Área Amplia
xDSL	Digital Subscriber Line