ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO DE UNA RED TRONCAL EN ANILLO DE FIBRA ÓPTICA PARA EL TRANSPORTE DE TRÁFICO IP SOBRE MPLS ENTRE LAS CIUDADES DE GUAYAQUIL, QUITO Y CUENCA "

TESIS DE GRADO

Previa a la obtención del Título de:

INGENIERO EN ELECTRONICA Y TELECOMUNICACIONES

Presentado por

DANIEL ALEJANDRO CAMPOSANO FIGUEROA

LENIN WAGNER FRANCO VINCES

Guayaquil - Ecuador

2008

DEDICATORIA

A mi madre. Aurora, eres un ejemplo de trabajo, dedicación y amor que difícilmente podré emular, mucho menos me alcanzará la vida para agradecerte todo lo que has hecho por mi. Te amo gordita.

A mi familia. Mi tía Amada, mis hermanos Manuel y Fernando y a todos mis primos que siempre han estado conmigo, gracias a todos ustedes por la permanente confianza y apoyo.

A Judith. Sin tu compañía, no solo en este desafío, sino en mi diario andar, nada tendría sentido, simplemente nada podría ser. Amor… ¡lo hicimos!

A mi Dios. Eres el dueño de cada segundo de mi vida, gracias Jesús.

Daniel Alejandro Camposano Figueroa

"Es preciso saber lo que se quiere; cuando se quiere, hay que tener el valor de decirlo, y cuando se dice, es menester tener el coraje de realizarlo"

Dedicado para mis padres que me brindaron todo su apoyo después de decirles "Quiero ser Ingeniero y estudiar en la ESPOL"

Lenin Wagner Franco Vinces

AGRADECIMIENTOS

Al Ingeniero Washington Medina, gracias por su apoyo, consejos y guía. Esta tesis es suya Wachito.

A todos nuestros profesores a lo largo de nuestra carrera, hubo excelentes maestros, pero sobre todo grandes amigos y consejeros.

A Joffre Aguirre, gracias hermano por todo el apoyo.

TRIBUNAL DE GRADUACION

Ing. Holger Cevallos

SUBDECANO DE LA FIEC

Ing. Washington Medina

DIRECTOR DE TESIS

Ing. Juan Carlos Aviles

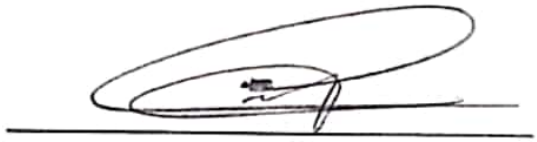
VOCAL PRINCIPAL 1

Ing. Carlos Salazar

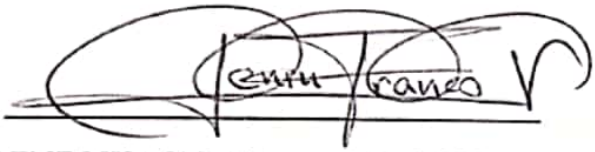
VOCAL PRINCIPAL 2

DECLARACION EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".



DANIEL CAMPOSANO FIGUEROA



LENIN WAGNER FRANCO VINCES

RESUMEN

El contenido de esta Tesis esta diseñado para abarcar tres aspectos básicos del diseño de la red: el aspecto teórico que fundamenta nuestra tesis, esto se lo identifica en los capítulos I y II. El aspecto físico de la red, el análisis de la técnica del tendido de microzanjado y los criterios de la selección de la ruta física; analizados en los capítulos III y IV. Por último el aspecto lógico, los criterios que se utilizaron para el diseño de la red desde el punto de vista activo de la red y desde los protocolos enrutado y de enrutamiento; estos analizados en los capítulos V, VI.

En el capítulo VII se realiza un resumen de cuadros comparativos de los costos de implementación de la red que ha sido diseñada.

Capítulo I: Describe los aspectos teóricos de la comunicación utilizando a la fibra óptica como medio de transmisión y las diferentes técnicas de empalme, fusión y tendido.

Capítulo II: Describe los fundamentos teóricos del protocolo MPLS y LDP, incluye también el análisis del protocolo de enrutamiento dinámico OSPF como protocolo IGP (protocolo interior) y del protocolo BGP (protocolo exterior).

Capítulo III: Describe los criterios de la selección física de la ruta por la cual se hará el tendido de fibra del diseño.

Capítulo IV: Describe los criterios que dimensionaron los equipos pasivos y activos del diseño. También, presenta el análisis del diseño de los cuartos de equipos, sus sistemas eléctricos y de protección.

Capítulo V: Describe los criterios que permitieron el diseño lógico de la red, incluyendo los criterios que llevaron a seleccionar a OSPF y BGP como los protocolos IGP y EGP respectivamente.

Capítulo VI: Describe la plataforma de pruebas que se utilizó para la validación del diseño realizado previamente, así como describe también las diferentes pruebas que se ejecutaron mediante el comando "SHOW" de CISCO para validar la configuración.

Capítulo VII: Describe los diferentes costos que se involucran en la implementación de la red que ha sido diseñada previamente.

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

En la actualidad, el mercado de las Telecomunicaciones se encuentra en un punto de inflexión en la curva de su evolución histórica: por un lado están los consumidores que van desde un sencillo y despreocupado cibernauta que cautivado por el encanto de un mundo virtual llamado Internet desea obtener la última canción de su artista favorito en el menor tiempo posible (canción que quizás aún no se haya estrenado) pasando por aquellas grandes corporaciones que con multitud de sucursales desean abaratar los costos de comunicación entre sus oficinas, por supuesto, teniendo siempre un mayor ancho de banda al mejor precio posible. Y por el otro lado tenemos a una marejada de empresas proveedoras del servicio de comunicación, grandes y pequeñas desangrándose una a otras, tratando de mantener a sus clientes (fidelizar a los clientes, ¿existe tarea más difícil?) y si queda tiempo, tratar de conseguir nuevos clientes. Entonces, ¿cual es el punto de inflexión que hemos mencionado? Se resume en tratar de dar 10 veces más ancho de banda mediante una tecnología que cueste 10 veces menos. El presente trabajo de tesis versa sobre una tecnología que es capaz de ofrecer una ventaja a las empresas de comunicaciones que se encuentren en este predicamento. Disponer de redes MPLS es ofrecer convergencia: voz, datos y video en un mismo canal a menor costo. Es poder ofrecer productos diferenciados a los clientes mediante la Ingeniería de Tráfico, conectar múltiples sucursales con costos bajos utilizando las conexiones IP-VPNs con caudales dinámicos. MPLS se traduce en flexibilidad, escalabilidad y estabilidad. Este tipo de redes, que requieren caudales

enormes de información, solamente podrían ser soportadas (y aprovechadas al máximo) por conexiones físicas que ofrezcan esta característica, gran ancho de banda. Por ello, el análisis de conexiones de fibra óptica es también un punto fuerte en el análisis y desarrollo en el presente trabajo.

A lo largo del desarrollo de esta tesis, se trata de abordar todo el proceso de análisis y diseño de una red que puede funcionar como backbone para una empresa proveedora de servicios de comunicaciones utilizando para ello a la fibra óptica como medio físico de transmisión y al protocolo IP como protocolo enrutado, soportado en una plataforma que este ejecutando protocolo MPLS a fin de otorgar una mejora en el uso del ancho de banda mediante la priorización del tráfico que ofrece este protocolo basado en etiquetas.

Para tal efecto hemos divido en 2 fases el diseño de nuestra propuesta: Fase 1, Diseño Físico de la Red. Esta fase abarca todo el estudio de la ruta, la técnica del tendido, que en nuestro caso será el micro-zanjado, y la característica del tipo de fibra a utilizar.
Fase 2, el diseño lógico de la red. Este apartado se encarga de analizar los equipos utilizados en la parte del networking, se definen aquí los protocolos IGP y EGP a utilizarse en la red y los criterios de diseño utilizados para su selección.

ANALISIS DEL PROBLEMA

i. ANTECEDENTES

Dada la creciente demanda de mayores caudales de información y de servicios de valor agregado a menores costos por parte de los clientes, las empresas proveedoras del servicio de comunicación se han visto en la necesidad de implementar nuevas redes tecnológicas o adecuar sus redes actuales de tal forma que les permita suplir la necesidad del mercado.

Las redes de acceso compartido, tales como ATM y Frame Relay, suplieron por un tiempo el acelerado crecimiento de la demanda de ancho de banda por parte de las empresas usuarias; sin embargo, en la actualidad tecnologías como MPLS satisfacen de mejor manera los requerimientos de los usuarios, ofreciendo calidad de servicio, enlaces privados virtuales (VPN) y una serie de servicios de valor agregado a un menor costo.

ii. JUSTIFICACIÓN

- MPLS es la tecnología de mayor implementación en la actualidad que permite brindar servicios de comunicación económicos, flexibles y robustos.

- El protocolo enrutado IP es el de mayor aceptación e implementación en las redes de comunicación actuales.

- El microzanjado es en la actualidad la técnica de tendido de fibra que optimiza de mejor forma la utilización de los recursos, ofreciendo menores tiempos de instalación, menores costos económicos y un bajo impacto ambiental.

iii. OBJETIVOS

- Diseñar una infraestructura completa para un enlace con fibra óptica, que proporcione un servicio de transporte de datos utilizando IP sobre protocolo MPLS, entre las ciudades de Guayaquil, Quito y Cuenca.
- Diseñar un enlace de fibra óptica según estándares internacionales: ISO - ITU – EIA / TIA.
- Realizar el dimensionamiento y configuración adecuada de los equipos activos de la red.
- Escoger la mejor ruta para el despliegue de la fibra óptica entre Guayaquil, Quito y Cuenca.
- Simulación de la red MPLS: Laboratorio basado en GNS3/Dinamyps.

CAPITULO I

Fundamentos Teóricos de Fibras Ópticas

1.1. Principios Básicos Para Un Enlace De Fibras Ópticas

1.1.1. Fibras ópticas

La Fibra Óptica consiste en un material transparente de sección cilíndrica y largo que confina y propaga las ondas luminosas por su interior. Está compuesta de tres capas diferentes como se muestra en la Fig. 1.1 : el núcleo central por donde se propaga la luz, el revestimiento que cubre el núcleo y que confina la luz dentro de él, y el recubrimiento que la dota de protección al revestimiento. El núcleo y el revestimiento están formados normalmente por vidrio de sílice, y el recubrimiento suele ser de material plástico o cubierta acrílica coloreada para facilitar su identificación.

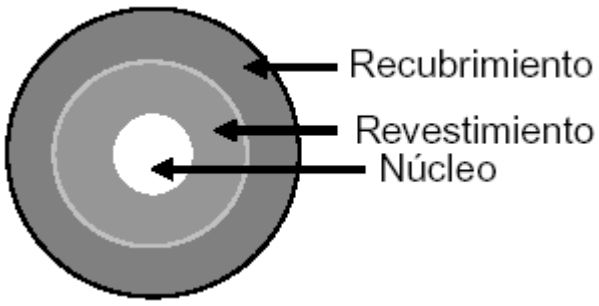


Fig. 1-1.- Fibra óptica corte transversal

Internamente la composición del núcleo y del revestimiento difieren ligeramente, debido a pequeñas cantidades de materiales que son añadidos durante el proceso de fabricación, esto altera

las características del índice de refracción de ambas capas, dando lugar a las propiedades ópticas necesarias para que se produzca el confinamiento de la luz en el interior del núcleo. En las Fibras más utilizadas, las conocidas como de salto de índice con lo que respecta a las fibras multimodales, el índice de refracción del núcleo tiene un valor constante y el del revestimiento otro ligeramente inferior. Esta diferencia de índice origina que los rayos de luz que se propagan suficientemente paralelos al eje de la fibra vayan sufriendo reflexiones totales en la interfase núcleo/revestimiento y no puedan salir del núcleo.

Estas fibras ópticas son capaces de conducir un haz de luz inyectado en uno de sus extremos mediante sucesivas reflexiones que lo mantienen dentro de si para salir por el otro extremo (Fig. 1.2). Es decir, es una guía de onda y en este caso la onda es de luz.

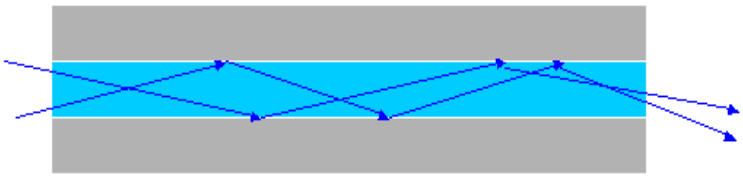


Fig. 1-2.- Corte longitudinal Fibra óptica multimodo

Estas fibras son desarrolladas para tener una gran capacidad de transmisión de luz, que en la practica están limitadas por equipos electrónicos complementarios y necesarios en un sistema de transmisión por fibras.

En la actualidad existen un tipo de Fibras Ópticas que están hechas completamente de plástico o de otros materiales transparentes, estas son generalmente más baratas pero tienen una atenuación mayor y una aplicación limitada. En la práctica, las Fibras se comercializan reuniendo un buen

número de ellas en el interior de un cable con otros tipos de protecciones que son muy variables, pues muy variables son las circunstancias que tendrán que soportar tanto durante su tendido una vez instaladas, que pueden ir desde un tendido aéreo (que puede necesitar protección anticazadores o subterráneo (que puede necesitar protección antirroedores) hasta un tendido transoceánico (que tendrá que soportar grandes tensiones durante su instalación).

Los logros con esta tecnología han sido más que satisfactorios y proporcionan muchas ventajas por ejemplo:

- ✓ **Inmunidad a interferencias electromagnéticas**. La fibra óptica es absolutamente inmune a las radio interferencias e impulsos electromagnéticos, presentando un menor índice de errores en la transmisión de señales digitales. Esto es de gran importancia en aplicaciones de control industrial donde se genera gran cantidad de ruido.
- ✓ **Menor peso y volumen.** Comparando las fibras ópticas y los cables coaxiales necesarios para obtener las mismas prestaciones, las primeras ocupan un volumen muy inferior y tienen menor peso.
- ✓ **Seguridad y aislamiento eléctrico**. En determinadas aplicaciones para ambientes peligrosos (ambientes explosivos o inflamables) o en electromedicina, las fibras ópticas son imprescindibles debido a la imposibilidad de producir descargas eléctricas o chispas.
- ✓ **Baja atenuación**. Permite realizar enlaces de mayor longitud sin necesidad de repetidores tan seguidos.
- ✓ **Seguridad frente a posibles intervenciones de la línea**. Aunque no es imposible 'pinchar' una fibra óptica, esto es más difícil que en otros soportes y normalmente se puede detectar la intervención.

- ✓ **Ancho de banda de gran capacidad**, lo que permite la transmisión de un gran volumen de información.

La fibra óptica también presenta algunos inconvenientes que no hay que olvidar. Por ejemplo:

- ✓ En los empalmes se utilizan técnicas muy complejas y necesitan de equipos muy caros y personal muy calificado.
- ✓ No hay una estandarización de los productos de distintas marcas, lo que plantea problemas de compatibilidad.
- ✓ La instalación de los conectores es compleja y requiere un personal con formación adecuada y certificado para garantizar que las
- ✓ La fibra óptica puede ser dañada, al igual que el cable de cobre, la fibra óptica puede ser deteriorada por excavaciones, corrimiento de tierras, vandalismo y accidentes.

Una de las características de la Fibra que suministra el fabricante es su “ancho de banda por distancia” (algunos la designan como “ancho de banda” simplemente) que define su capacidad de transmisión de información a una cierta distancia, depende de los valores de los coeficientes de atenuación y de dispersión de dicha fibra y lo más frecuente es suministrarla en MHz x Km. el producto de ambos factores no debe superar el valor que facilita el fabricante. Para conseguir que su valor sea elevado hay que ser muy cuidadosos durante el proceso de fabricación, téngase en cuenta que, por ejemplo, una variación del 0,1 por 100 en el diámetro del núcleo puede significar unas pérdidas de potencia tales que hagan esa Fibra inservible para altas prestaciones. Además, aunque cada vez se van consiguiendo Fibras con menores atenuaciones, al no existir ningún material completamente transparente, la luz que viaja en una Fibra Óptica siempre irá perdiendo algo de su potencia con la distancia. Las pérdidas de luz de este tipo se deben a las impurezas

existentes en el vidrio utilizado y a la absorción de la luz por las propias moléculas del material empleado y dependen de la longitud de onda de la luz utilizada y del material por el que se propaga.

Para el silicio las pérdidas más bajas se encuentran en tres intervalos de longitudes de onda que son conocidos como las tres “ventanas” de las comunicaciones ópticas y que son las utilizadas habitualmente, pues al ser en ellas más baja la atenuación se puede enviar la señal más lejos sin necesidad de amplificaciones intermedias. Aunque el no disponer de materiales con atenuación suficientemente baja fue el problema inicial que mantuvo parado el desarrollo de esta tecnología durante bastantes años, actualmente no solamente se fabrican Fibras con atenuaciones extraordinariamente bajas, sino que además, con la utilización de los amplificadores ópticos, se consigue incluso amplificar de nuevo la señal debilitada sin tener que abandonar el dominio óptico, con lo que la atenuación ha dejado de ser el principal problema que limita la capacidad de las Fibras.

1.1.1.1 Clasificación

Básicamente, existen dos tipos principales de fibra óptica: Multimodo y Monomodo. La fibra óptica multimodo es adecuada para distancias cortas, ejemplo las redes LAN o sistemas de video vigilancia, mientras que la fibra óptica monomodo está diseñada para sistemas de comunicaciones ópticas de larga distancia.

La clasificación de estas se expresa en el siguiente cuadro.

<table>
<tr><th>TIPO</th><th>CLASE</th><th>APLICACIÓN</th><th>NOTA</th></tr>
<tr><td rowspan="2">Multimodo
G.651</td><td>Índice Simple</td><td rowspan="2">1.- Baja Velocidad

2.- Distancias Cortas</td><td>El índice de refracción es único en toda la fibra</td></tr>
<tr><td>Índice Gradual
G.651</td><td>El índice de refracción es una función de la distancia al núcleo</td></tr>
<tr><td rowspan="3">Monomodo
G.652</td><td>Dispersión Desplazada
G.653</td><td rowspan="3">1.- Alta Velocidad

2.- Largas Distancias</td><td rowspan="3">Recomendado para Largas Distancia</td></tr>
<tr><td>Corte Desplazado
G.654</td></tr>
<tr><td>Disp. Desp, No Nula
G.655</td></tr>
</table>

En las Fibras ópticas la luz viaja en trayectorias determinadas llamadas modos. La fibra monomodo tiene solamente una trayectoria posible mientras que la fibra multimodo tiene varias. Las monomodo tiene más capacidad de transportar información y por eso es usada en sistema que requieren trasladar gran cantidad de información, es extremadamente difícil distinguir una fibra monomodo de una multimodo a simple vista, no existe diferencia en la apariencia externa, solo en el tamaño del núcleo .

Los diámetros usuales de fibra óptica se fabrican en cinco grupos principales, especificándose el tamaño de la fibra óptica que se encuentran con el formato núcleo/revestimiento, 8 a 10/125 μm se las conoce como fibras monomodos y se utiliza para transmisiones de datos de alta velocidad y largas distancias, 50/125 μm fue la primera fibra multimodal de las telecomunicaciones su pequeña apertura numérica y pequeño núcleo hacen que la potencia de la fibra óptica sea la menor de todas las fibras pero sin embargo es la de mayor ancho de banda potencial de todas las fibras multimodales, 62.5/125 μm en la actualidad es la fibra que más se utiliza y comercializa, tiene un ancho de banda potencial menor que la anterior pero es menos susceptible a la perdidas por

microcurvaturas, su mayor apertura numérica y diámetro de núcleo proporciona un mayor acoplamiento, 85/125 μm esta fibra posee mejor acoplamiento de luz y gracias a que su revestimiento es de 125 μm, permite la utilización conectores y empalmes estándar, 100/140 μm es la mas fácil de conectar menos sensible a las tolerancias del conector y a la acumulación de suciedad en los mismos, pero sin embargo es la de menor ancho de banda potencial y es utilizada en requerimientos de baja velocidad y es muy difícil encontrarla en el mercado de las telecomunicaciones.

Las fibras ópticas utilizadas para los enlaces troncales son las monomodos, esta fibra se caracteriza por tener muy baja atenuación, por lo tanto se logra obtener así una mayor distancia entre repetidoras, así mismo tiene muy baja dispersión por lo que se alcanzan velocidades binarias muy altas. Este tipo de fibras están normalizada en la recomendación ITU G.652 y existen millones de Km. de este tipo de fibra, instalados en redes ópticas de todo el mundo.

En las fibras monomodos solo se puede propagar de una única forma de onda, en esta se elimina las limitaciones de ancho de banda que se tienen con las fibras multimodos debido a desfases de tiempos en los recorridos de las ondas luminosas una ventaja muy importante que se encuentra en el pequeño diámetro de su núcleo constituye una cierta dificultad al permitir acoplar solo señales con suficiente energía lumínica, proporcionada por fuentes luminosas con una densidad muy elevada como por ejemplo Diodos Láser o Diodos

Dados que los diferentes parámetros constitutivos de la fibra monomodo son muy difíciles de medir individualmente, se propuso caracterizar las fibras por medio de magnitudes de significado directo para el cliente como son: Apertura numérica, Campo Modal y Revestimiento.

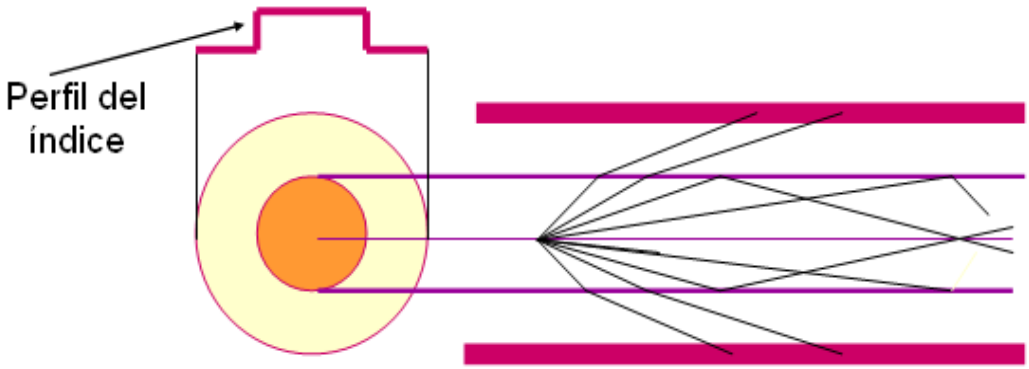


Fig. 1-3.- Fibra óptica multimodo perfil escalonado

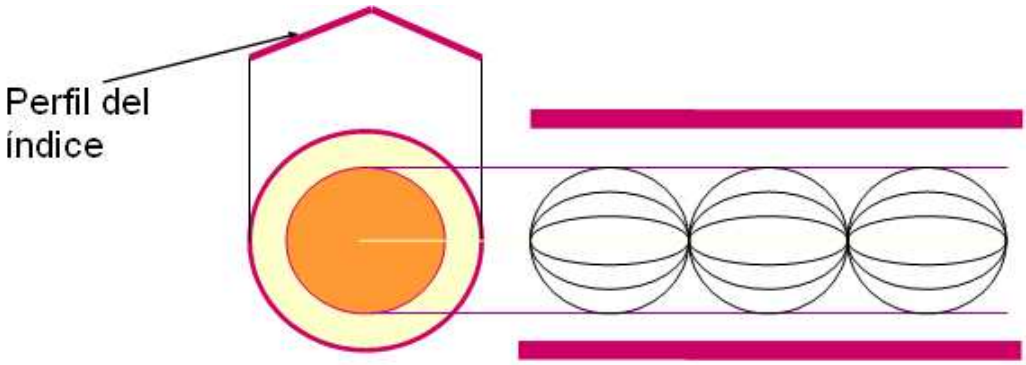


Fig. 1-4.- Fibra óptica multimodo perfil Gradual

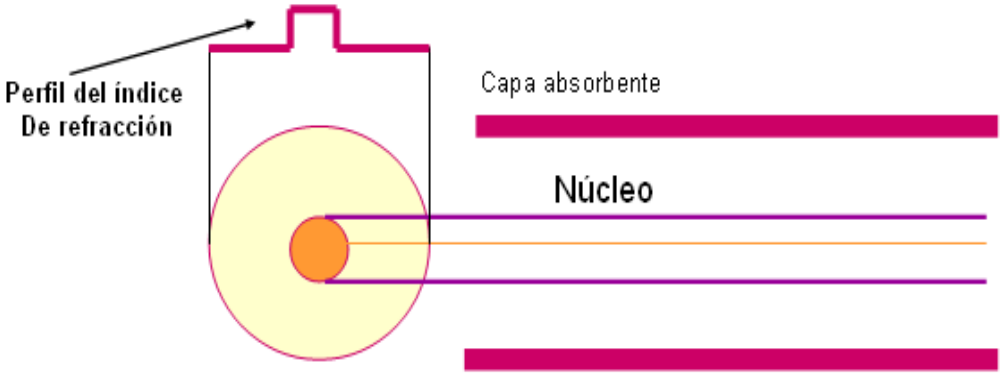


Fig. 1-5.- Fibra óptica multimodo perfil monomodo

1.1.1.2 Tipos de Estructuras

Los Cables de fibra óptica de acuerdo a su estructura están disponibles en construcciones básicas:

- Cable de estructura holgada
- Cable de estructura ajustada

Cable de estructura Holgada

Este tipo de cables consta de varios tubos de fibra rodeando un miembro central de refuerzo, y rodeado de una cubierta protectora. El rasgo distintivo de este tipo de cable son los tubos de fibra. Cada tubo, de dos a tres milímetros de diámetro, lleva varias fibras ópticas que descansan holgadamente en él. Los tubos pueden ser huecos o, más comúnmente estar llenos de un gel resistente al agua que impide que ésta entre en la fibra. El tubo holgado aísla la fibra de las fuerzas mecánicas exteriores que se ejerzan sobre el cable.

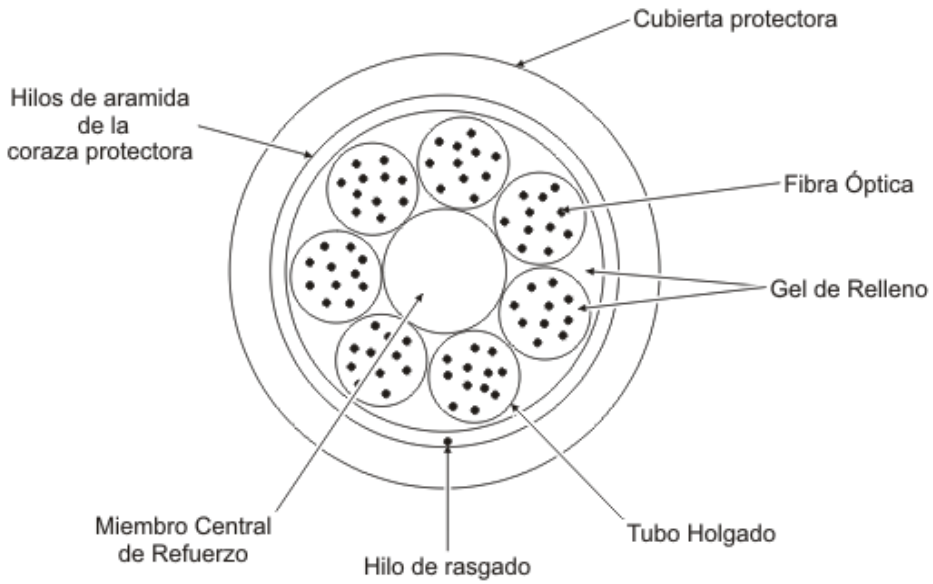


Fig. 1-6.- Cable de estructura Holgada

El centro del cable contiene un elemento de refuerzo, que puede ser acero, Kevlar o un material similar. Este miembro proporciona al cable refuerzo y soporte durante las operaciones de tendido, así corno en las posiciones de instalación permanente. Debería amarrarse siempre con seguridad a la polea de tendido durante las operaciones de tendido del cable, y a los anclajes apropiados que hay en cajas de empalmes o paneles de conexión.

La cubierta o protección exterior de el cable se puede hacer, entre otros materiales, de polietileno, de armadura o coraz a de acero, goma o hilo de aramida, y para aplicaciones tanto exteriores o interiores. Con objeto de localizar los fallos con el OTDR de un a manera más fácil y precisa, la cubierta está secuencialmente numerada cada metro (o cada pie) por el fabricante.

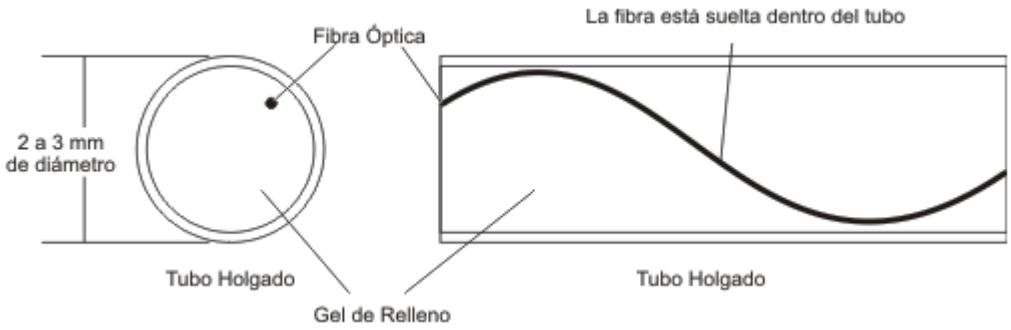


Fig. 1-7.- Tubo Holgado del cable de fibra

Los cables de estructura holgada se usan en la mayoría de las instalaciones exteriores, incluyendo aplicaciones aéreas, en tubos o conductos y en instalaciones directamente enterradas. El cable de estructura holgada no es muy adecuado para instalaciones en recorridos muy verticales, porque existe la posibilidad de que el gel interno fluya o que las fibras se muevan.

Cable de estructura ajustada

Contiene varias fibras con protección secundaria que rodean un miembro central de tracción, y todo ello cubierto de una protección exterior. La protección secundaria de la fibra consiste en una cubierta plástica de 900 μm de diámetro que rodea a! recubrimiento de 250 μm de la fibra óptica.

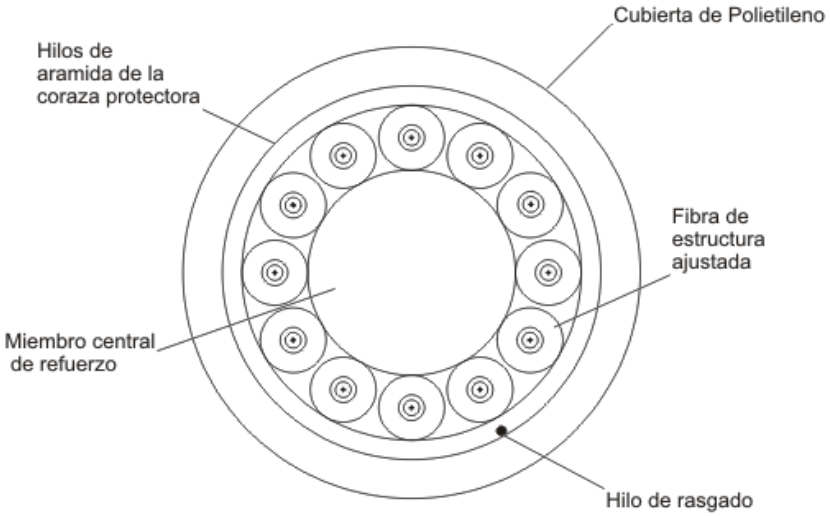


Fig. 1-8.- Cable de estructura ajustada

La protección secundaria proporciona a cada fibra individual una protección adicional frente al entorno así como un soporte físico. Esto permite a la fibra ser conectada directamente (conector instalado directamente en el cable de la fibra), sin la protección que ofrece una bandeja de empalmes. Para algunas instalaciones esto puede reducir el costo de la instalación y disminuir el número de empalmes en un tendido de fibra. Debido al diseño ajustado del cable, es más sensible a las cargas de estiramiento o tracción y puede ver incrementadas las pérdidas por micro curvaturas.

Por una parte, un cable de estructura ajustada es más flexible y tiene un radio de curvatura más pequeño que el que tienen los cables de estructura holgada. En primer lugar. es un cable que se ha diseñado para instalaciones en el interior de los edificios. También se puede instalar en tendidos

verticales más elevados que los cables de estructura holgada, debido al soporte individual de que dispone cada fibra.

1.1.1.3 Campo Modal

El diámetro del campo modal (MFD) representa una medida del enlace transversal de la intensidad del campo electromagnético del modo en una sección transversal.

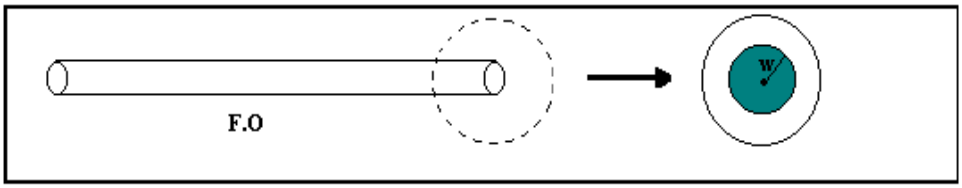


Fig. 1-9.- Diámetro del Campo Modal

Error de concentricidad del campo modal

Es la distancia entre el centro modal y el centro de la superficie del revestimiento. El error de concentricidad recomendado para el campo modal a 1310 nm no debe exceder de 1 µm.

NOTA 1 – Para determinadas técnicas de empalme y ciertos requisitos de pérdida en los empalmes, pueden ser apropiadas tolerancias de hasta 3 µm.

NOTA 2 – El error de concentricidad del campo modal y el error de concentricidad del núcleo, representado por la iluminación transmitida utilizando longitudes de onda diferentes de 1310 nm (incluida la luz blanca), son equivalentes. En general, la desviación del centro del perfil del índice de refracción y el eje del revestimiento representa también el error de concentricidad del campo modal, pero si apareciese alguna diferencia entre el error de concentricidad del campo modal,

medido de acuerdo con el RTM *, *referente test method*, y el error de concentricidad del núcleo, el primero constituirá la diferencia.

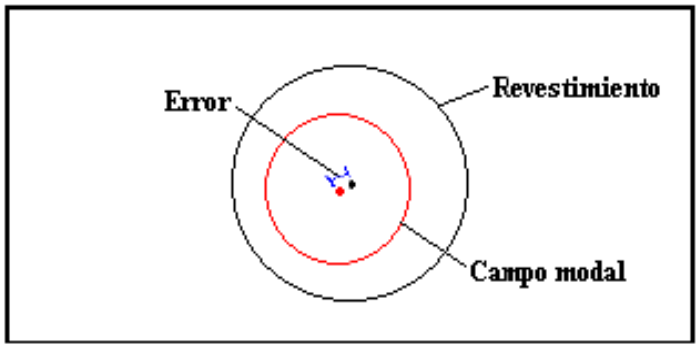


Fig. 1-10.- Error de concentricidad del campo modal

No circularidad del campo modal

En la práctica, la no circularidad del campo modal de las fibras que tienen campos modales nominalmente circulares es lo suficientemente baja como para que la propagación y los empalmes no se vean afectados. En consecuencia, no se considera necesario recomendar un valor determinado de no circularidad del campo modal. En general, no es necesario medir la no circularidad del campo modal con fines de aceptación

* RTM. Método de prueba de referencia

Centro del campo modal

El centro del campo modal es la posición del centroide de la distribución espacial de intensidad en la fibra y se lo calcula de la siguiente forma.

$$r_c = \frac{\iint_{Area} rI(r)dA}{\iint_{Area} I(r)dA}$$

1.1.1.4 Apertura Numérica

La Apertura numérica es comúnmente usada para describir la aceptancia de luz o capacidad de acceso de la señal óptica a la fibra y, para calcular la eficiencia de acoplamiento de potencia de fuente a fibra óptica, la cual esta relacionada con el ángulo de máxima aceptancia

En las características de la fibra viene abreviada con las letras AN y está relacionada matemáticamente con el máximo ángulo de acoplamiento.

- AN= sen (ángulo máximo de acoplamiento)
- N1= índice de refracción del revestimiento
- N2= índice de refracción del revestimiento

Los ángulos máximos de acoplamiento típico para una fibra multimodal varían desde 10 a 30 grados. Valores típicos de AN varían desde 0.2 a 0.5. Normalmente se especifica el valor de AN para una fibra óptica.

1.1.2. Sistemas De Transmisión Por Fibras

Para la instalación de sistemas de fibra óptica es necesario utilizar técnicas y dispositivos de interconexión como empalmes y conectores. Los conectores son dispositivos mecánicos utilizados para recoger la mayor cantidad de luz. Y los conectores realizan la conexión del emisor y receptor óptico.

1.1.2.1. Diagrama de bloques de un sistema de transmisión por fibra

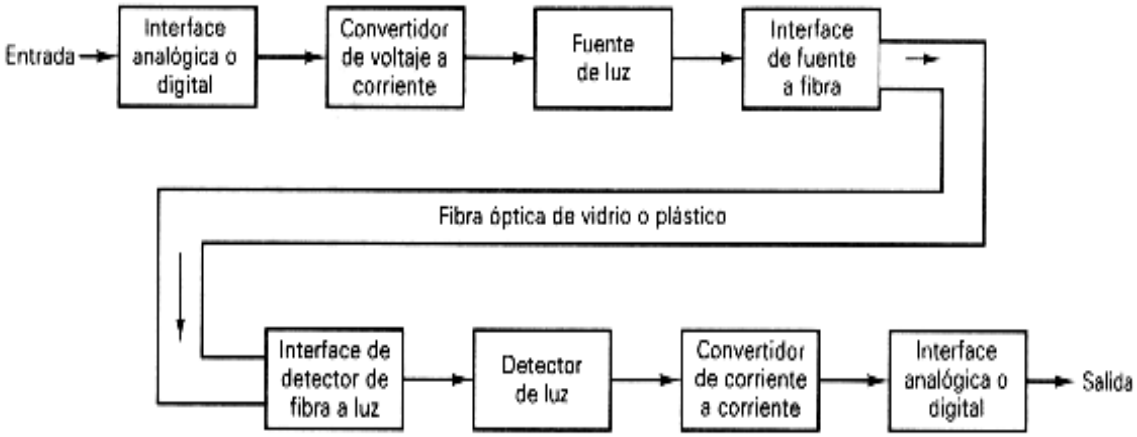


Fig. 1-11.- Diagrama de bloques de un sistema de transmisión por fibra

1.1.2.2 Componentes De Un Sistema

Los sistemas de transmisión por fibra están compuestos por tres bloques importantes los cuales son: transmisor, receptor, y guía de fibra. El transmisor, cuya misión es la de convertir la señal eléctrica en señal óptica susceptible de ser enviada a través de una fibra óptica. Cuando la señal luminosa es transmitida por la fibra, en otro extremo del circuito se encuentra otro componente del sistema al que se le denomina detector óptico o receptor, cuya misión consiste en transformar la señal luminosa en señal eléctrica, similar a la señal original.

El transmisor esta compuesto por una interfase analógica o digital, un convertidor de voltaje a corriente, una fuente de luz y un adaptador de luz de fuente a fibra, esta fuente de luz se puede modular por una señal digital o analógica. Para la modulación analógica, la interfase de entrada acopla las impedancias y limita la amplitud de la señal de entrada. Para la modulación digital, la

fuente original puede ya estar en forma digital o, si esta en la forma analógica, se debe de convertir a un flujo de pulsos digitales. Para el ultimo de los casos se debe incluir el la interfase un convertidor analógico a digital.

El convertidor de voltaje a corriente sirve como una interfase eléctrica, entre los circuitos de entrada y la fuente de luz. La fuente de luz es o un diodo emisor de luz (LED) o un diodo de inyección de láser (ILD). La cantidad de luz emitida por un LED o un ILD es proporcional a la cantidad de la corriente de excitación. Por lo tanto, el convertidor de voltaje a corriente convierte un voltaje de señal de entrada a una corriente que se usa para dirigir la fuente de luz, toda la luz que es emitida por la fuente es llevada hacia la fibra por medio de una interface mecánica parecido a un lente y tiene por objetivo acoplar la mayor cantidad de luz posible del cable de fibra en el detector de luz. El detector de luz frecuentemente es un diodo PIN (tipo p –tipo n) o un APD (fotodiodo de avalancha). Ambos, el diodo APD y PIN, convierten la energía de luz a corriente. En consecuencia, se requiere un convertidor de corriente a voltaje. El convertidor de corriente a voltaje transforma los cambios en la corriente del detector a cambios en el voltaje de la señal de salida

Los diodos láser emisores de luz pueden seleccionar y controlar la longitud de onda de emisión, la anchura espectral de emisión es mucho más estrecha y puede transportar más concentración de energía por longitud de onda y la distancia de alcance es mayor. Al ser controlada la emisión de longitud de onda, es posible reunir muchas longitudes en una misma fibra sin interactuar entre ellas y así construir un sistema de transmisión que aprovecha la misma fibra para transmitir simultáneamente más información. Los receptores, básicamente, pueden tener mayor o menor sensibilidad y de ahí su posible uso. Además dependiendo del tipo de material (Ge, Si, etc.) tienen una sensibilidad especifica según la longitud de onda y, por tanto, su uso es en la 1ª ventana (850

nm), la 2ª (1300 nm) o bien en la 3ª (1550 nm). En base a estas características se dedican a unas u otras aplicaciones.

El fundamento de transmisión por fibra se basa en convertir las señales eléctricas en un código óptico para que, a través de dicha fibra, transporte la información con la mayor integridad y garantía posible.

Una vez que la señal se ha convertido de formato eléctrico a óptico, existen diferentes mecanismos de codificación para el transporte de dichas señales a través de la fibra que facilitan, en gran medida, la recuperación de las mismas en el extremo remoto y las convierten a eléctricas con la integridad máxima para los datos transportados. Una vez superado este nivel de transporte, existe otro proceso de nivel superior, ajeno al puro transporte, que se encargaría de aplicar técnicas de recuperación de errores. Cada código de transporte utilizado encapsula el protocolo específico de canal.

Existen, como se ha mencionado, tres zonas para esta transmisión: en 850 nm, 1300nm, y 1550 nm. La primera generación de los sistemas de comunicación óptica, introducida comercialmente en 1980, operaba en longitudes de onda de 0.8 um la llamada primera ventana de comunicaciones ópticas. Estos sistemas operaban a una tasa de transmisión de 45 Mbps con una distancia entre repetidores (puntos de regeneración de señal) de 10 Km. La máxima distancia posible entre repetidores estaba dada por la atenuación de las fibras ópticas que limitaban la relación señal-ruido entregada por el sistema.

Quedaba claro, en la época, que era deseable transmitir información en longitudes de onda mas largas aprovechando la menor atenuación de las fibras y así conseguir aumentar la distancia entre

repetidores. Esto impulso el desarrollo de láser de semiconductores que emitieran luz en longitudes de onda de 1.3 um donde la atenuación de la fibra es menor a 1 dB/Km. Esta nueva generación operando en la segunda ventana fue introducida en la primera mitad de los 80 y, como explicaremos mas adelante, estos sistemas estaban limitados a una capacidad menor a 100 Mbps a la dispersión modal propias de la fibra multimodo. Este último problema fue solucionado mediante el uso de fibras monomodos y, en 1987, ya existían sistemas con capacidades de 1.7 Gbps y repetidores separados por 50 Km.

Desde el punto de vista de la atenuación de la fibra esta claro que es deseable trabajar en torno del mínimo en torno del mínimo en la región de 1.5 um donde la atenuación es 0.2 dB/Km. Esta región es llamada tercera ventana, sin embargo, las llamadas fibras monomodo Standard presentan un valor de dispersión cromática elevado en la tercera ventana.

La búsqueda de una fibra óptica que presentara un mínimo de dispersión cromática en la tercera ventana llevo al desarrollo y posterior introducción comercial a comienzos de los años 90, de las llamadas fibras DSF (dispersión shifted fibers). Estas fibras tienen una dispersión cromática aproximadamente 10 veces inferior al de las fibras monomodo estándar.

El receptor recibe la secuencia de bit ópticos, la transforma en una secuencia de bit eléctricos este paso se le denomina fotodetección, recupera la sincronización y toma una decisión sobre el valor de bit recibido mediante la comparación con un valor umbral generalmente fijo si la potencia recibida en el intervalo de tiempo que supera al valor de umbral el detector decidirá 1 caso contrario decidirá 0. Un error de detección se produce cuando un bit “1” transmitido es detectado como un bit “0”y viceversa. Los sistemas de comunicación modernos de alta capacidad trabajan con tasas de error inferiores a una detección errónea cada 10 o 16 bits transmitidos un solo error

cada 10 billones de bits. Para cumplir con este estricto criterio a lo largo de toda la vida útil del sistema se utilizan técnicas electrónicas de corrección de errores (forward error correction), implementadas en el receptor, que permiten mantener una adecuada tasa de error aun en presencia de degradaciones de relación señal – ruido, lineales y no lineales. El costo que se paga es el de transmitir la información a una tasa que puede estar entre 7 % y el 20 % mayor. Esto se denomina overhead y requiere la utilización de componentes electrónicos de mayor ancho de banda (y costo, sobre todo para sistemas que operan a tasas de 40 Gb/s).

1.1.2.3 Especificaciones requeridas para un sistema de transmisión

Todos los sistemas de transmisión por fibra deben acoger todas las necesidades de los usuarios relacionados con el correcto uso de estos. A continuación mencionamos importantes requerimientos en este tipo de sistemas

- ✓ Dimensionamiento del sistema a fin de adaptar la transmisión a los requerimientos de ancho de banda de los futuros clientes
- ✓ Todos los empalmes y conectores deben ser instalados de tal forma que las perdidas se minimicen, ya que los cálculos están basados en valores estandarizados de perdidas por acople y empalmes.
- ✓ El tendido de la fibra óptica debe de cumplir las normativas explicadas en lo posterior para garantizar que la fibra no sufra después de la instalación.
- ✓ La calidad de los materiales a utilizar debe ser garantizada para garantizar una larga vida al sistema de transmisión
- ✓ Luego de instalar todo el sistema de transmisión es importante manejos con sistemas computarizados con la finalidad de reducir por completo la intervención de humanos y así reducir errores y costos por mantenimiento de equipos

- ✓ Para la fibra óptica escogida la pureza del material del núcleo sea tan alta, que la atenuación se mantenga dentro de los límites razonables.

1.1.3. Tipos De Tendido

En la actualidad podemos decidir que tipo de tendido de fibra se pueden realizar en un sistema de transmisión bajo consideraciones como: facilidad de instalación, futuros mantenimientos, topologías, clima, y seguridad del trabajo una vez instalado. Todas estas consideraciones deben ir de la mano con un estudio técnico que considere futuras ampliaciones y mejoras del sistema.

Tendido del cable en canalizaciones

El tipo de cable que se coloca cuando se realizan tendidos en canalizaciones tiene un diámetro entre 10 y 16 mm, el método consiste en colocar conductos de hormigón y dentro de ellos colocar subconductos de polietileno en los cuales se alojara un cable de fibra en cada subconducto, este método ayuda a que la fibra esta mas pretejida, además en el momento de cambiar una fibra por otra es mucho mas fácil y se puede realizar sin tener contacto con las otras.

Tendido del Cable Subterráneo

El primer parámetro que se debe tener en consideración cuando se realiza este tipo de tendido es el suelo, y se lo realiza por lo general en zonas rurales que permitan realizar zanjas que estan entre 70 y 80 cm de profundidad y 25 cm de ancho. Es importante considerar que se debe tener en cuenta que en la superficie exista la menor intensidad de vibraciones por lo que hay que tomar en cuenta la distancia que se encuentre de la calles.

Tendido del cable Aéreo

Este tipo de tendido involucra instalar la fibra en los postes de transmisión eléctrica, optimizando así los costos ya que se utilizan los postes que interconectan el sistema nacional interconectado eléctrico y telefónico, gracias a las características de la fibra óptica y de la señal que se transmite los grandes campos magnéticos que se generan no afectan el sistema.

Los tendidos aéreos pueden realizase de dos formas.

- ✓ Utilizando los modernos cables O.P.G.W o ADSS. que son fabricados con un elemento autosoportable.
- ✓ La segunda opción es utilizando los hilos de tierra o cables de las líneas de alta tensión y sobre ellos adosar un cable óptico dieléctrico por medio de grapas o arrollamiento sobre ambos cables de alambres.

El tendido se los realiza utilizando maquinas y dispositivos de control que regulan y miden constantemente la tensión del cable para asegurar que la tensión máxima de tendido del cable no sobrepase los limites permitidos, este control ocurre en todos los tipos de tendido.

La instalación del cable se lo realiza de la siguiente manera: se ata el cable de fibra a lo largo de los dos postes con los autosoportados luego se lleva el cable de fibra por el neutro de los postes de alta tensión asegurándose de que el cable sea conectado a tierra, se debe tomar en cuenta la tensión por el pandeo según las especificaciones del cable. Existen equipos especializados para realizar los tendidos aéreos que monitorean la tensión con que se va halando el cable y da la opción de visualizarla en un monitor, en cada poste el cable es fijado en él, colocando las abrazaderas en los extremos muertos, algo muy importante es cuando se realiza un empalme se

debe considerar que las cajas emplamadoras deben ser a prueba de intemperie, y en los postes se dejan reservas de expansión de aprox. unos 6 metros enrollados.

Es aconsejable realizar mediciones a la fibra antes y después de la instalación con el OTDR para garantizar que la fibra óptica se encuentra en perfecta condición previa y posterior al tendido.

Tendido Por microzanjas

El Microducto es un nuevo concepto de diseño de instalación subterránea que ha sido introducida en Europa y Norte América durante los últimos años.

Ha sido desarrollado para los anillos internos urbanos por su versatilidad de despliegue. Debido a su menor costo de despliegue, el concepto ahora es utilizado para redes de larga distancia también.

El Microducto es un ducto muy pequeño generalmente en el rango de 4mm - 12.7mm (diámetro externo) que puede ser soplado dentro de un ducto vacío de ¾" - 2" o instalado como una subdivisión en un ducto existente ocupado de 1" a 2".

Las micro zanjas constituyen una nueva y ventajosa técnica de construcción para canalizaciones de cables ópticos en carreteras. Se trata de canalizaciones de tamaño muy reducido que se construyen sobre asfalto u hormigón de manera rápida, económica y su anchura puede variar entre 10 y 15mm.

Ventajas del Microducto

Eficiencia: al reducir el espacio desperdiciado del ducto, la Microtecnología nos permite la máxima utilización de las actuales y futuras infraestructuras en comunicación.

Mejora de la rentabilidad: permite la máxima rentabilidad y mayor retorno de la inversión por todos los clientes actuales o futuros gastos de derecho de vía.

Versatilidad: la tecnología está cambiando constantemente; por lo que, sólo instalando las fibras que se necesitan hoy en día se tiene la oportunidad de utilizar lo último en fibra ya que la tecnología está disponible.

Expansión de la Red: al colocar varios Microductos en los ductos más grandes vacíos (o algunos Microductos dentro de ductos ocupados), las preocupaciones de futuras expansiones se resuelven. Futuras expansiones no interrumpirán los servicios existentes.

Rapidez en la instalación: la Microtecnología permite instalaciones más rápidas, reduciendo nuevamente los costos de instalación global al cliente.

Mejora la utilización de capital: los costos concernientes a los cables de fibra óptica son generalmente bajos; el Microcable viene en presentaciones de 2 a 72 fibras. Utilizando bajas cantidades de cable el costo es dramáticamente menor. Se puede únicamente instalar los microcables para satisfacer los requerimientos de capacidad de los clientes. De esta forma se pueden mantener las inversiones realmente ajustadas a los flujos de efectivo.

1.1.4. Tipos de Empalmes

Existen dos técnicas para realizar los empalmes, una de ellas son los empalmes por fusión que son los empalme por fibras prealineadas del núcleo o la alineación del revestimiento. Que el núcleo este completamente alineado produce la menor perdida de empalmes en el caso de las fibras monomodos, es importante realizar fortalecer el empalme con un refuerzo mecánico. En los empalmes mecánicos la alineación es determinada por los componentes del dispositivo empalmador y mantenida mediante adhesivos.

Empalmes por fusión

Fig. 1-12.- Procedimiento de empalme de fibras por fusión.

Las técnicas por fusión, están clasificados en base al tipo de fuente de calor utilizada: una descarga eléctrica, un láser gaseoso o una llama .El primero de ellos es el más ampliamente utilizado en el caso de fibras de sílice.

En especial, se han desarrollado varias técnicas para realizar empalmes por medio de descarga eléctrica, tales como el método de prefusión, el método de descarga de alta frecuencia con un elevado voltaje de trigger (HHT), y el método de calentamiento uniforme para realizar empalmes de múltiples fibras

Los métodos de empalme por fusión utilizan una fuente de calor para fundir y unir las fibras ópticas. A diferencia de otros métodos que utilizan materiales de adaptación o adhesivos, en este caso no existe ningún otro material más que la propia fibra en la región del empalme. Por lo tanto, este método posee inherentemente bajas pérdidas por reflexión y alta fiabilidad.

Los empalmes de Fibra Óptica (FO) son de carácter permanente, para su realización se requiere una maquina empalmadora especializada, que pueden ser manual o automática. Una máquina empalmadora automática alinea los núcleos de las dos fibras enfrentadas con motores servocontrolados por una cámara que realimenta su posición. Una vez logrado esto, se produce un arco eléctrico generado por dos electrodos, con lo cual se logra la fusión de las fibras.

Fig.1-13.- Maquina empalmadota automática

El proceso paso a paso se da de la siguiente forma**:**

1.- Se identifica el tipo de fibra con el cual se trabajara, MM o SM, para seleccionar en el menú de la fusionadora el tipo de fusión de acuerdo al tipo de fibra.

2.- Se retiran los recubrimientos de protección, aproximadamente unos 10 cm., se utiliza una pinza especial con el cuidado de no cortarla y de extraer por completo la cubierta de protección

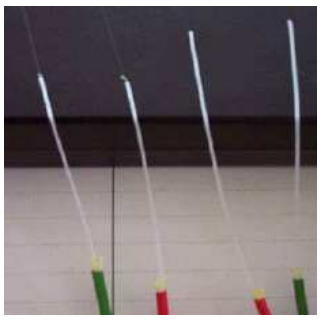


Fig. 1-14.- Fibra óptica con las cubiertas retiradas

3.- Se coloca el protector del empalme en uno de los cables de FO con la precaución de no dañarla.

4.- Se coloca cada FO en la maquina de corte, a una longitud desead,. La herramienta de corte está basada en el rayado del vidrio y partido por presión, la fibra debe por tanto estar completamente limpia, sin residuos de recubrimiento, lo cual nos impedirá que la fibra sea cortada..

Fig. 1-15.- Fibra óptica colocada en la peladora

5.- Una vez cortada cada FO, se deberá mantener en lugar limpio

6.-La fibra se coloca dentro de la maquina fusionadora una en cada extremo, a las distancias indicadas en el equipo. Una vez asegurados las dos fibras, se coloca la tapa y se presiona el botón de set, se inicia de esta manera el proceso automático de fusión

Fig. 1-16.- Fibra óptica colocada en la Fusionadora

El procedimiento de empalme de fibras por fusión utilizando descarga eléctrica se muestra en la figura 1. En primer lugar, se quitan las cubiertas de las fibras y se cortan.

Ambas fibras se sitúan con una cierta separación entre ellas en una máquina empalmadora de fibras y se pulsa un botón para comenzar el proceso. Hasta este punto el trabajo se realiza manualmente por parte de un operario. En el momento de pulsar el botón de la máquina, ésta comienza a mover las fibras para reducir la separación entre las mismas. Durante el movimiento de las fibras, se genera una descarga eléctrica que se mantiene durante un período de tiempo predeterminado. Este proceso tiene lugar de forma automática en la máquina empalmadora. Por último, la región donde se ha producido el empalme se protege para facilitar el manejo de la fibra. Actualmente existen máquinas completamente automáticas que realizan todas las acciones: desde quitar las cubiertas hasta proteger el empalme

1.1.5. Tipos de Conectores

Los conectores son los elementos que se encargan de conectar los hilos de fibra a un elemento de red, ya puede ser un transmisor o un receptor. Los tipos de conectores disponibles son muy variados, entre los que podemos encontrar se hallan los siguientes:

FC, que se usa en la transmisión de datos y en las telecomunicaciones.

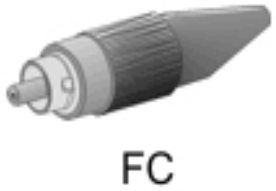


Fig. 1.17.- Conector tipo FC

Características

- Generalmente se construyen de una sola pieza
- Cumplen con los estándares TIA/EIA 604.
- Compatible con los cables de grosores entre 900 μm y 2.0 a 3.0 mm

Especificaciones

- Perdidas de inserción de 0.15 db. Típico para fibras monomodo
- Perdidas de retorno optico menores a – 45 db tipicos
- Rango de temperatura entre -40 ^{o}C y 80 ^{o}C
- Resistencia > 25 Lb (strainght pull)

LC y MT-Array que se utilizan en transmisiones de alta densidad de datos

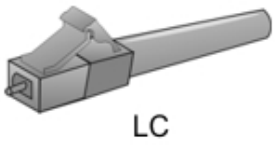


Fig. 1.18.- Conector tipo LC

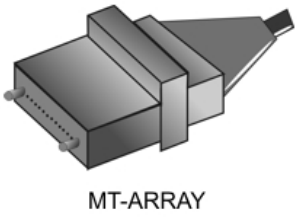


Fig. 1.19.- Conector tipo MT – ARRAY

SC y SC-Dúplex se utilizan para la transmisión de datos

Fig. 1.20.- Conectores tipo SC y SC Duplex

Características

- Generalmente se construyes de una solo pieza
- Cumplen con los estándares TIA / EIA 604

- Permiten instalación de campo
- Es compatible con cables de grosor entre 900 μm y 2.0 a 3.0 mm.

Especificaciones

- Perdidas de inserción de 0.15 db. Típico para fibras monomodo
- Perdidas de retorno optico menores a – 45 db tipicos
- Rango de temperatura entre -40 ^{o}C y 75 ^{o}C
- Resistencia > 25 Lb (strainght pull)

ST o BFOC se usa en redes de edificios y en sistemas de seguridad

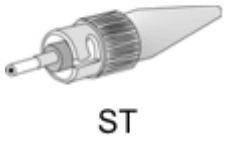


Fig. 1.21.- Conectores Tipo ST

FDDI, se usa para redes de fibra óptica

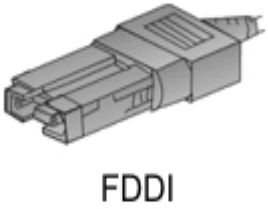


Fig. 1.22.- Conectores Tipo FDDI

1.1.6. Localización de fallas

La herramienta principal para la detección y localización de fallas ópticas es el OTDR (reflectometro óptico en el dominio coherente). Estas técnicas aprovechan la dispersión de reyleigh para obtener una imagen de la perdida versus la distancia a lo largo de la fibra óptica.

OTDR

Esta prueba consiste en enviar pulsos de la luz repetitivos en un extremo de la fibra. Esta luz es dispersada continuamente a lo largo de la fibra y retorna al equipo de prueba. Debido a que la velocidad de la luz en la fibra de vidrio es constante, el tiempo de retorno es convertido en distancia de tal manera que el OTDR produce un trazo perdida versus distancias. Estos trazos se muestran en un display o pueden se impreso o grabados para propósitos de análisis y comparación

La precisión de la ubicación de una anomalía en el trazo (por ejemplo, un empalme o una ruptura) depende de algunos factores, pero en particular de la duración de los pulsos transmitidos. La distancia en la fibra que el OTDR puede analizar es limitada por consideraciones de señal a ruido. La potencia de la señal se puede incrementar alargando la duración de los pulsos de luz lanzados, pero a expensas de la reducción de precisión

1.1.7. Perdidas del enlace.

Las pérdidas son consideradas factores fundamentales que limitan el rendimiento de los sistemas de comunicación por fibra óptica. Las pérdidas reducen el promedio de potencia que llega al receptor. La distancia de transmisión es una limitante inherente del sistema de fibra óptica, si consideramos que los receptores requieren una cantidad mínima de potencia para

reconocer la señal de transmisión. Las perdidas que se presentan en un sistema de comunicación por fibras son las siguientes.

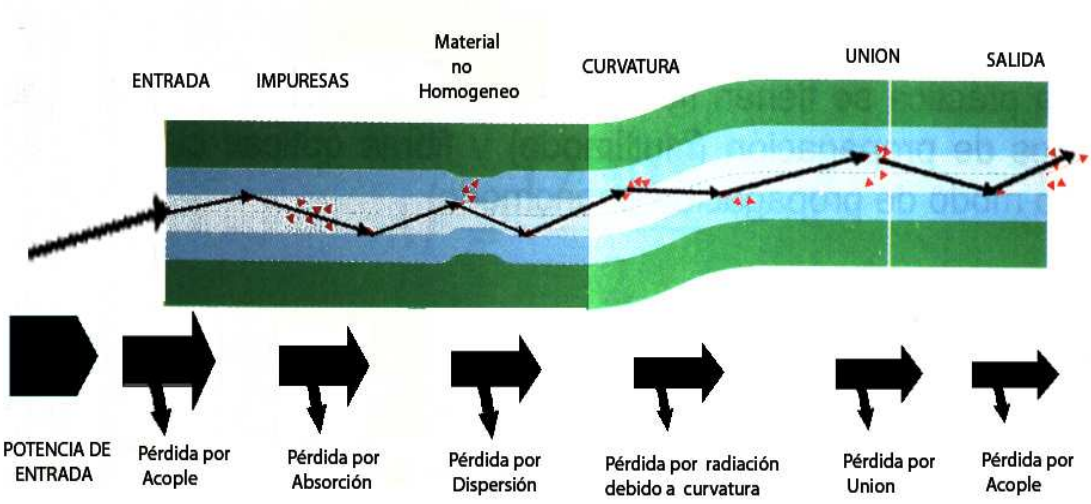


Fig. 1-23.- Pérdidas en un sistema de comunicación por fibras

1.- Pérdidas por acoplamiento.

En los cables de fibra las pérdidas de acoplamiento pueden ocurrir en cualquiera de los tres tipos de uniones ópticas: conexiones de fuente a fibra, conexiones de fibra a fibra y conexiones de fibra a fotodetector. Las pérdidas de unión son causadas más frecuentemente por uno de los siguientes problemas de alineación: mala alineación lateral, mala alineación de separación, mala alineación angular y acabados de superficie imperfectos.

Mala alineación lateral.

Esto es el desplazamiento axial o lateral entre dos piezas de cables de fibra contiguas. La cantidad de pérdida puede ser desde un par de décimas de un decibel a varios decibeles. Esta pérdida

generalmente es insignificante si los ejes de la fibra están alineados dentro del 5% del diámetro más pequeño de la fibra.

Mala alineación de la separación.

Esta a veces se llama, separación de la extremidad. Cuando los empalmes se hacen en la fibra óptica, las fibras deben tocarse. Entre más separadas estén las fibras, mayor es la pérdida de la luz. Si dos fibras están unidas con un conector, las puntas no deben tocarse. Esto se debe a que las puntas frotándose una con otra en el conector, causarían daño a cualquiera o ambas fibras.

Mala alineación angular.

Esto veces se llama desplazamiento angular. Si el desplazamiento angular es menor que 2', la pérdida será menor que 0.5 dB.

Acabado de superficie imperfecta.

Las puntas de las dos fibras unidas deben estar altamente pulidas y encuadrarse juntas adecuadamente. Si las puntas de la fibra están a menos de 3' de la perpendicular, las pérdidas serán menores que 0.5 dB

2.- Pérdidas por Absorción

Las pérdidas por absorción en las fibras ópticas son análogas a la disipación de potencia en los cables de cobre; las impurezas en la fibra absorben la luz y la convierten en calor. El vidrio ultrapuro usado para fabricar las fibras ópticas es aproximadamente 99.9999% puro pero aun así, las pérdidas por absorción entre 1 y 1000 dB/Km. son típicas. Esencialmente, hay tres factores

que contribuyen a las pérdidas por absorción en las fibras ópticas: absorción ultravioleta, absorción infrarrojo y absorción de resonancia del Ion.

Absorción ultravioleta.

La absorción ultravioleta es provocada por electrones de valencia en el material de silicio del cual se fabrican las fibras. La luz ioniza a los electrones de valencia en conducción. La ionización es equivalente a la pérdida total del campo de luz y, en consecuencia, contribuye a las pérdidas de transmisión de la fibra.

Absorción infrarroja.

La absorción infrarroja es un resultado de fotones de luz que son absorbidos por los átomos de las moléculas, en el núcleo de vidrio. Los fotones absorbidos se convierten a vibraciones mecánicas aleatorias típicas de calentamiento.

Absorción de resonancia de Ion.

La absorción de resonancia de Ion es causada por los iones OH- en el material. La fuente de los iones OH- son las moléculas de agua que han sido atrapadas en el vidrio, durante el proceso de fabricación. La absorción del Ion también será causada por las moléculas de hierro, cobre y cromo.

3.- Pérdidas por dispersión modal

La dispersión modal o esparcimiento del pulso, es causado por la diferencia en los tiempos de propagación de los rayos de luz que toman diferentes trayectorias por una fibra. Obviamente, la dispersión modal puede ocurrir sólo en las fibras de multimodo. Se puede reducir considerablemente usando fibras de índice graduado y casi se elimina totalmente usando fibras de índice de escalón de modo sencillo.

La dispersión modal puede causar que un pulso de energía de luz se disperse conforme se propaga por una fibra. Si el pulso que está esparciéndose es lo suficientemente severo, un pulso puede caer arriba del próximo pulso (este es un ejemplo de la interferencia de intersímbolo). En una fibra de índice de escalón multimodo, un rayo de luz que se propaga por el eje de la fibra requiere de la menor cantidad de tiempo para viajar a lo largo de la fibra. Un rayo de luz que choca a la interface de núcleo/cubierta en el ángulo crítico sufrirá el número más alto de reflexiones internas y, en consecuencia, tomar la mayor cantidad de tiempo para viajar a lo largo de la fibra.

4.- Pérdidas por curvaturas

Durante el proceso de fabricación, el vidrio es producido en fibras muy largas de un diámetro muy pequeño. Durante este proceso, el vidrio está en un estado plástico (no líquido y no sólido). La tensión aplicada al vidrio durante, este proceso, causa que el vidrio se enfríe y desarrolle irregularidades submicroscópicas que se forman de manera permanente en la fibra. Cuando los rayos de luz que se están propagando por una fibra chocan contra una de estas impurezas, se difractan y esto causa que la luz se disperse o se reparta en muchas direcciones. Una parte de la luz difractada continua por la fibra y parte de ésta se escapa por la cubierta. Los rayos de luz que se escapan representan una pérdida en la potencia de la luz. Esto se llama pérdida por dispersión de Rayleigh.

CAPITULO II

Fundamentos Teóricos Multiprotocol Label Switching – MPLS

2.1 Conceptos Básicos de redes IP-MPLS

2.1.1 Generalidades

En la actualidad, cada día son más las empresas proveedoras de servicios de comunicaciones que no solo deciden proteger la inversión realizada en su infraestructura actual, sino que, debido al alto nivel de competitividad en este agresivo mercado de las Telecomunicaciones y las cada vez más exigentes necesidades de sus clientes, se han visto en la necesidad de buscar formas de generar nuevos servicios que les permita fidelizar a sus clientes actuales e ir a la captura de nuevos clientes.

Multiprotocol Label Switching (MPLS) es un excelente método para poder ofrecer esos servicios agregados que actualmente con redes IP tradicionales no son posibles. MPLS y su "reenvío de etiquetas" le permitirán a redes actuales con switches ATMs por ejemplo, conmutar paquetes dentro de su red con un mínimo consumo de procesador debido a que el criterio de reenvío se realiza únicamente considerando una pequeña parte de la cabecera de un paquete IP: su etiqueta MPLS.

MPLS integra de muy buena forma la robustez y manejo de tráfico de la capa de Enlace de Datos y la escalabilidad y flexibilidad de la capa de Red (Fig. 2-1). Cuando es usado en conjunto con

otras tecnologías estándares, MPLS permitirá a las empresas proveedoras de servicios de comunicaciones habilitar en sus redes servicios de valor agregado tales como:

a.- Ingeniería de Tráfico.

b.- Redes Privadas Virtuales (VPN)

c.- Calidad de Servicio (QoS)

Fig. 2-1.- MPLS en el modelo OSI

2.1.2 MPLS - Características Básicas

Multiprotocol Label Switching fue desarrollado para aprovechar la alta penetración de las redes IP actuales basadas en IP ROUTING fortaleciéndolas con la versatilidad que ofrece tecnologías de capa 3 como el IP SWICHTING o conmutación basada en cache que por ejemplo proporciona CEF (Cisco Express Forwarding) en equipos Cisco.

MPLS es una tecnología de reenvío de paquetes que utiliza etiquetas añadidas a los mismos en su ingreso al dominio MPLS para tomar las decisiones de reenvío; esta es una de sus principales características y es precisamente ésta quien le da a las redes MPLS una de sus principales ventajas tecnológicas:

La conmutación de etiquetas, se realiza independientemente del protocolo de enrutamiento

Las etiquetas de MPLS, usualmente corresponden a direcciones IP de destino, tal como el enrutamiento IP tradicional, pero según la necesidad del servicio puede incluir parámetros tales como: Calidad de servicio, direcciones IP de origen, circuitos de capa 2 (PVCs en redes ATM).

En resumen, podemos expresar que las características principales de una red MPLS serían:

- ✓ MPLS se apalanca de las fortalezas del IP SWITCHING como del CEF switching.
- ✓ MPLS se basa en el reenvío de paquetes mediante el análisis de sus etiquetas.
- ✓ Usualmente las etiquetas de MPLS corresponden a la dirección IP destino.
- ✓ MPLS fue diseñado para soportar múltiples protocolos de capa 3.

2.1.3 MPLS – Arquitectura

La arquitectura principal de MPLS esta compuesta principalmente por 2 componentes:

1. Plano de Control
2. Plano de Datos

2.1.3.1 Plano de Control

El plano de control, dentro de la arquitectura de MPLS, es el responsable del intercambio de la información de enrutamiento y de etiquetas entre todos los dispositivos adyacentes en un dominio MPLS. (Fig. 2-2)

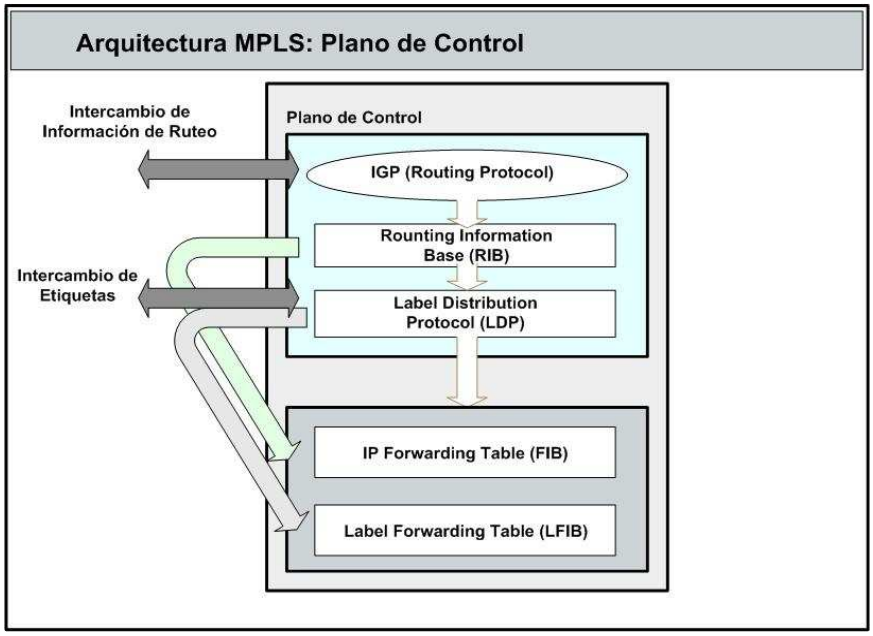


Fig. 2-2.- Plano de Control

El plano de control elabora la tabla de enrutamiento (Routing Information Base [RIB]) basado en el protocolo de enrutamiento que se este ejecutando en el dominio MPLS. Los protocolos que son soportados en MPLS son: Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), Intermediate System to Intermediate System (IS-IS), Routing Information Protocol (RIP) y el Border Gateway Protocol (BGP). Cabe anotar que únicamente en redes MPLS para el CORE se puede ejecutar como IGP los protocolos OSPF (Open Shortest Path First) y el IS-IS (Intermediate System – Intermediate

System) cuando se necesitan aplicaciones como Ingeniería de Tráfico o VPNs peer to peer, mientras que hacia los clientes finales si se puede ejecutar cualquier protocolo de enrutamiento dinámico o rutas estáticas según conveniencia.

Para el manejo de la información de la etiquetas, el plano de control utiliza protocolos especializados para esta labor, llamados: Label Exchange Protocol. Entre estos protocolos tenemos: MPLS Label Distribution Protocol (LDP), el protocolo propietario de Cisco Tag Distribution Protocol (TDP) y el BGP que se utiliza cuando se levantan VPNs en MPLS. Adicionalmente, se puede mencionar que para una aplicación especial como lo es la Ingenierìa de Tráfico o Traffic Engineering (TE) se utiliza el Resource Reservation Protocol (RSVP) para la propagación de esas etiquetas.

El plano de control es la responsable de la elaboración de 2 tablas fundamentales en la operación de redes MPLS:

1) Forwarding Información Base (FIB), mediante la información de la RIB.
2) Label Forwarding Información Base (LFIB), mediante el protocolo de intercambio de etiquetas escogido y la tabla RIB.

La tabla LFIB contiene los valores de las etiquetas asignadas y la asociación con la interfaz de salida para los paquetes con esa etiqueta.

2.1.3.2 Plano de Datos

El plano de datos o también conocida como plano de reenvíos, esta encargada como su nombre lo indica, del reenvío tanto de los paquetes y/o de etiquetas basándose en la información contenida en la FIB y LFIB independientemente de los protocolos escogidos para el enrutamiento y el intercambio de etiquetas. Fig. 2-3

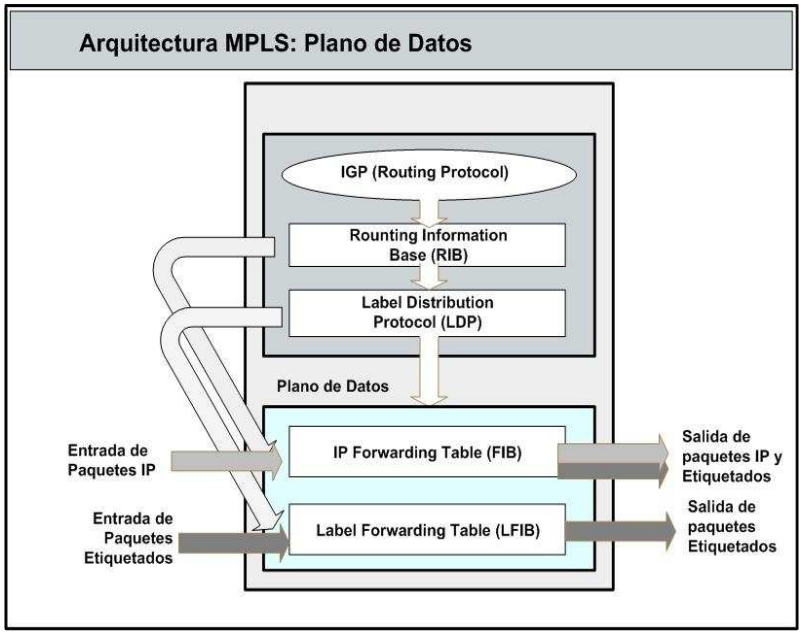


Fig. 2-3.- Plano de Datos

La funcionalidad del plano de datos varía según el dispositivo donde se este ejecutando, como veremos más adelante, en dispositivos LSR se limitará al reenvío de paquetes etiquetados y en dispositivos Edge LSR podrán ejecutarse tanto el reenvío de paquetes IP como de paquetes etiquetados.

2.1.4 Dispositivos MPLS

Los dos componentes básicos de toda red MPLS son:

I. Label Switch Router (LSR)

II. Edge Label Switch Router (E-LSR)

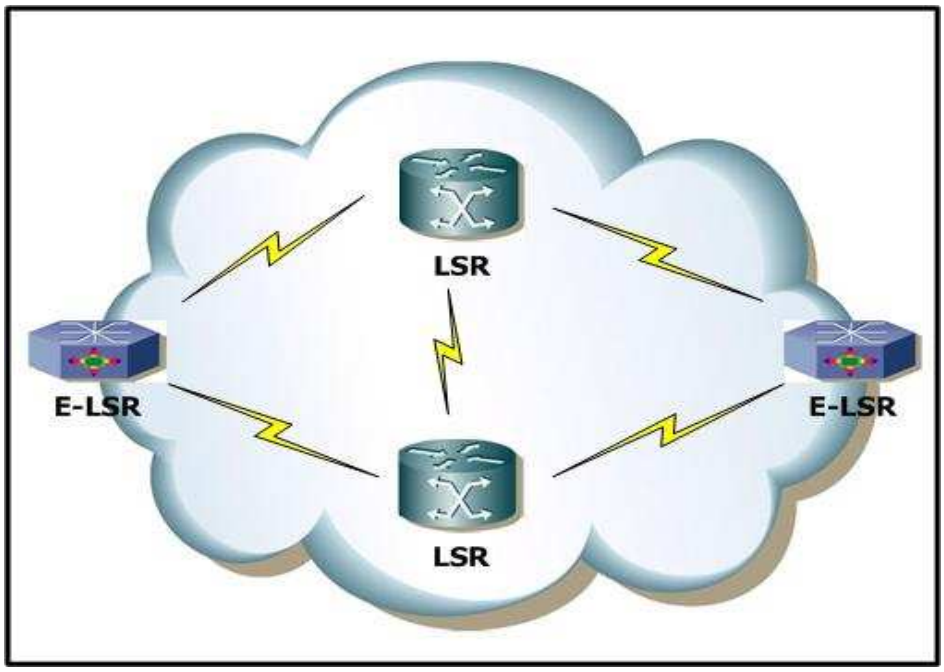


Fig. 2-4.- Dispositivos LSR

Los equipos LSRs y Edge-LSRs están usualmente habilitados para realizar un enrutamiento IP y una conmutación de etiquetas. Sus nombres, básicamente dependen de la ubicación dentro de un dominio MPLS, siendo los equipos core o centrales llamados LSR y los ubicados en el borde del dominio o frontera son llamados Edge-LSR.

Un equipo LSR también recibe el nombre de Provider Router (P) y su función primaria es la de direccionar paquetes dentro del dominio MPLS basándose en la conmutación de sus etiquetas.

Un equipo Edge-LSR es conocido también como Provider Egde Router (PE) y su función básica al ser frontera en un dominio MPLS es conocer los “dos mundos”; es decir, esta en la faculta de poder realizar conmutación de etiquetas hacia el interior del dominio MPLS así como enrutamiento tradicional basado en IP si la comunicación es hacia fuera del dominio MPLS.

Los equipos PE son los encargados de “etiquetar” a los paquetes cuando ingresan a la nube MPLS y por supuesto, de retirar las etiquetas cuando los paquetes abandonan la red MPLS.

2.1.4.1 Arquitectura de los equipos LSR (P)

La arquitectura de los equipos LSR constaría básicamente de los planos de control y de datos. La función primaria de cada dispositivo LSR son el intercambio de etiquetas con otros dispositivos LSRs y el direccionamiento de los paquetes que ya han sido etiquetados. Para esto, cada LSR requiere de un protocolo de enrutamiento de capa 3 (OSPF por ejemplo) y de un protocolo de intercambio de etiquetas (LDP por ejemplo). Fig.2-5

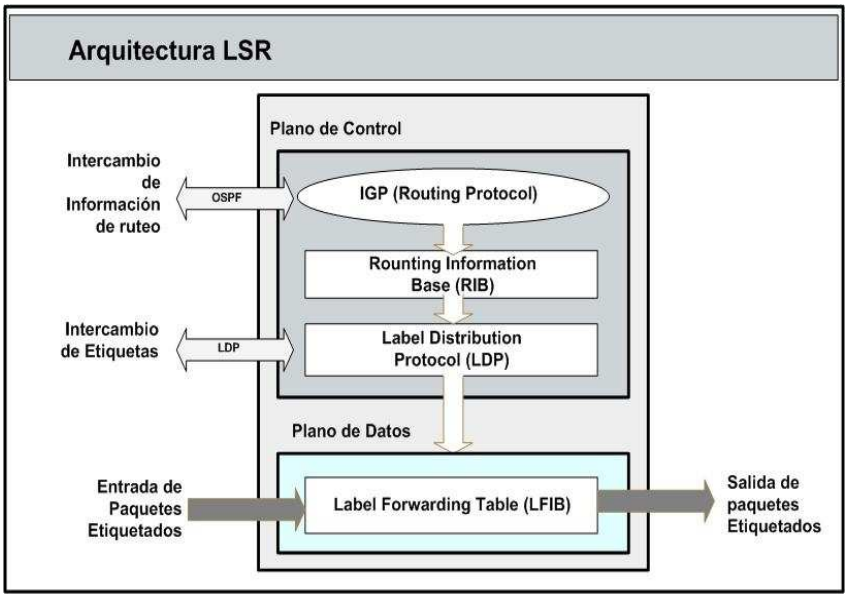


Fig. 2-5.- Arquitectura de un LSR

2.1.4.2. Arquitectura de los equipos Edge-LSR (PE)

Estos equipos adicional a su labor (como LSR) de reenviar paquetes etiquetados, también pueden reenviar paquetes IP hacia y desde una red de dominio MPLS, las siguientes combinaciones se pueden presentar en las operaciones de este equipo:

- ✓ Recibir un paquete IP y reenviarlo como paquete IP. (En base a su dirección de destino).
- ✓ Recibir un paquete IP y después de etiquetarlo, reenviarlo como un paquete etiquetado.
- ✓ Recibir un paquete etiquetado y después de un intercambio de etiqueta, reenviarlo como paquete etiquetado.
- ✓ Recibir un paquete etiquetado y después de un retiro de etiqueta, reenviarlo como paquete IP.

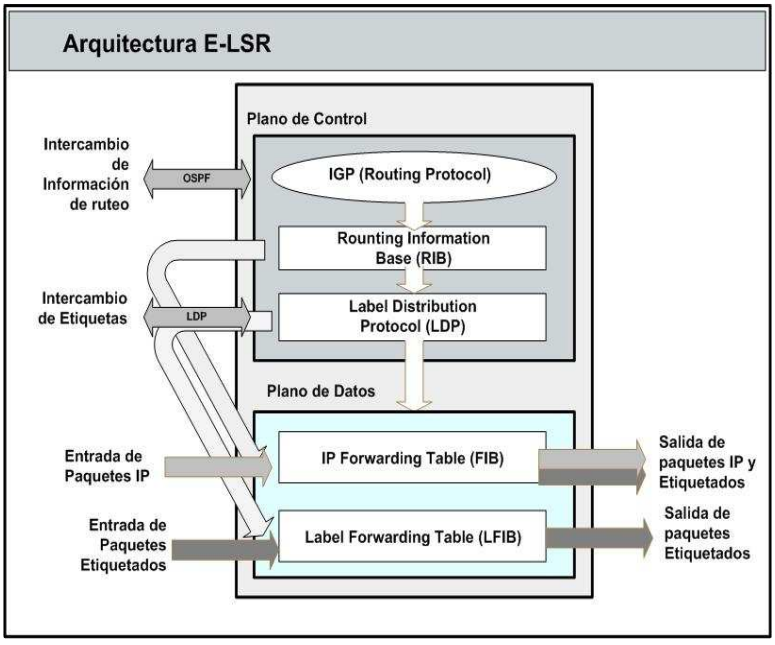


Fig. 2-6.- Arquitectura de un Edge-LSR (PE)

2.2 Teoría de Etiquetas y Manejo de Pilas.

Como hemos visto en los apartados anteriores, la fortaleza de las redes MPLS radica en su rápido análisis de la cabecera de los paquetes (solo analiza la etiqueta MPLS) con lo cual se toma rápidamente las decisiones de reenvío y se disminuye el consumo del procesador en los equipos de capa 3. En los articulados siguientes nos dispondremos a conocer con el mayor detalle posible acerca de estas etiquetas MPLS y su teoría del manejo de colas y de los principales actores que le dan a MPLS los criterios de reenvío de paquetes “etiquetados”.

2.2.1 Etiquetas MPLS

Las etiquetas MPLS son paquetes de 4 bytes, de longitud fija, que son insertados por los equipos LSR cuando los paquetes transitan por un dominio MPLS, sirviendo estas etiquetas para determinar las decisiones de reenvío para estos paquetes e incluso el tratamiento que se le dará durante su transito por la red, si tuvieren configurado calidad de servicio QoS.

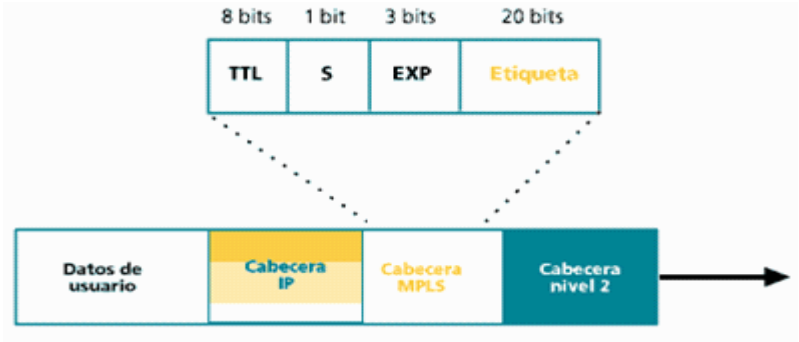


Fig. 2-7.- Ubicación de la etiqueta MPLS en modo de paquetes. (Frame – Mode)

Las etiquetas MPLS, tienen validez local, es decir, cada LSR colocará su propia etiqueta según la FEC (Forwarding Equivalence Class) que este en ese momento en su registro. Sin embargo a esta

independencia, cada cierto tiempo se producirá un intercambio de FECs entre equipos LSRs adyacentes.

2.2.1.1 Forwarding Equivalence Class - FEC

La tabla FEC es una tabla que crea cada router LSR conforme va etiquetando los paquetes que transitan por él. Esta tabla se va llenando con las estadísticas de etiquetado y de envío de cada paquete, es decir, paquetes que han tenido un trato similar en el reenvío corresponderán a una misma FEC. Cuando un paquete nuevo ingresa al router LSR este consultará la FEC actual en su registro y validará parámetros como dirección de destino, calidad de servicio asignada para poder asignar un valor de etiqueta conforme al mapeo que haga con la FEC. En caso de no existir una FEC para ese paquete, se procederá a la creación de una FEC (para ese paquete) que servirá luego para paquetes que ingresen con similares características.

MPLS utiliza reenvío de paquetes basadas en FECs para convertir redes IP NO orientadas a la conexión en redes orientadas a la conexión.

2.2.1.2 Formato de las Etiquetas MPLS

La siguiente figura (Fig. 2-8) describe la composición de una etiqueta MPLS.

Fig. 2-8.- Etiqueta MPLS y sus campos.

Los 32 bits (4 bytes) de longitud de cada etiqueta MPLS, se componen de los siguientes campos:

LABEL: Son 20 bits de longitud para este campo, básicamente aquí se define el nombre (valor) de la etiqueta asignada para ese paquete. Los valores del 0 al 15 son reservadas.

EXP: Estos 3 bits asignadas a este campo, utilizadas básicamente para indicar la clase de servicio que tendrá ese paquete. CoS (Class of Service).

S: Este bit es utilizado para manejar la pila de etiquetas, esto quiere decir que MPLS permite etiquetar con múltiples etiquetas a los paquetes. Si este bit esta marcado (1), esto indica que esta etiqueta es la última asignada.

TTL: Time-to-Live, este campo, al igual que en cabeceras IP normales, tiene el afán de evitar loops (círculos de transito) de paquetes.

Cuando MPLS esta corriendo en modo paquetes (Frame-Mode) la etiqueta es insertada entre la cabecera de la capa 2 y 3, con la excepción de redes ATM (Cell-mode) donde MPLS utiliza las propias celdas ATM (VPI/VCI) para definir la etiqueta.

El alcance de esta tesis, se enfocará en el modelo Frame-Mode que es el de mayor cobertura en la industria.

2.2.2 Pilas de Etiquetas MPLS

En redes MPLS, usualmente, se asigna una etiqueta por cada paquete; sin embargo, estas redes están en plena capacidad de insertar dos o más etiquetas (pila de etiquetas) a cada paquete según la necesidad y tratamiento que se les quiera otorgar a estos paquetes.

Aquí es donde entra en operación el bit S anteriormente mencionado, el cual indica cuando esta marcado con 1, que esa etiqueta es la última antes de iniciar los bits de información del cliente Fig. 2-9. A pesar de recibir una pila de etiquetas, cada LSR solo trabajará con la primera etiqueta de la pila, esto es muy importante puesto que las etiquetas intermedias solo serán tomadas en cuenta a medida que las etiquetas de borde se vayan retirando.

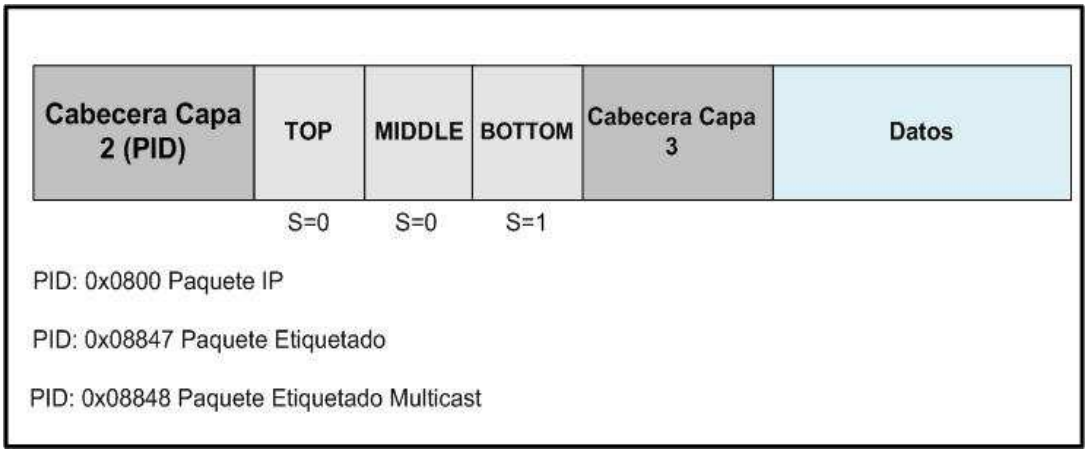


Fig. 2-9.- Formato de una pila de etiquetas

Pero, ¿Cuándo se necesitarían varias etiquetas? La respuesta a esta pregunta sería, depende de lo que se quiera hacer con ese paquete. A continuación detallamos algunos escenarios posibles:

- Cuando se levantan VPNs (Virtual Private Networks) sobre redes MPLS: Aquí, se requerirán de 2 etiquetas MPLS, la primera indicará el router de salida y la segunda identificará la VPN a la que pertenece dicho paquete marcado.
- Cuando se realiza Ingeniería de Tráfico (TE – Traffic Engineering) sobre redes MPLS: En este escenario se utilizarán al menos 2 etiquetas MPLS, la primera identificará al punto final (end-point of TE tunnel) del túnel levantado para realizar la ingeniería de tráfico y la siguiente etiqueta marcará el punto de destino del paquete.
- Cuando se levantan VPNs sobre túneles TE: Aquí se utilizarán tres o más etiquetas y resulta de la combinación de los anteriores escenarios.

En la siguiente figura se puede apreciar un ejemplo de una pila de etiquetas cuando es utilizada en un túnel TE sobre MPLS.

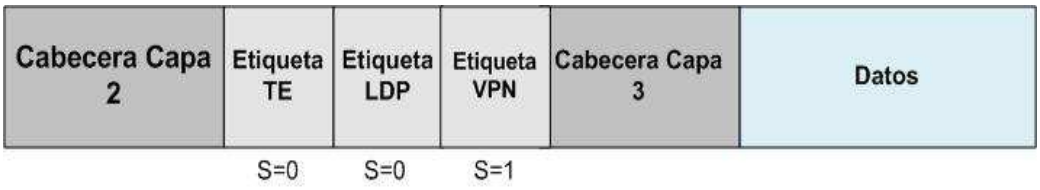


Fig. 2-10.- Ejemplo de una pila de etiquetas

La primera etiqueta es usada para conmutar el paquete a lo largo de la red MPLS, en este caso es la etiqueta que indica el punto final del túnel TE.

Las etiquetas intermedias, serán ignoradas por los routers intermedios. En este caso, serán utilizadas para identificar el router de salida y la VPN asociada para ese paquete.

2.2.3 Asignación de Etiquetas y su Distribución

En este apartado identificaremos la forma en la que el LABEL DISTRIBUTION PROTOCOL (LDP) se encarga de asignar y distribuir las etiquetas y las tablas FEC entre todos los equipos LSR participantes del dominio MPLS.

2.2.3.1 Estableciendo Sesiones LDP con LSRs Adyacentes.

La forma de establecer una sesión LDP con equipos vecinos, se realiza en dos pasos:

1. Mensajes HELLO: son mensajes enviados periódicamente (cada 5 sec) por cada interfaz MPLS habilitada; este mensaje es enviado usando protocolo UDP (User Datagram Protocol) por el puerto 646 utilizando la dirección de multicast (tráfico multidestino) 224.0.0.2 para que llegue a todos los routers de la subred.

2. Los routers que reciban este mensaje HELLO y estén habilitados con MPLS, responderán a este mensaje intentando abrir una sesión TCP con el router emisor del mensaje HELLO; esta sesión sería levantada utilizando el puerto 646.

Fig. 2-11.- Paquete Hello y sus campos.

Es importante acotar que el campo LDP ID es usado para identificar el router origen y el LABEL SPACE que define la forma de asignar etiquetas: Por plataforma o por interfaz.

En el siguiente gráfico (Fig. 2-12) se muestra el procedimiento de descubrimiento de vecinos LDP en un dominio MPLS. Se puede apreciar como los equipos habilitados con MPLS envían paquetes HELLO a todos sus vecinos MPLS; estos responderán a este mensaje levantando una sesión TCP. Los equipos con mayor IP de loopback o IP de interfaz configurada será quien genere la sesión TCP. Todos los equipos continuarán enviado paquetes HELLO para descubrir cualquier vecino nuevo o detectar fallas.

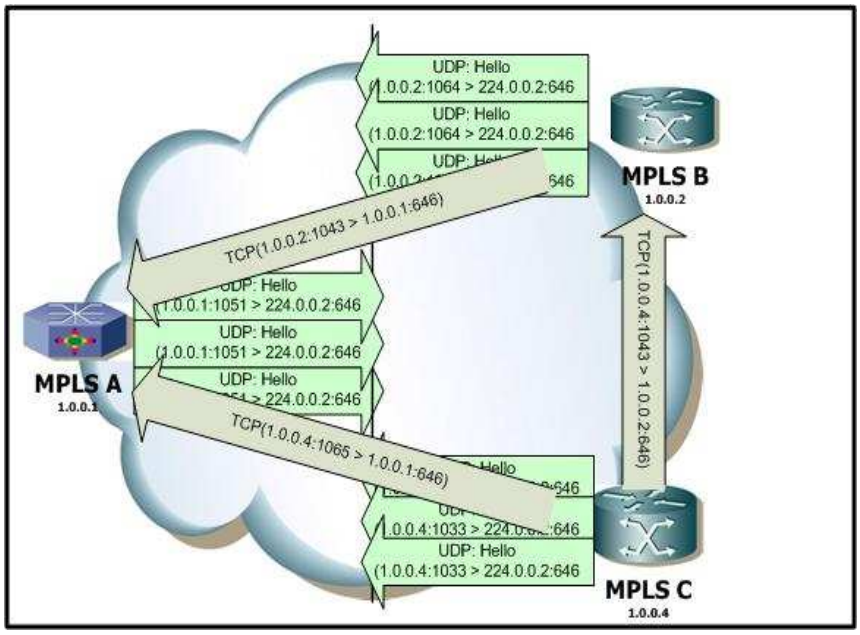


Fig. 2-12.- Descubriendo vecinos LDP

Después de inicializada la sesión TCP, estos equipos comenzarán a intercambiar la información de las etiquetas asignadas por ellos.

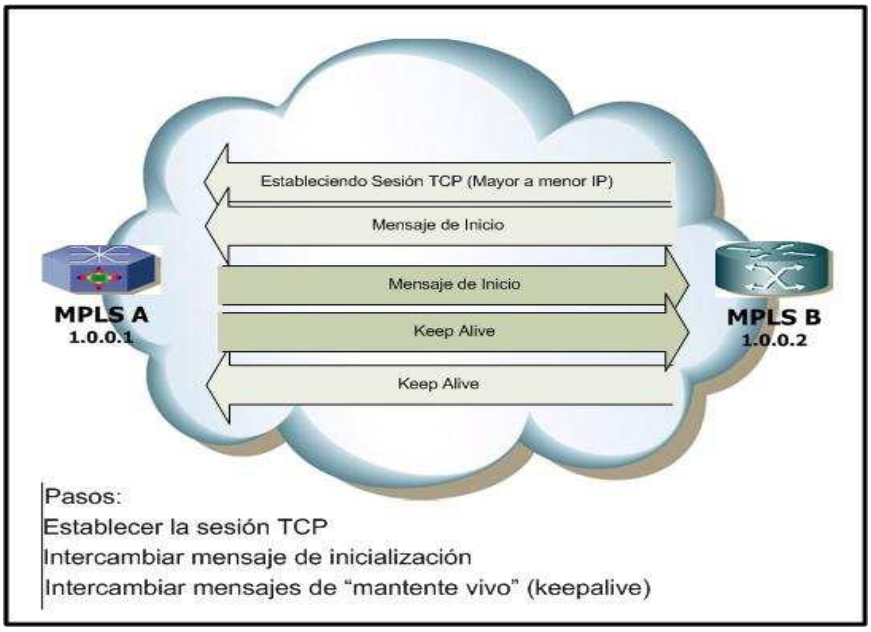


Fig. 2-13.- Negociación de la sesión LDP

2.2.3.2 Estableciendo Sesiones LDP con LSRs NO Adyacentes.

La forma en que los equipos LSR encuentran vecinos LDP que no son adyacentes, es muy similar al proceso que se emplea cuando si lo son, el único punto de divergencia es que no se utiliza una dirección multicast para el descubrimiento, sino una dirección UNICAST (la dirección de ese vecino) en los paquetes HELLO.

Cuando un vecino LDP es descubierto, el siguiente proceso para levantar la sesión TCP es similar al utilizado con routers adyacentes.

2.3 Frame – Mode MPLS (MPLS en redes de Paquetes de tamaño variable)

Con todos los conceptos previamente vistos, estamos ya en la posibilidad de cubrir y analizar detalles específicos de MPLS ejecutándose sobre una red de transmisión de paquetes (Frame mode) que es la base del desarrollo de este trabajo de tesis.

En la industria actualmente se pueden encontrar dos plataformas donde se ejecuta el protocolo MPLS: en redes de envío de paquetes (Frame Mode) como redes Frame Relay, Ethernet entre otras y redes de envío de celdas (Cell Mode) que se basan en tecnología ATM.

Como hemos visto, en el modo de paquetes, MPLS se basa en la inserción de una etiqueta en la cabecera de los paquetes IP, ubicándola entre la información de capa 2 y de capa 3; sin embargo, en redes ATM (MPLS/ATM) esta inserción no es posible dado que las celdas utilizadas son ya de tamaño fijo y no se permite la inserción de bits adicionales, por ello en esa tecnología se "reutiliza" los campos de los VPI/VCI para que estos sean utilizados como identificadores de las celdas y realizar el proceso de conmutación de celdas según estas el valor que se le haya asignado como etiqueta a cada VCI.

2.3.1 Distribución de Etiquetas en FRAME - MODE

Como sabemos, MPLS inserta una un campo ETIQUETA en los paquetes IP que luego será utilizado para tomar la decisión de reenvío durante su transito por el dominio MPLS. Y aunque las etiquetas insertadas tienen únicamente validez local, deben ser comunicadas a los vecinos LSR directamente accesibles.

Para esto, se plantearon 2 opciones:

I. Modificar los actuales protocolos de enrutamiento para que permitan agregar estos campos para difundir la información de las etiquetas.
II. Crear un nuevo protocolo para el intercambio de etiquetas.

Problema para la opción I: Habría que modificar los protocolos: OSPF, EIGRP, IS-IS, RIP…y cualquier otro protocolo que se desarrollara, lo cual a más de todo el trabajo que habría que invertir en estos cambios, seguramente causaría un serio problema de incompatibilidad dado que no todos los routers soportan todos los IGP mencionados.

Por tanto, la Internet Engineering Task Force (IETF) optó por el desarrollo del protocolo especializado en el intercambio de etiquetas – LDP.

2.3.2 Ruta Conmutada de Etiquetas (Label Switched Path -LSP)

La ruta conmutada de etiquetas (LSP) , es básicamente el camino que se forma al reenviar paquetes etiquetados de una manera asociados a una FEC, es decir la secuencia de equipos LSR por los que deberán transitar paquetes etiquetados de igual forma. Se puede decir que LSP en MPLS es similar en concepto a los circuitos virtuales en Frame Relay o ATM. El equipo que inicia la ruta se lo denomina cabecera o entrada y el que la termina se denomina cola o de salida, todos los demás equipos intermedios se denominan de core, todos estos, en su conjunto forman la ruta (LSP) por la que los paquetes etiquetados serán conmutados.

Estos equipos de entrada y salida, son encargados de insertar, remover o conmutar etiquetas. Es decir están en la capacidad de realizar IP routing o IP switching según sea el caso; mientras que los equipos de core solo pueden intercambiar etiquetas.

El encargado de distribuir de la etiquetas entre equipos LSR del dominio MPLS es el LDP, quién a su vez utiliza la información contenida en la RIB acerca del NEXT HOP (siguiente salto) de cada equipo para determinar la ruta más corta hacía los destinos de los paquetes, es decir levantar

el LSP. Adicionalmente, se indica que las rutas LSP son unidireccionales, es decir no pueden ser utilizadas para responder tráfico, entonces se deberá asignar un LSP de retorno.

Cabe indicar que se debe evitar al momento de la configuración del IGP habilitar la sumarización de rutas, dado que esto provocaría que el LSP se rompa en dos tramos.

2.3.3 Distribución de Etiquetas – UP y Downstream

En operación normal, cada LSR en un dominio MPLS asignará de forma independiente a cada red registrada en su tabla de encaminamiento (tabla de enrutamiento) una etiqueta de vigencia local.

Esta etiqueta será comunicada a cada LSR vecino con el que haya iniciado una sesión LDP; cuando este envía los valores de sus etiquetas a sus vecinos se conoce como VECINO UPSTREAM y el equipo LSR que recibe las etiquetas se convierte en vecino DOWNSTREAM.

Cuando las etiquetas son enviadas por pedido de un equipo vecino, se define el downstream bajo demando y cuando es enviado sin ser requerido, downstream sin solicitar. Fig. 2-14

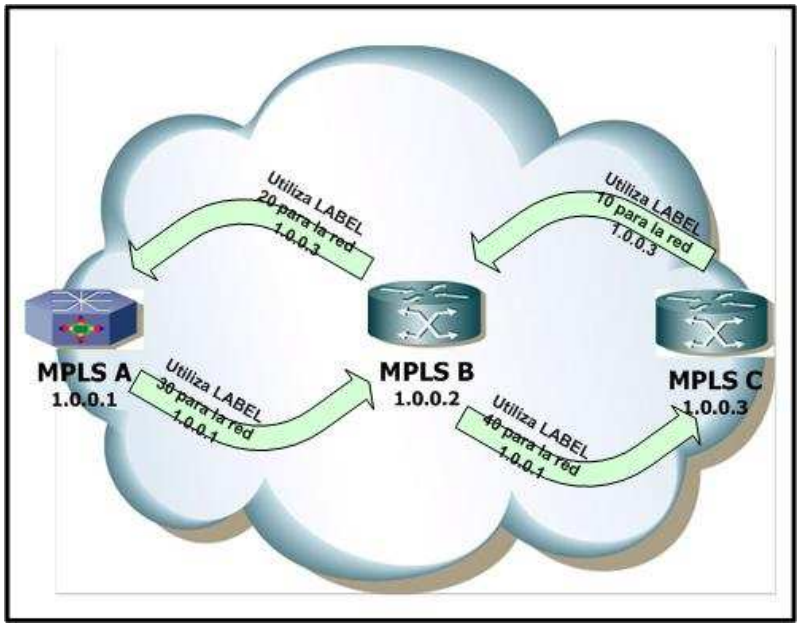


Fig. 2-14 DOWNSTREAM sin solicitar

2.3.4 Estableciendo una sesión MPLS

Para que una red MPLS se considere plenamente funcional, el IGP (Interior Gateway Protocol) y el LDP (Label Distribution Protocol) deben haber generado las siguientes tablas:

- ✓ RIB: Routing Information Base, esta tabla contiene la información de enrutamiento de la red obtenida por el protocolo IGP escogido, en nuestro caso será OSPF e incluye información el next hop (siguiente salto) en la red IP.
- ✓ LIB: Label Information Base, esta tabla es elaborada por el protocolo LDP y contiene las etiquetas locales asignadas en cada equipo LSR y las etiquetas que sus vecinos han asignado.

- ✓ FIB: Forwarding Information Base, es una tabla que se forma con la información contenida en la tabla RIB que contiene básicamente el siguiente LSR asignado para cada paquete que transite por el LSR local y la etiqueta que este le asignará.
- ✓ LFIB: Label Forwarding Information Base, esta tabla contiene información que proviene del IGP (RIB) y el LDP (LIB) y contiene la etiqueta actual del paquete, la nueva que se asignará y su siguiente LSR destino (next hop).

Una vez que los equipos LSR (Edge y de core) hayan intercambiado sus etiquetas locales por el método DOWNSTREAM y las tablas mencionadas anteriormente estén completas, presentamos el siguiente escenario de operación:

A.- Ingresa un paquete IP (no etiquetado) con destino a una red de la nube MPLS. (Fig. 2-15)

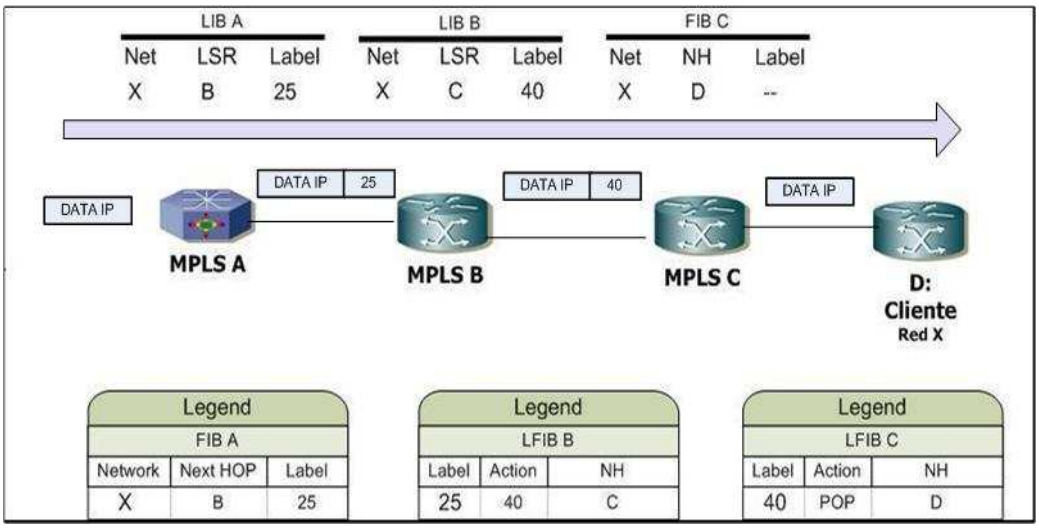


Fig. 2-15.- Red MPLS y transito de paquetes

Eventos:

1) El equipo Edge-LSR (A) analiza su cabecera, detecta que no esta etiquetado y mediante su tabla RIB sabe que su destino estará dentro de la nube MPLS, por lo tanto le inserta una etiqueta (según la tabla FIB) y lo envía al siguiente destino (LSP establecido).
2) El Equipo Core LSR (B) recibe el paquete etiquetado, analiza su tabla LFIB y conforme al siguiente salto (LSR) cambia la etiqueta.
3) El equipo Edge-LSR (C) retira la etiqueta (puesto que el paquete ha llegado a su destino y sale del dominio MPLS) y encamina hacia el destino utilizando su tabla LFIB.

En la mayoría de redes actuales utiliza la técnica PHP (Penultimote Hop Popping) se retira la etiqueta en el penúltimo router MPLS a fin de que al llegar al equipo Edge este no realice una búsqueda en la tabla LFIB (dado que no hay más nodos MPLS adelante) y solo realice la búsqueda en la tabla FIB para llegar al destino fuera de la red MPLS.

2.4 Aplicaciones sobre Redes IP-MPLS

Sin lugar a dudas las redes MPLS ofrecen en la actualidad una ventaja competitiva a las empresas proveedores de servicios que las han desplegado en detrimento de las empresas que aún mantienen su infraestructura anterior tales como redes IP tradicionales, redes ATM, redes Frame relay, etc.

Entre las bondades de redes MPLS podemos destacar su rápida implementación sobre infraestructura existente, la transparencia de protocolo de enrutado (IP, IPX, Apple Talk), la diversidad de transporte que soporta y sobre todo la estabilidad y escalabilidad que ofrece su conmutación de etiquetas.

Los servicios o aplicaciones que se ofrecen sobre redes IP-MPLS podemos mencionar:

- Unicast IP Routing
- Multicast IP Routing
- Redes Privadas Virtuales – VPNs
- Calidad de Servicio – QoS
- Ingeniería de Tráfico – TE

En las siguientes líneas expresaremos los criterios básicos de las aplicaciones más importantes que se pueden desarrollar sobre redes MPLS.

Unicast IP Routing

Esta es la aplicación básica de las redes MPLS y se refiere simplemente al enrutamiento IP pero no basado el la dirección IP destino como normalmente se realiza sino que mediante la conmutación de etiquetas.

Este servicio ofrece 2 mejoras significativas sobre el enrutamiento tradicional:

- La habilidad de usar etiquetas como criterio de reenvío de paquetes.
- La posibilidad de transportar una pila de etiquetas asignadas al paquete.

Esa habilidad de transportar pilas de etiquetas, es la base para aplicaciones más robustas y complicadas como lo son las VPNs y la ingeniería de tráfico.

Y como hemos acotado antes, la habilidad de utilizar la tabla LFIB como criterio para el reenvío permite realizar búsquedas más eficientes con lo cual disminuye el consumo del procesador. Adicional, también provee soporte para servicios orientados a la conexión debido a la FEC ya que se establece un circuito virtual de conmutación llamado LSP.

Multicast IP Routing

Las redes MPLS permiten el enrutamiento a varios destinatarios simultáneamente. Para este efecto se utiliza el protocolo PIM (Protocol Independet Multicast propietario de Cisco) en su versión 2 con extensión para MPLS que permite la propagación de la información de enrutamiento y de las etiquetas.

Al igual que con el Unicast, aquí las FEC sirven para la toma de decisión de reenvío, con la diferencia de que a cada FEC están asociadas varias direcciones destino y no solo una. Un buen ejemplo de esta aplicación es la video conferencia bajo demanda.

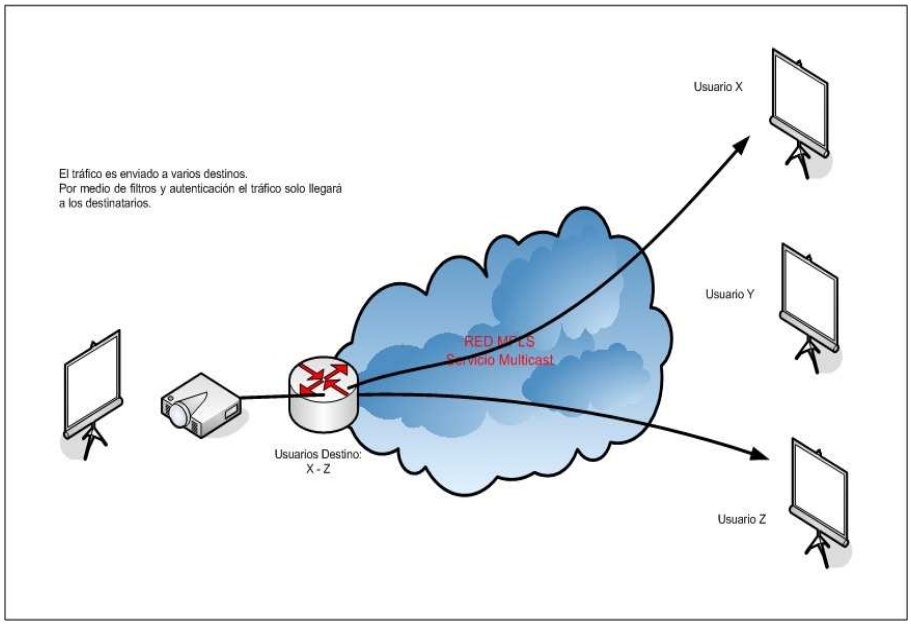


Fig. 2-16.- Video bajo demanda

Redes Privadas Virtuales – VPN

En MPLS las redes privadas virtuales son por excelencia el producto estrella para las empresas proveedoras de servicio dado que sin esta división virtual de la red, el negocio como tal no tendría sentido.

Para cada usuario de una VPN/MPLS. La red aparece como una red privada mediante la cual se puede acceder a cualquier otro punto de la empresa (cliente) que este conectado a la misma VPN, pero no a otras VPNs (sitios) de otra organización.

MPLS permite implementar VPNs que soporten servicios como:

- Multicast
- QoS (Calidad de Servicio)

- Tráfico de Voz: VoIP – ToIP
- Centralizar servicios: Web posting por ejemplo.

Las redes de los clientes son aprendidas mediante cualquier protocolo de enrutamiento dinámico desde el router de borde del cliente (CE) o mediante protocolo BGP si es aprendido desde otro router de la red MPLS.

Las VPNs sobre MPLS utilizan 2 etiquetas:

- La primera etiqueta indica el router de salida
- La segunda etiqueta indica la interfaz de salida en el router de egreso.

El LDP es necesario para enlazar la primera etiqueta con el camino que deberá seguir a lo largo de la nube MPLS hasta el router de salida, es decir indicará el Label switch path o camino de conmutación de la etiquetas mientras que el MP-BGP (Multiprotocol BGP) permite propagar la información de enrutamiento de la VPN y las etiquetas dentro del domino MPLS. Para esta aplicación, la FEC (Forwarding equivalente Class) corresponde al identificador de la VPN.

En los siguientes apartados explicaremos más detalle de las redes privadas virtuales sobre MPLS.

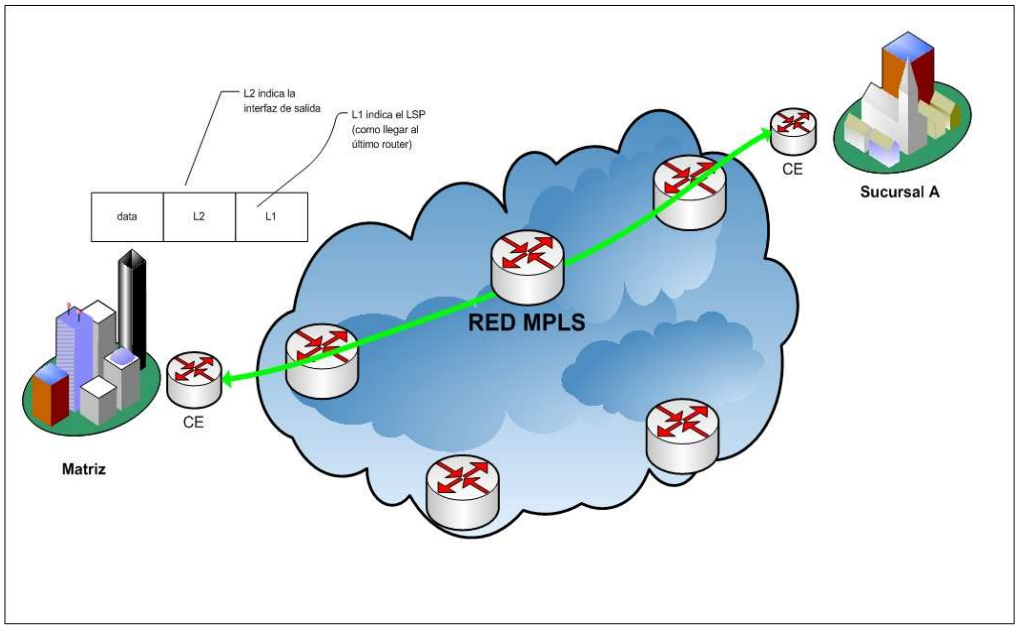


Fig. 2-17.- Virtual Private Network – VPN

Calidad de Servicio – QoS

Como hemos visto anteriormente, las etiquetas MPLS tienen un campo llamado EXP (experimental) mismo que es un campo de 3 bits que sirve para determinar el tratamiento que se le debe ofrecer al paquete según la tabla de calidad de servicio que el proveedor haya definido previamente.

Este tratamiento puede incluir acciones como:

- Garantizar ancho de banda.
- Mejorar retardos, ejemplo: Aplicaciones VoIP y videoconferencia.
- Ofrecer rutas no congestionadas.
- Priorizar un tipo de tráfico sobre otro, ejemplo: VoIP sobre http.

- Utilización dinámica e inteligente del canal: Si un caudal no se utiliza se reasigna ese ancho de banda a otro requerimiento.

Otra opción que se tiene para ofrecer calidad de servicio es poder establecer caminos diferenciados (LSPs) para cada tipo de tráfico, siendo la más eficiente asignada para los datos críticos. Sin embargo, la utilización de los bits experimentales es la técnica más difundida para la aplicación de QoS.

Para este servicio en redes MPLS, la FEC corresponde a la combinación de la red destino y su clase de servicio asignado.

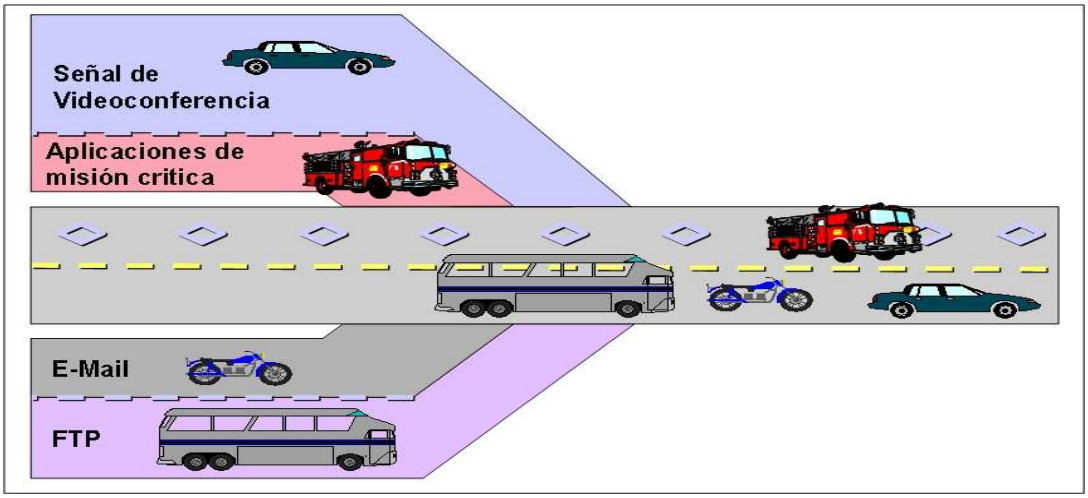


Fig. 2-18.- Calidad de Servicio

Ingeniería de Tráfico – TE

La Ingeniería de Tráfico (TE) en redes MPLS, permite determinar la ruta más eficiente (no necesariamente la más corta) en base a los requerimientos del flujo de datos buscando siempre la optimización de los recursos y desempeño de la red

Lo anterior apunta a un objetivo general, que es minimizar la congestión al mismo tiempo que intentar incrementar la eficiencia de la utilización de los recursos.

TE permite a los administradores de la red poder realizar las siguientes actividades:

- Controlar el flujo del tráfico en la red.
- Reducir la congestión en la red.
- Optimizar la utilización de los recursos de la red.

Para poder implementar TE sobre redes MPLS, se requiere cumplir con los siguientes requerimientos:

- Cada LSR debe tener una visión completa de la red, y esto es solo posible si se selecciona a OSPF o IS-IS como protocolo de enrutamiento IGP.
- Cada LSR necesita información adicional acerca de los enlaces de la red. Esta información incluye recursos disponibles. OSPF y IS-IS tienen estas extensiones que permiten la propagación de esta información.
- El protocolo RSVP (Resource Reservation Protocol) es utilizado para establecer el tunel TE (la ruta más eficiente) y para propagar las etiquetas del TE.

2.5 IP – VPNs

2.5.1 Generalidades

Hasta ahora, todo lo que hemos visto funcionaría perfecto desde la visión de una empresa grande que desea comunicación con sus sucursales, funciona perfecto el esquema de enrutamiento basado en el intercambio de etiquetas, el establecimiento de las mejores rutas gracias al IGP (OSPF en nuestro caso) y la propagación de las etiquetas mediante el protocolo de distribución (LDP en nuestro caso); todo esto, visto desde la óptica de un cliente, más sin embargo desde la

óptica de una empresa proveedora de servicios, quien básicamente es quien tiene el capital suficiente para implementar una red a nivel nacional, con equipos que fácilmente superar los 200K dólares americanos (esto lo analizaremos más adelante en el capítulo de costos) tal como esta planteada la red generará más problemas que beneficios. Problemas de escasez y poca optimización de recursos, altos costos de renta de los servicios, compleja administración son entre otros los problemas que se enfrentaban las empresas cuando la única forma de conexión eran los enlaces punto a punto.

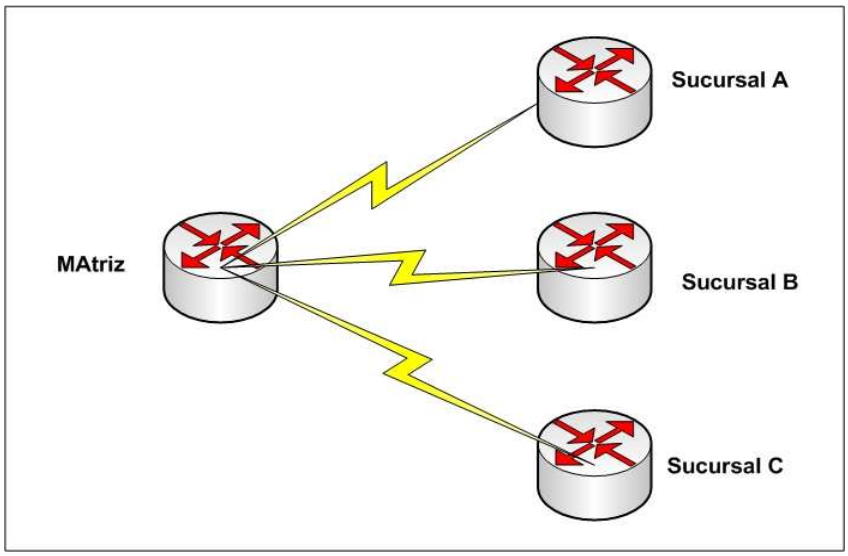


Fig. 2-19.- Conexiones Tradicionales Punto a Punto

Redes privadas virtuales (VPN) surgieron como la alternativa para rentabilizar y expandir el negocio de las telecomunicaciones. Estas surgieron con la aparición de la tecnología X.25 y Frame Relay que utilizaban circuitos virtuales para establecer conexiones punto a punto sobre la red compartida del proveedor de servicios. Estas tecnologías permitieron ofrecer conexiones compartidas sobre una misma red lo que se reflejó en una reducción de los costos y por ende en el interés de los usuarios a acceder a estas tecnologías.

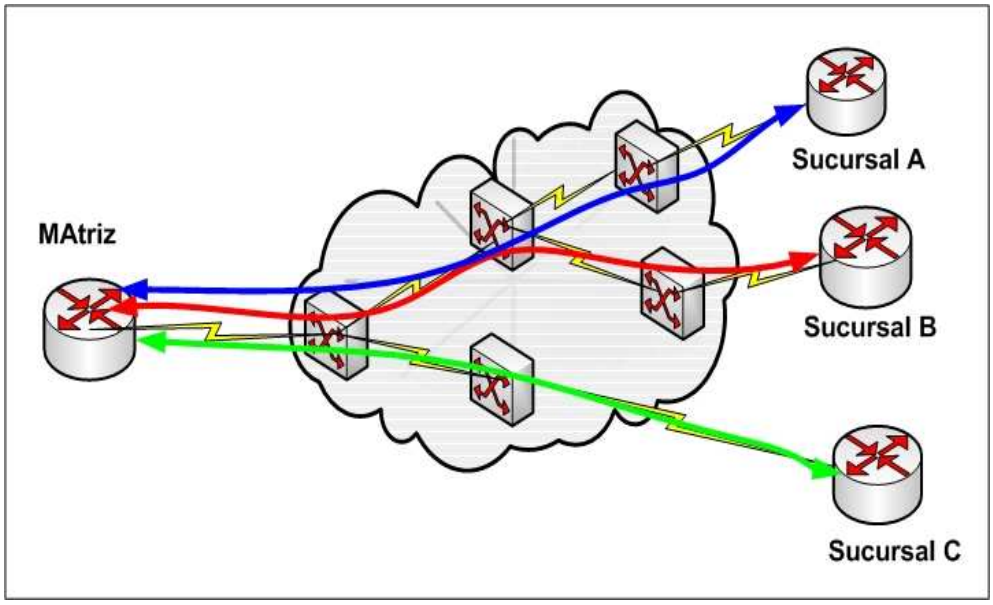


Fig. 2-20.- Circuitos virtuales sobre redes conmutadas.

2.5.2 Clasificación

A nivel de VPNs se consideran 2 clasificaciones según su forma de implementación:

- ✓ VPN Overlay (transparentes)
- ✓ VPN Peer to Peer (entre iguales)

Cuando el proveedor de servicios ofrece una conexión entre la matriz de la empresa contratante y sus sucursales a nivel de la capa de enlace de datos (Capa 2), se denominan redes overlay, dado que el proveedor estable las conexiones virtuales punto a punto pero solo a nivel de capa 2 mientras que el cliente es responsable de todas las capas superiores. Ejemplo de esta tecnología eran las conexiones ofrecidas sobre redes ATM y Frame Relay.

Cuando el protocolo IP logró su aceptación como estándar más utilizado para las redes de comunicaciones, muchos proveedores optaron por implementar un backbone de IP puro y para lograr establecer las VPNs se recurrió a lo que se conoce ahora como túneles IP y es cuando se desarrollaron las primeras versiones de VPNs de capa 3. Este tipo de VPN implica siempre aumentar el tamaño de la cabecera IP por el tunel que se esta levantando sea por IP security (IPsec) o por el método Generic Routing Encapsulation (GRE). De estos métodos, el GRE es el más sencillo de implementar, pero tiene la desventaja de enviar el tráfico de forma transparente (no cifrada) por lo que para redes compartidas como el Internet, no es una solución recomendable. El método de IPsec ofrece cifrado y autenticación pero solo soporta protocolo IP.

La desventaja principal de este tipo de VPNs se refiere al número de enlaces punto a punto virtuales que se deben establecer entre los sitios del cliente. La formula para calcular el número de enlaces virtuales que se deben establecer en el peor de los casos, para redes full mesh (conexión todos contra todos) es:

$$\frac{N^* (N-1)}{2}$$

Donde N es el número de puntos que tiene la red del cliente; es decir para una empresa mediana que cuenta con una matriz y 5 sucursales, el número total de enlaces virtuales que se deberán establecer asciendo a la cantidad de 15 para asegurar la conectividad total de su red.

Las redes Peer to Peer se presentan como alternativa ante el problema de la escalabilidad presentada por las redes Overlay, estas redes actúan de forma más cercana con el cliente, al aprender sus rutas (redes locales) y propagarlas por el backbone de la red del proveedor. Con esto, se logra que cualquier nodo de la red del proveedor sepa como llegar a cualquier sitio del cliente sin necesidad de levantar circuitos punto a punto virtuales.

Entre las desventajas de este modelo de VPN tenemos el conocimiento que el proveedor de servicios puede llegar a tener acerca del direccionamiento IP del cliente, y que el tiempo de convergencia de sus redes dependerá básicamente del proveedor que es quién propaga las rutas del cliente por su backbone. Adicional a esto se puede mencionar que una mala configuración del proveedor pudiera causar que el tráfico de varios clientes de pudieran mezclar y que se pudieran presentar problemas de redes privadas duplicadas entre los clientes.

2.5.3 VPN – MPLS

Las VPNs basadas en tecnología MPLS se apalancan con los beneficios de VPNs overlay y los beneficios de las VPNs peer to peer. Entre las características de las VPNs basadas en MPLS se pueden mencionar:

- Los equipos PE del proveedor participan en el proceso de enrutamiento con el cliente.
- Los equipos PE del proveedor transportan por separado las redes de los clientes, lo que implica una perfecta separación entre clientes.
- Los clientes pueden usar cualquier direccionamiento IP sin temor a una replicación con otro cliente.

En una red MPLS que ha implementado redes privadas virtuales, es muy similar a la arquitectura de las VPNs peer to peer cuando se utiliza un router dedicado por cada cliente, con la diferencia que en el esquema MPLS, el PE es en términos de hardware un solo dispositivo pero a nivel lógico se divide en varios “routers” virtuales por cada cliente. Este proceso es viable mediante lo que se conoce como: Virtual Routing Tables (VRF – Tablas virtuales de enrutamiento). Cada VRF contiene la información de enrutamiento de ese cliente (tabla RIB) y la tabla FIB que se va formando gracias a la activación del CEF.

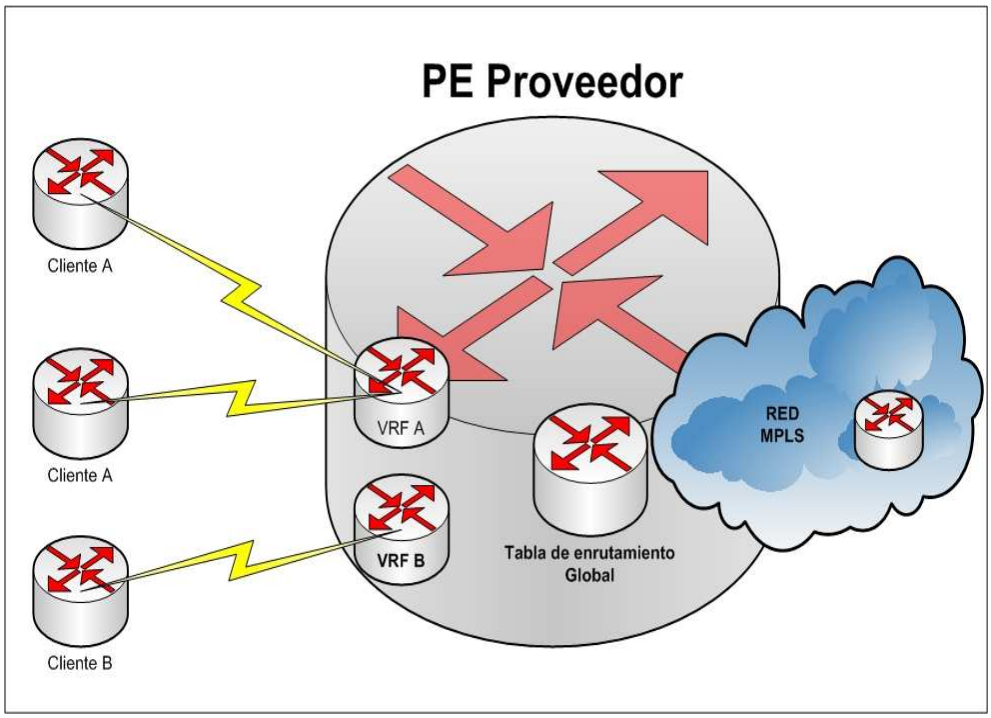


Fig. 2-21.- Arquitectura del PE en una VPN-MPLS

Una vez que el router PE aprende las rutas del (los) clientes es necesario hacer que los demás equipos del dominio MPLS las puedan aprender, para tal efecto presentamos las siguientes opciones y su análisis:

1.- Implementar un protocolo IGP dedicado por cada cliente para que sus rutas puedan propagarse.

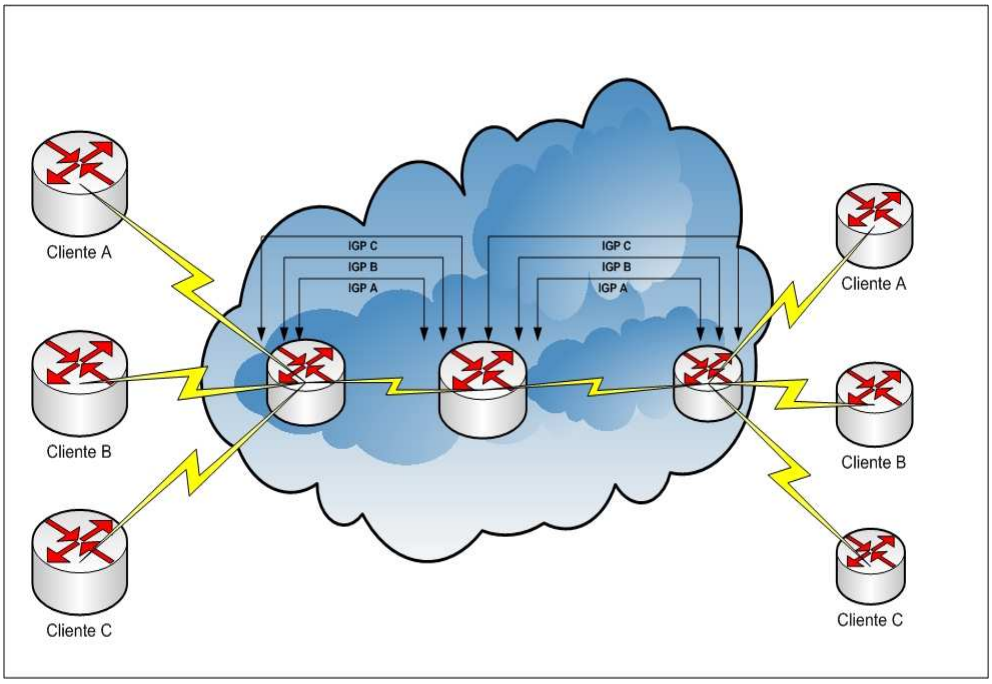


Fig. 2-22.- Propagar rutas con un IGP dedicado por cliente.

Este método puede conllevar las siguientes desventajas:

- Los equipos PE pueden llegar a tener una cantidad considerable de sesiones IGP ejecutándose.
- Los equipos P deberán transportar las rutas del cliente.

2.- Implementar un solo IGP que propague las rutas de los clientes a lo largo del dominio MPLS.

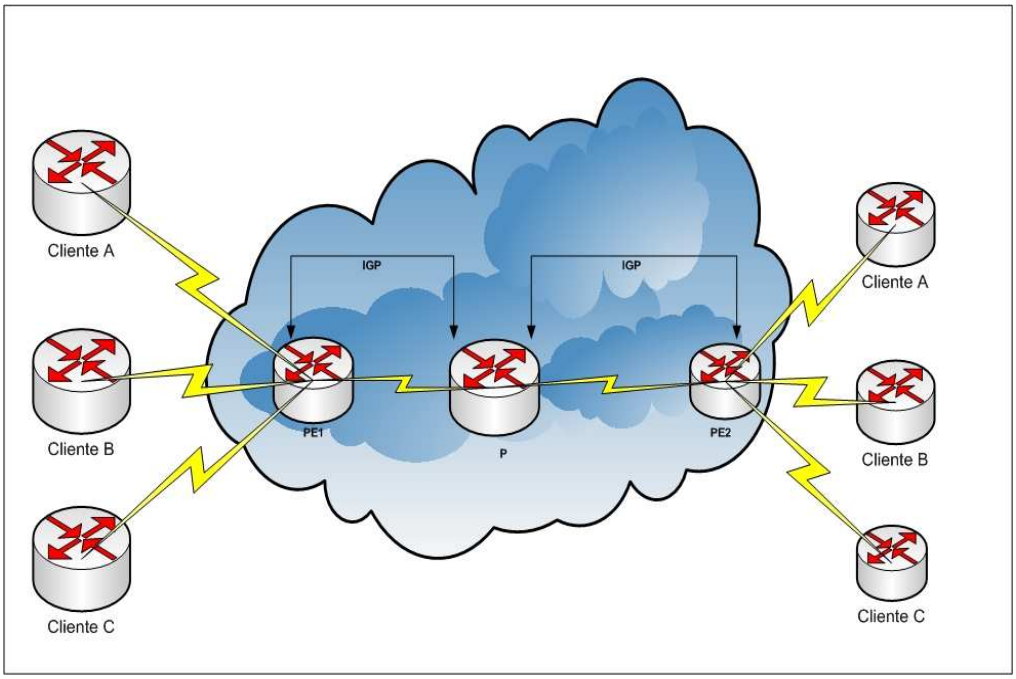


Fig. 2-23.- Propagar rutas con un solo IGP dedicado.

Este método a pesar de reducir el número de sesiones levantadas en los PE mantiene el inconveniente que hacer participar a los equipo P en el enrutamiento del cliente.

3.- El método efectivo que permite tanto evitar el número de protocolos de enrutamiento que se deben ejecutar y a la vez evitar que los equipos P conozcan las rutas del cliente consiste en implementar un protocolo que pueda transportar las rutas del cliente SOLO entre los equipos PE y utilizar las etiquetas MPLS para transportar los paquetes entre estos equipos PE.

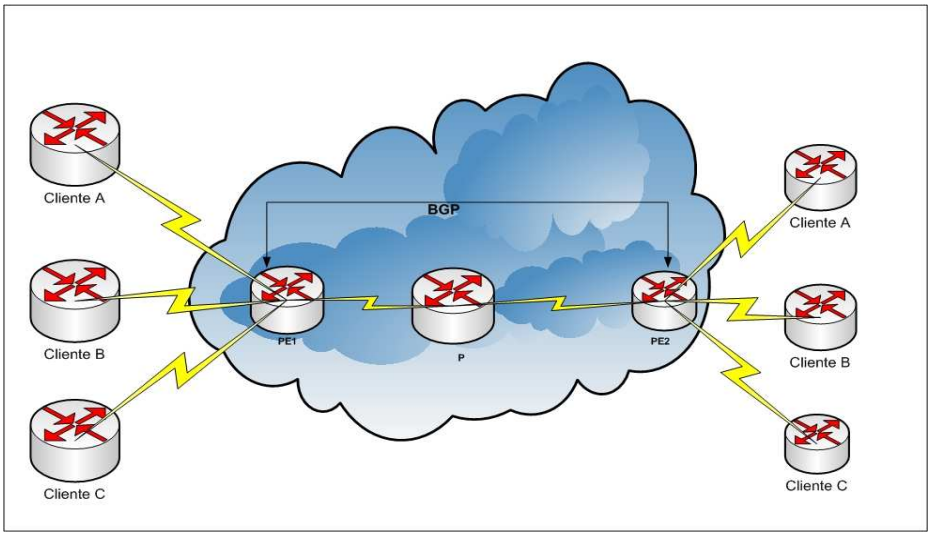


Fig. 2-24.- Propagación de rutas utilizando BGP

Este es el mejor método utilizado por los grandes proveedores para poder utilizar las VPNs de forma eficiente dado que BGP es el único protocolo de enrutamiento que soporta grandes cantidades de rutas y esto podría ocurrir por ejemplo si los PE pueden aprender rutas del Internet.

Sin embargo, aún continuamos un problema, ¿Cómo poder propagar redes privadas de los clientes repetidas? Este problema es solucionado agregándole una "marca" única a cada ruta aprendida por el BGP y esto es posible dada la riqueza de este protocolo en cuanto a atributos y cantidad de información que es capaz de transportar. (Ver subcapítulo BGP para mayores detalles de este protocolo).

2.5.3.1 Route Distinguishers - RD

Las RD marcas de 64 bits que son usadas solamente para transformar una red IPv4 de 32 bits de un cliente que no es única en una red de 96 bits totalmente única conocida como VPN

versión 4 o direcciones VPN IPv4. Con esta transformación se obtiene redes privadas de los clientes totalmente únicas dado que el marcador RD es impuesto por el proveedor.

VPNv4 son únicamente intercambiadas entre los equipos PE; ellas nunca podrán ser utilizadas o conocidas por los CE o equipos del cliente. Entre los equipos PE, BGP deberá por lo tanto poder intercambiar prefijos IPv4 o prefijos VPN-IPv4, debido a esta cualidad una sesión BGP levantada entre routers PE es conocida como MP – BGP o Multiprocol Border Gateway Protocol.

La forma de propagar las rutas del cliente a través de la red MPLS del proveedor se puede resumir en los siguientes pasos:

1. Cliente envía sus rutas hacia el PE, mediante rutas estáticas o cualquier protocolo IGP.
2. Los equipos PE añaden un prefijo a las redes del cliente, el prefijo RD convierte a las redes IPv4 en redes VPN IPv4.
3. Las redes VPN IPv4 son propagadas a los demás routers PE mediante el Multiprotocol Interior Border Gateway Protocol (MP-IBGP).
4. EL PE retira el prefijo RD convirtiendo a las redes del cliente nuevamente en redes IPv4.
5. Las redes del cliente son enviadas hacia la sucursal destino mediante rutas estáticas o cualquier IPG.

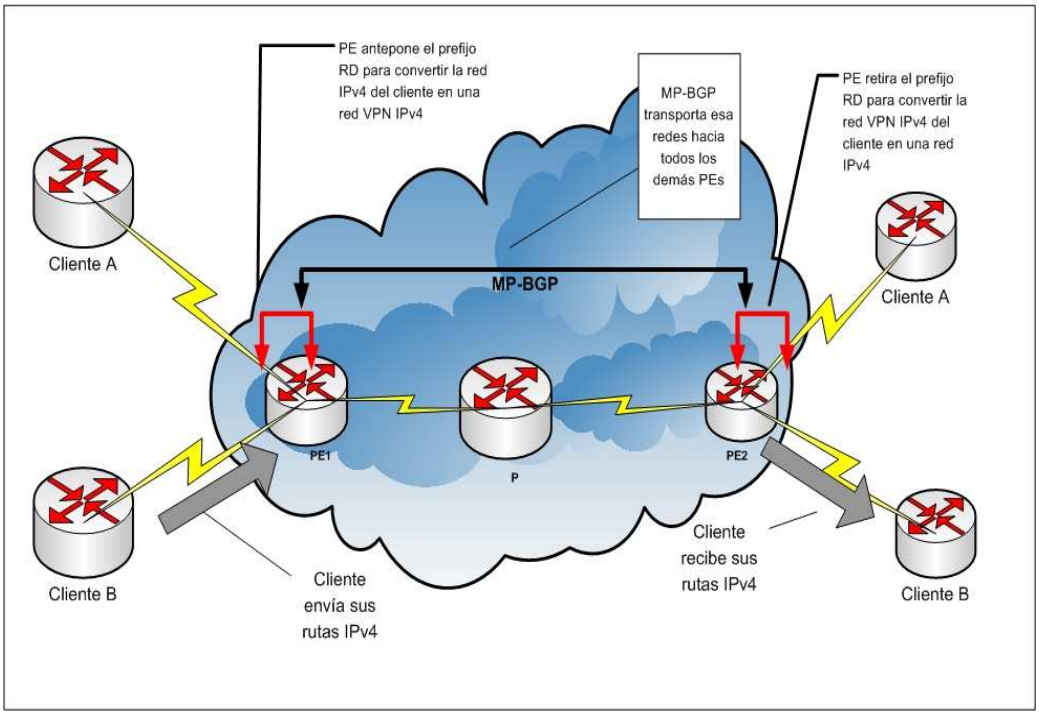


Fig. 2-25.- Forma de propagación de las redes VPN IPv4

2.5.3.2 Route Target - RT

Como hemos visto, las RD cumplen una función primaria básica, única y local: marcar las redes de los clientes (añadiéndoles 64 bits) para que puedan transitar por el backbone del proveedor sin el riesgo de ser repetida por algún otro cliente. Comúnmente, se asocia al valor del RD como el identificador de la VPN; sin embargo este diseño no contempla el soporte cuando se requiere una comunicación entre varias VPNs.

Entonces, cuando por alguna razón las empresas desean establecer comunicación entre una o varias de sus sucursales, por ejemplo los bancos privados con el Banco Central nos vemos en la necesidad de añadir un nuevo identificador para permitir este esquema de conexión.

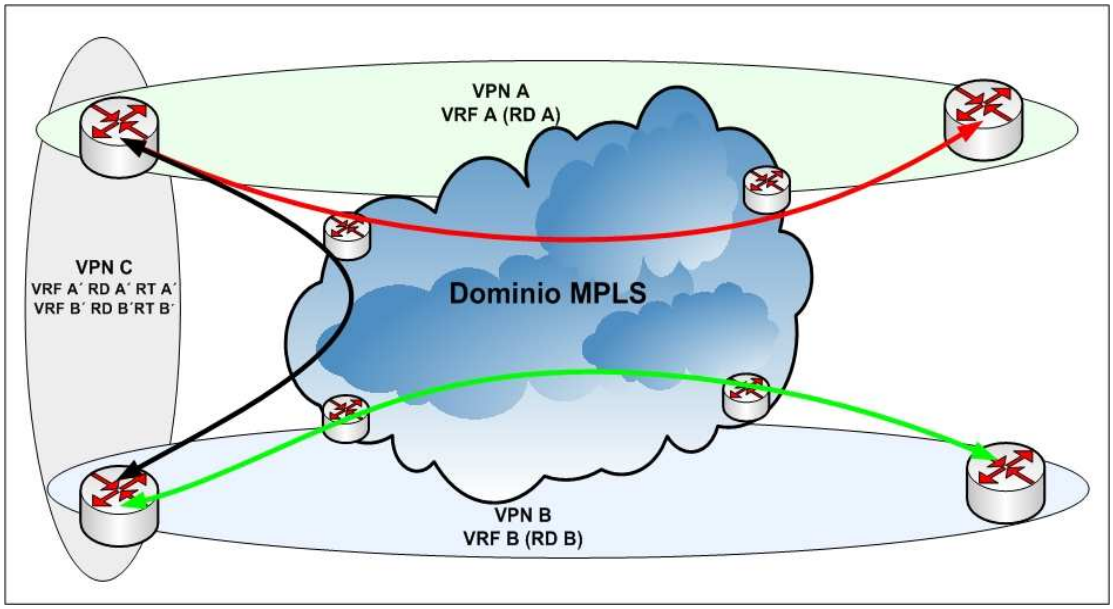


Fig. 2-26.- Extranets MPLS

Entonces surge la figura de un nuevo marcado, conocido como Route Target (Ruta objetivo); este es básicamente un atributo del protocolo BGP que se añade a la dirección IPv4 del cliente una vez convertida en VPN IPv4. Las RT sirven para indicar a cual o cuales VPNs pertenece la ruta a la cual esta añadida y tienen un valor de 64 bits.

Las RTs que son añadidas a las rutas del cliente, se denominan RTs exportables y son configuradas de forma separada por cada VRF existente en el router PE. Este grupo de RTs (exportables) identifican la(s) VPN(s) a las cuales están asociados los sitios contenidos en la tabla virtual de enrutamiento. Cuando las direcciones VPN IPv4 son propagadas mediante el MP-IBGP hacia los demás PEs, estos deberán discriminar que rutas deberán aceptar en sus diferentes VRFs para luego ser enviadas a sus sitios destino y esto es posible mediante las RTs contenidas en esas direcciones.

En esquemas sencillos, las RDs identifican a las VPNs, pero en esquemas donde existen varias VPNs y muchas de ellas con sitios en común, las RTs indican una MEMBRESIA de VPN.

2.5.3.3 VRF – Virtual Routing Forwarding

Las VRFs son instancias de enrutamiento y reenvío que pueden ser utilizadas por una o varias VPNs conectadas al mismo equipo PE y con similares requerimientos de conexión.

Las tablas VRFs son una parte fundamental en la implementación de las VPNs en redes MPLS, y su estructura básica sería la siguiente:

- Tabla de enrutamiento
- Tabla CEF
- Lista de las interfaces asociadas con la VRF
- RDs – Route Distinguisher
- RTs – Route Target: Import – Export

La importancia de las VRFs radica en que permite ejecutar protocolos entre el CE y el PE de forma independiente al ejecutado en el core MPLS debido a que con VRF genera una tabla virtual para cada instancia de enrutamiento con un cliente, es decir, en un PE puedo tener **n** instancias virtuales de enrutamiento con **n** clientes sin que estas tablas afecten la tabla global de la red MPLS.

Las rutas recibidas por las instancias de enrutamiento asociadas a la VRF son colocadas en la tabla de enrutamiento contenida en la VRF. Esta tabla de enrutamiento soporta las mismas características que la tabla de enrutamiento global que se esta ejecutando en el PE como

mecanismos de filtrado y de selección de rutas provenientes de varios protocolos, conocido como distancias administrativas.

Cada VRF elabora la tabla FIB en base a la información contenida en su tabla de enrutamiento, esta tabla es utilizada para reenviar los paquetes a través de las interfaces asociadas a la VRF, interfaces que pueden ser lógicas, físicas o incluso sub-interfaces que soporten CEF.

2.6 Internal Gateway Protocol – IGP

2.6.1 Protocolo de Estado de Enlace.

En el mundo del networking existen dos grandes clasificaciones para los protocolos de enrutamiento interno -IGP- los de vector distancia (IGRP, RIP, etc) y los de estado enlace (OSPF, IS-IS). Ambos tipos de protocolos buscan rutas a través de sistemas autónomos, pero utilizan distintos algoritmos para realizar esta tarea.

Los algoritmos de estado del enlace, o también conocidos como Primero la ruta más corta (SPF: Shortest Path First), mantienen una compleja base de datos de la información topológica de la red como por ejemplo routers lejanos y su interconexión; mientras que los algoritmos de vector distancia no pueden proveer información tan detallada sobre redes lejanas a su nodo. En este apartado nos concentraremos en los protocolos de estado enlace y en especial al escogido para el desarrollo de este trabajo: OSPF.

En redes con protocolos SPF, una vez que se obtiene la información acerca de los nodos vecinos, cada router calcula las mejores rutas hacia todos los destinos de la red, y es debido a que cada

router posee una visión completa de toda la red es menos propenso a que se propague información incorrecta o desactualizada.

Entre las principales características de los protocolos basados en el algoritmo SPF podemos mencionar: responden rápidamente ante cambios topológicos de la red, envían actualizaciones desencadenadas solo ante cambios en la red, envían actualizaciones periódicas conocidas como actualizaciones del estado de enlace y usan el mecanismo “HELLO” para evaluar la posibilidad de comunicarse con los vecinos.

Entre los principios básicos que se ejecutan cuando se esta utilizando protocolos de estado enlace se encuentran:

- ✓ Cada router establece a una relación “adyacencia” con todos sus vecinos.
- ✓ Cada router genera advertencias acerca del estado de sus enlaces (LSA: Link State Advertisements) que son distribuidas a todos los routers de la red.
- ✓ Cada router mantiene una base de datos con todos los LSAs recibidos, mismos que le permiten elaborar una base de datos topológica de la red y otra base de datos del estado de los enlaces.
- ✓ Con esta base de datos, cada router ejecuta el algoritmo de Dijkstra para determinar la ruta más corta para cada destino de la red. La información de las rutas más cortas serán almacenadas en la tabla de enrutamiento.

* Cada LSA contiene: Identificador del enlace, estado del enlace, costo, vecinos del enlace.

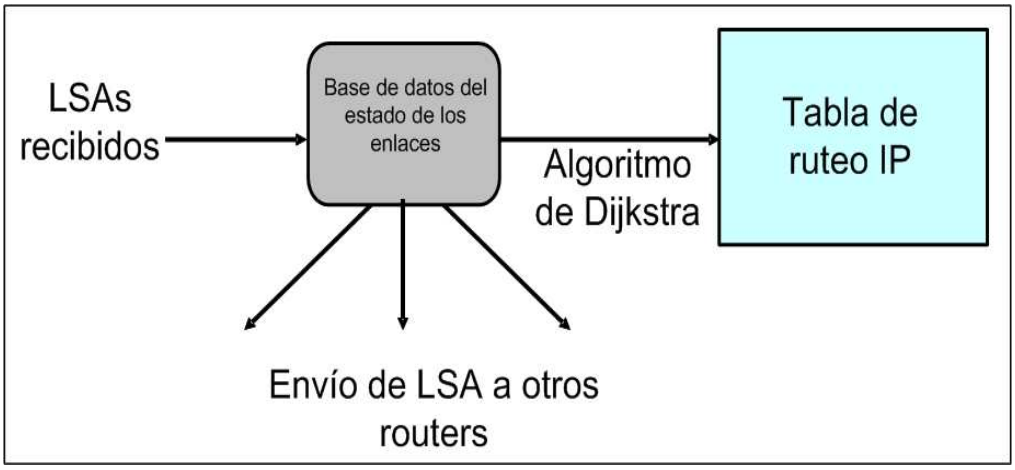


Fig. 2-27.- Operación de los LSAs

Debido a la completa visión que llega a tener cada unos de los nodos que conforman la red, estos equipos sufren de una demanda mayor de consumo de procesamiento y memoria, siendo esta una de las principales desventajas de este tipo de protocolos.

2.6.2 Introducción OSPF (Open Shortest Path First)

El protocolo de primero la ruta más corta de estándar abierto (por ello la palabra OPEN) es en la actualidad el más utilizado de los protocolos de estado enlace debido a su robustez y escalabilidad.

Aquí un poco de historia de las distintas versiones de OSPF:

- 1989: RFC 1131 OSPF Version 1
- 1991: RFC1247 OSPF Version 2
- 1994: RFC 1583 OSPF Version 2 (revised)
- 1997: RFC 2178 OSPF Version 2 (revised)
- 1998: RFC 2328 OSPF Version 2 (current version)

- En la actualidad, la norma RFC 5340 es la que aplica para el conocido OSPF versión 3 con soporte para IPv6.

2.6.3 Características Principales

Cuando nos encontramos con redes pequeñas las posibles rutas que se deben calcular utilizando el algoritmo de Dijkstra son pocas y por ende lo serán las tablas LSDB (Link State Data Base) que almacena los estados de los enlaces de cada routers y ARDB (Adjacency Routers Data Base) que almacena la información de los vecinos con quienes se han iniciado sesiones OSPF consumiendo de esta forma pocos recursos de procesamiento y memoria, siendo nuestro trabajo relativamente sencillo y de fácil administración; sin embargo, cuando las redes empiezan a crecer y por ende sus sucursales y nodos comienzan a incrementarse el cálculo de todas las posibles rutas (es necesario para determinar la más corta) mediante Dijkstra se torna complicado y dado que las tablas antes mencionadas crecen en tamaño el consumo de procesamiento puede provocar el colapso de un equipo que no este preparado para este desempeño. Para esto, se el protocolo OSPF ha contemplado la segmentación jerárquica de sus nodos, concibiendo 2 categorías que paso a explicar (Fig 2-X):

Áreas de Tránsito o Backbone: Conocidas también como áreas 0, siendo su principal función interconectar otros tipos de áreas creadas en una nube OSPF. Por cada red, solo existirá un área 0 y esta no estará interconectada con usuarios finales sino solamente con otras áreas.

Áreas Regular: Este tipo de áreas sirven para conectar a los usuarios o recursos de la red. Este tipo de áreas usualmente sirven para agrupar tipos de usuarios según perfil o situación geográfica.

Este tipo de áreas no permiten el tráfico de áreas externas tratando de alcanzar destinos de otras áreas.

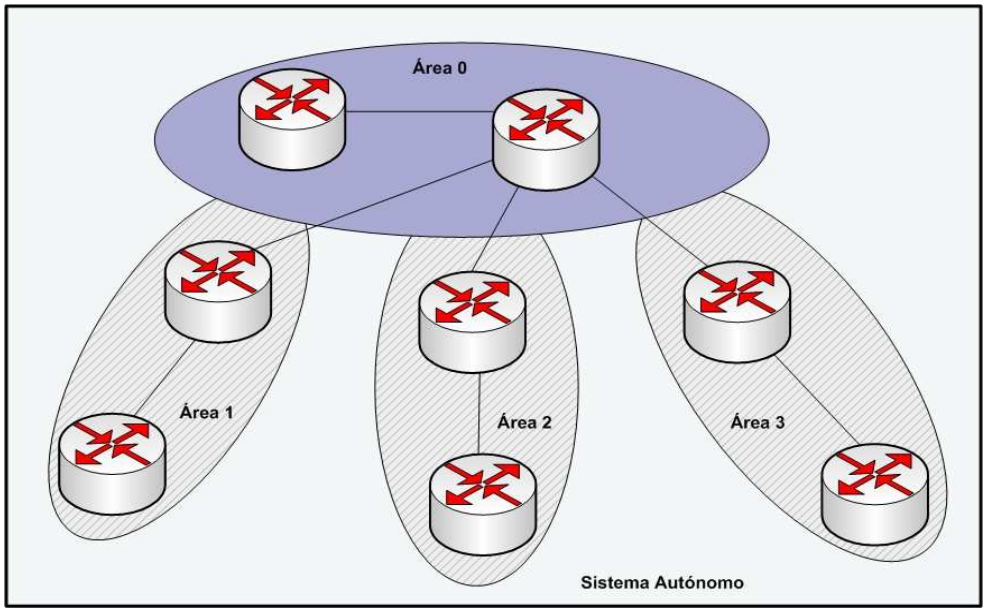


Fig. 2-28.- Áreas OSPF

Todo el tráfico entre las áreas 1, 2, 3 deberá pasar por el área 0, es por ello que el diseño siempre se tenga cuidado con el dimensionamiento del área 0, pues esta debe estar conectada directamente a las otras áreas. Se recomienda que cada área tenga hasta 50 routers como máximo.

Los routers que pertenecen al área de backbone se denominan routers CORE (principales) y a los que son frontera con el área cero, se los llama routers de borde. Estos equipos en particular, cumplen un papel muy importante en el desempeño de la red por las siguientes razones:

- ✓ Separar las zonas de inundación LSA.
- ✓ Son el primer punto para la sumarización.
- ✓ Sirven como default route (ruta por defecto).

- ✓ Mantienen la base de datos de los LSA para cada área a la que pertenecen.

Nota: Las mejores prácticas para el diseño en OSPF indican que lo recomendable es que cada router borde este conectado únicamente a 2 áreas.

2.6.4 Funcionamiento OSPF

2.6.4.1 Adyacencias OSPF

Los tipos de red sobre los cuales se puede ejecutar OSPF son 3 que paso a mencionar:

1. Redes Punto a Punto. Ej. PPP o HDLC
2. Redes de difusión o Broadcast. Ej. Ethernet
3. Redes de multiacceso sin difusión o non-broadcast multiaccess (NBMA). Ej Frame relay o ATM.

Un router en el cual se esta ejecutando OSPF debe primero establecer adyacencia con todos los routers vecinos. Esto es posible mediante el intercambio de paquetes hello, a continuación se presentan los pasos a seguir:

- El router envía y recibe paquetes hello hacia y desde sus vecinos. El formato típico de estos paquetes es en multicast, es decir, enviado a todos los pertenecientes a la red.
- El router verifica los parámetros del paquete hello (varían según el protocolo) y pueden ser por ejemplo: Si el vecino pertenece al mismo AS (sistema autónomo) y área.
- Después de que 2 routers establecen adyacencia, sincronizan sus bases de datos (LSDB) mediante el intercambio de LSAs. Una vez realizado esto, en OSPF se considera que están en completa adyacencia.

- De ser necesario (cambios de topología por ejemplo) los ruteadores intercambiaran nuevos LSAs para asegurar una completa sincronización de las tablas dentro del área.

Dos routers conectados mediante un enlace WAN punto a punto utilizando protocolos HDLC o PPP establecen completa adyacencia el uno con el otro.

Por el contrario, en una disposición LAN (Fig 2-29) se selecciona a un "representante" que se lo conoce como DR (designated router) y a otro como su respaldo BDR (backup designated router). Todos los ruteadores forman una completa adyacencia contra estos dos equipos e intercambian LSAs solo y exclusivamente contra ellos. Esto permite que no se inunde la red con tráfico repetido entre los routers pues uno solo es el encargado de recibir los LSA y transmitirlos a todos los miembros de la red, incluyendo a los nuevos vecinos que se agreguen en un futuro.

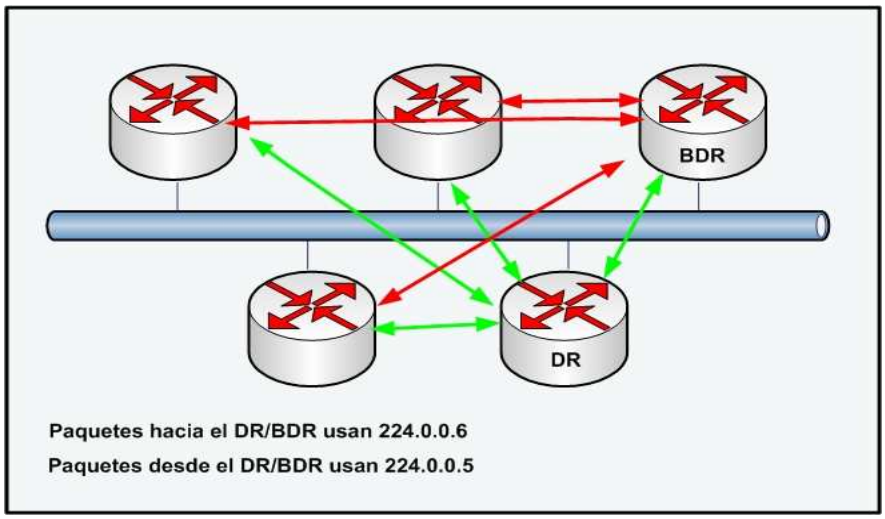


Fig. 2-29.- Router Designado en un ambiente broadcast.

En redes NBMA la designación de dispositivos DR y BDR se convierten en un problema debido a la naturaleza de estas redes de no permitir tráfico multicast, sin embargo la signación manual, aunque tediosa, permite solventar este problema.

La forma en que OSPF asigna a los ruteadores como designado y alterno se basa en un parámetro llamado prioridad durante el intercambio de paquetes hello. Generalmente, se designa al que tenga mayor prioridad y en caso de existir algún empate, ganará el que tenga la IP más alta configurada en la interfaz o de loopback. (Fig 2-x)

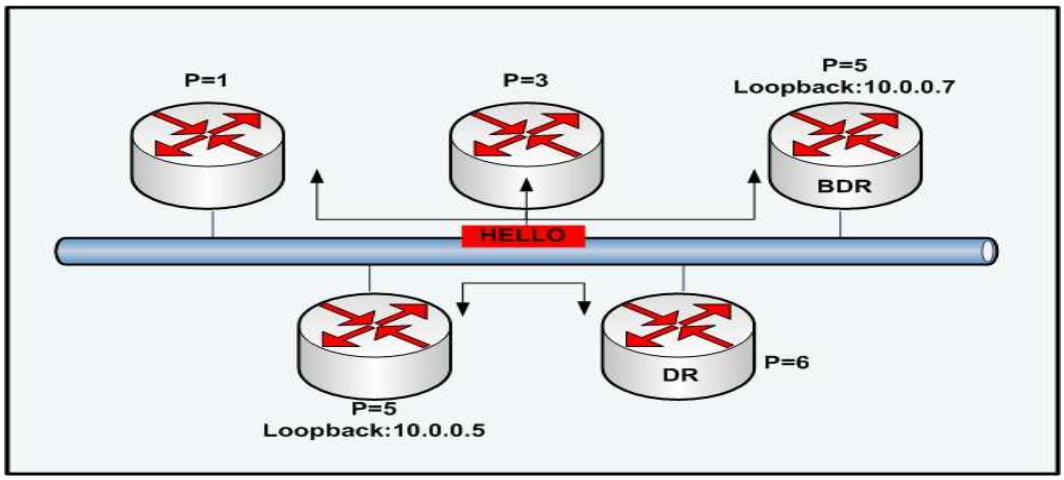


Fig. 2-30.- Criterios de Selección de un DR y BDR.

2.6.4.2 Tipos de paquetes OSPF

Entre los principales tipos de paquetes que encontramos dentro del protocolo OSPF podemos anotar:

Tipo	**Nombre**	**Descripción**
1	Hello	Descubre vecinos y establece adyacencias.
2	DBD	Verifica la sincronización de las base de datos.
3	LSR	Pedido de un router a router por el registro del estado de un enlace
4	LSU	Envío del estado de un enlace ante un pedido de un router vecino.
5	LSAck	Permite reconocer otro tipo de paquetes

Tabla 2-1.- Tipos de Paquetes OSPF

Todos los 5 tipos de paquetes OSPF son encapsulados directamente dentro de un paquete IP. Los paquetes OSPF no utilizan TCP o UDP debido a que OSPF requiere un modo confiable de transporte de paquetes, por lo cual se ha definido su propia rutina IP para el envío de sus paquetes.

En la cabecera IP, el identificador de protocolo para los paquetes OSPF es el 89 y cada paquete viene definido con el mismo formato de cabecera OSPF, tal como se detalla a continuación:

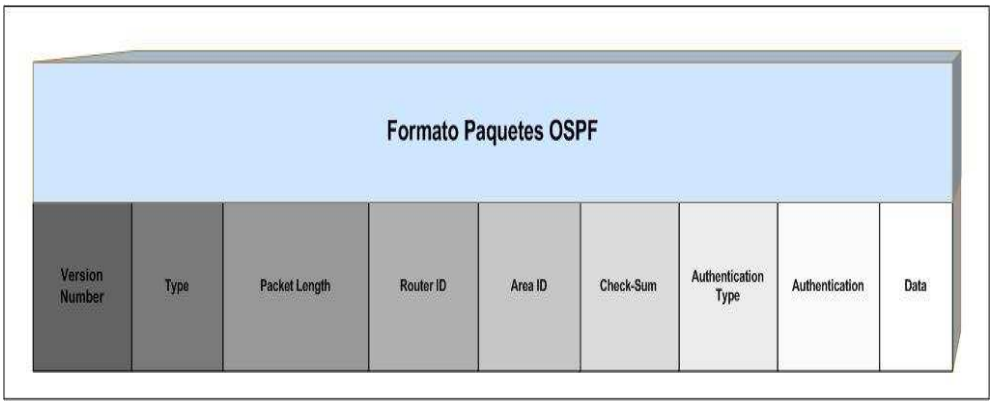


Fig. 2-31.- Formato Cabecera OSPF

Version number: Esto indica la versión de OSPF que se esta ejecutando. Versión 2 es la actual.

Type: Indica los diferentes 5 tipos de paquetes OSPF.

Packet Length: Indica la longitud de los paquetes dado en bytes.

Router ID: Indica el router fuente del paquete.

Area ID: Indica el área de procedencia del paquete.

Checksum: Es utilizado para asegurar que no existió error durante la transmisión del paquete OSPF.

Authentication Type: Sirve para detectar el tipo de autenticación que se esta utilizando en OSPF.

Authentication: Se habilita cuando se esta utilizando alguna autenticación como MD5.

Data – Paquetes Hello: Incluye la lista de los vecinos conocidos.

Data – paquetes DBD: Contiene un resumen de la base de datos de los estados de enlace. (LSDB) adicional incluye la información de los routers conocidos y su último número de secuencia.

Data – paquetes LSR: Contiene el tipo de paquete LSU necesitado y el identificador del router que necesita el LSU.

Data – paquetes LSU: Contiene el listado completo de los LSA.

Data – paquetes LSAsk: Esta vacío.

Como hemos visto a lo largo de este capítulo, la adyacencia entre todos los routers OSPF es necesaria para el correcto funcionamiento de este protocolo, y esta adyacencia o vecindad es lograda mediante el intercambio en 2 vías de los ya mentados paquetes HELLO; esta comunicación en 2 vías se refiere a que cada router debe verificar que este en la lista del paquete hello del router con quien quiere establecer la adyacencia.

La información contenida en cada paquete hello es la siguiente:

Router ID: El “router ID” o identificador de router es un número de 32 bits que identifica únicamente a un router. Generalmente, este identificador es seleccionado de la IP más alta configurada en todas las interfaces OSPF activas, a menos que la IP loopback este configurada, en ese caso esa será el identificador. Este es un valor muy importante pues como vimos antes, en caso de empate en prioridades para la designación del DR (designed router) el identificador más alto romperá dicho empate.

Intervalos Hello y Dead: El intervalo hello especifica la frecuencia en segundos en las que el router enviará paquetes hello a sus vecinos, 10 segundos es el tiempo por defecto. El intervalo "dead" o límite es el tiempo máximo que esperará cada router antes de declarar un vecino fuera de servicio. El intervalo dead es de 4 veces el valor de un intervalo hello por defecto y debe ser el mismo en todos los routers para que la adyacencia pueda ser establecida.

Neighbors - Vecinos: Este campo enlista todos los routers vecinos con los que se ha establecido una comunicación en 2 vías.

Area ID: Este identificador de área, sirve para indicar a los routers vecinos el área y segmento a la que pertenece el router fuente.

Prioridad: Es un número de 8 bits e indica la prioridad del router fuente. Sirve para la selección del DB y DBR.

Direcciones IP DR y BDR: Si fueron ya seleccionados, estos campos indican las direcciones IP de los DR y BDR para ese segmento.

Password: Si esta habilitada la opción de autenticación, ambos routers deberán tener configurada la misma clave para poder proceder a la adyacencia.

2.7 External Gateway Protocol – EGP

2.7.1 Introducción Border Gateway Protocol – BGP

Un AS (Sistema Autónomo) es una colección de redes bajo una sola administración técnica. Un IGP está corriendo dentro de un AS, resultando en un óptimo ruteo intra-AS. Un EGP está corriendo entre sistemas autónomos para habilitar políticas de routing y proveer seguridad.

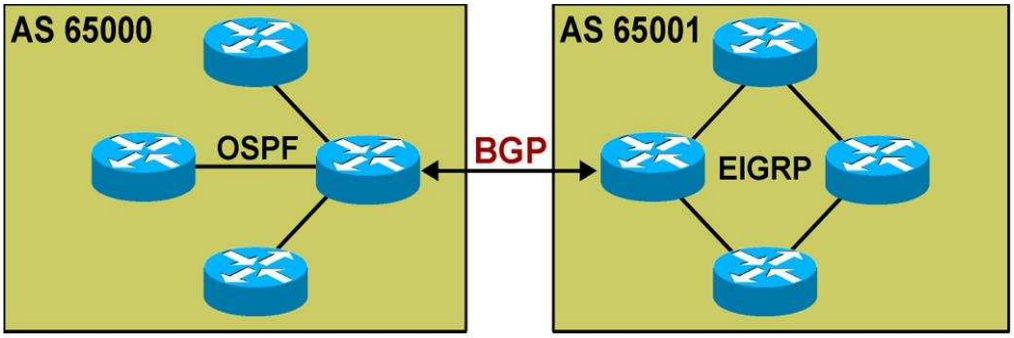


Fig. 2.32.- EGP –IGP en una red

Entre los objetivos del diseño de una red cuando se utiliza un protocolo EGP se pueden mencionar:

- **Escalabilidad:** La Internet tiene más de 200,000 rutas y sigue en crecimiento.
- **Intercambio de información de ruteo en forma segura:** Routers desde otro AS no pueden ser alterados
- **Soporte para políticas de ruteo:** Routing entre sistemas autónomos no siempre debe seguir el camino más óptimo.

¿Qué es BGP?

Es un protocolo de enrutamiento externo (EGP) que sirve principalmente para el intercambio de rutas entre sistemas autónomos (como ISPs). BGP también es fundamental para el funcionamiento de otras aplicaciones como MPLS VPN.

Características principales de BGP

- Protocolo considerado como de tipo vector distancia con mejoras: los updates son fiables (reliable), sólo enviados ante cambios en la topología (triggered) y tienen atributos especiales (AS number, etc).
- Los vecinos BGP utilizan TCP (179) para establecer una sesión y enviarse actualizaciones.
- Su distancia administrativa es de 20 (EBGP - External BGP) o 200 (IBGP - Internal BGP).
- Es 'classless': La máscara de subred viaja en los updates (soporta VLSM).
- Es capaz de filtrar y escoger rutas como ningún IGP, en base a sus atributos especiales: AS Number, local-preference, origin, community, etc.
- Los vecinos deben ser configurados manualmente en ambos extremos, pudiendo estos autenticarse.
- Por defecto sus tiempos de convergencia son lentos, pero lo que se pierde en convergencia se gana en estabilidad y escalabilidad, que es la prioridad ante la gran cantidad de rutas y posibles cambios de topología en los dominios de red tan amplios donde BGP generalmente es utilizado.

2.7.2 BGP: Arquitectura y funcionamiento

2.7.2.1 Establecimiento de sesión e intercambio de rutas.

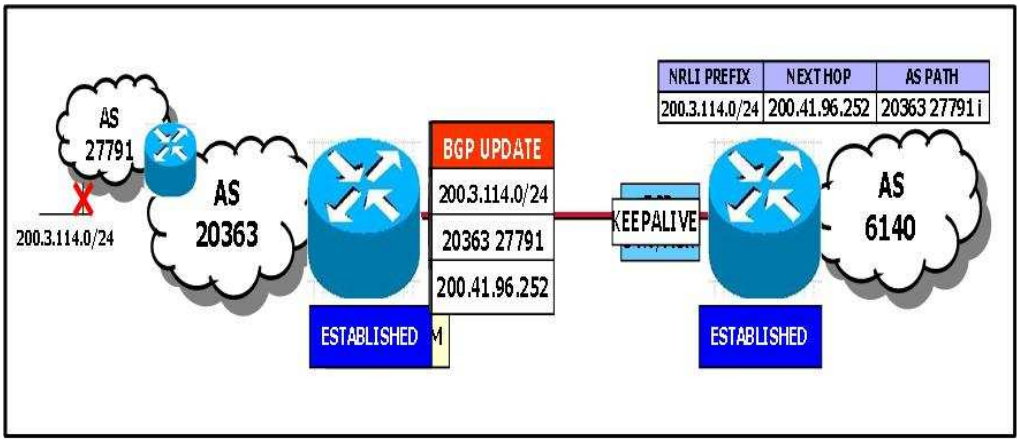


Fig. 2-33.- Estableciendo una sesión BGP

Para que se produzca el establecimiento de una sesión BGP y el posterior intercambio de rutas, se deben cumplir los siguientes pasos:

IDLE: El router aún no evalúa la conectividad con el vecino.

ACTIVE: La IP configurada es alcanzable en la tabla de rutas, el primero que haya establecido esto inicia el '3-way handshake' de TCP usando la dirección IP del vecino en el puerto 179.

OPEN SENT: uno de los router envía un mensaje OPEN (el primero que lo haga), el cual incluye la versión de BGP, el número de AS, el 'hold-time' , el BGP router ID y parámetros opcionales (p.e. autenticación).

OPEN CONFIRM: Si el vecino acepta los parámetros del mensaje OPEN, responde con su propio mensaje OPEN, poniendo al router que lo recibe en este estado.

ESTABLISHED: Si el router local acepta los parámetros del mensaje OPEN del vecino, entonces la sesión BGP se establece con un mensaje keepalive, en adelante estos mensajes se intercambiarán cada 60 segundos (por defecto).

UPDATES: Una vez iniciada la sesión, los routers se intercambian toda su tabla BGP mediante mensajes UPDATE, hasta que toda la tabla haya sido enviada. Los mensajes UPDATE están formados por prefijos alcanzables llamados Network Layer Reachability Information (NRLI) y atributos (al menos Next hop, AS-Path y Origin). También pueden incluir prefijos que ya no son alcanzables (withdrawn routes).

NOTIFICATIONS: son mensajes enviados a un vecino para informar de un error en la sesión.

2.7.2.2 Tipos de atributos en rutas BGP

Los diferentes atributos existentes en rutas BGP se podrían clasificar de la siguiente forma:

- **Well-known mandatory:** Son atributos que son reconocidos en todas las implementaciones de BGP, además deben estar incluidos en todos los updates, de otra forma se generará un mensaje de error (notification). Estos son: Origin, Next-hop y AS-Path.

- **Well-known discretionary**: Son atributos que son reconocidos por todas las implementaciones pero no necesariamente tienen que ser enviados en los updates. Estos son: Local preference, Atomic-aggregate y Aggregator.

- **Optional transitive:** Son atributos que no necesariamente deben ser reconocidos por todas las implementaciones, pero son propagados entre vecinos así estos no los reconozcan. Ejemplo: Community.

- **Optional non-transitive:** Son atributos que no necesariamente deben ser reconocidos por todas las implementaciones y tampoco se deben enviar a otros vecinos así estos sean reconocidos. Ejemplos: Multi-exit Discriminator (MED), Cluster-list, Originator ID.

2.7.2.3 Descripción de atributos en rutas BGP

Origin: Especifica cuál es el origen del NRLI.

VALOR	DESCRIPCIÓN
IGP	Ruta originada en un IGP dentro del AS
EGP	Ruta originada por Exterior Gateway Protocol (Descontinuado)
Incomplete	Otro medio, por ejemplo redistribución

Tabla 2-2.- Atributo ORIGIN

Next-hop: generalmente es la dirección IP del vecino EBGP que envió el update (EBGP) o la del que lo originó (IBGP).

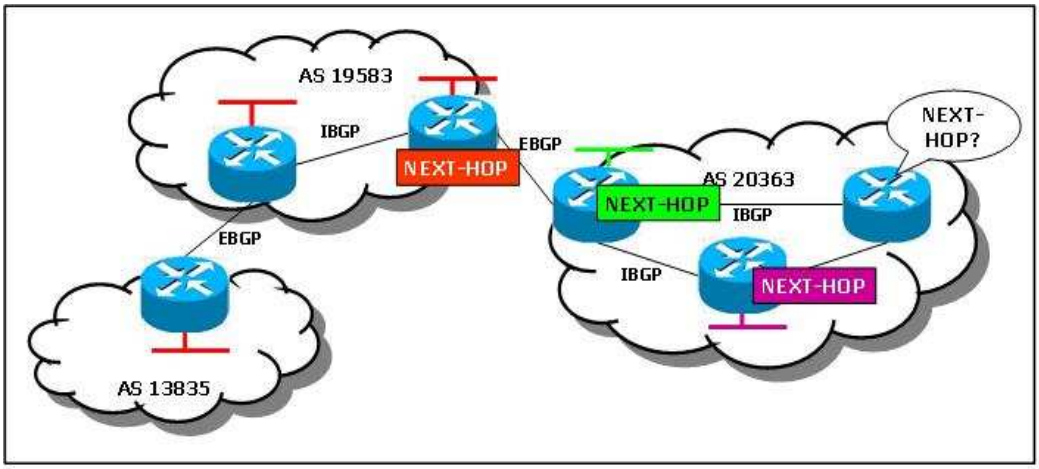


Fig. 2-34.- Atributo Next Hop

AS-Path: Es una secuencia de números de AS que se forma conforme una ruta se va propagando. Mientras más corto sea el AS-Path, la ruta se considerará más cercana. También sirve para evitar 'loops', si un router ve su propio AS en un update, inmediatamente lo desecha.

Los ASN (AS Number) son asignados por ARIN, van desde el 1 hasta el 65535. A partir del 64512 los ASN son de uso privado.

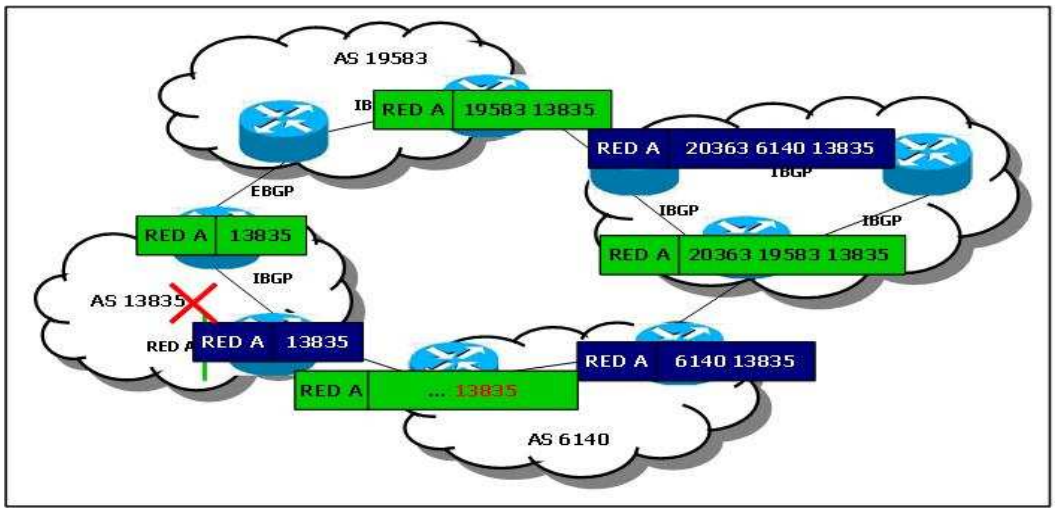


Fig. 2-35.- Atributo AS-Path

Local-Preference: Es utilizado y propagado entre vecinos del mismo AS (IBGP). Sirve para influenciar el tráfico que sale del AS, distinguiendo entre rutas iguales: La ruta con mayor valor tendrá preferencia.

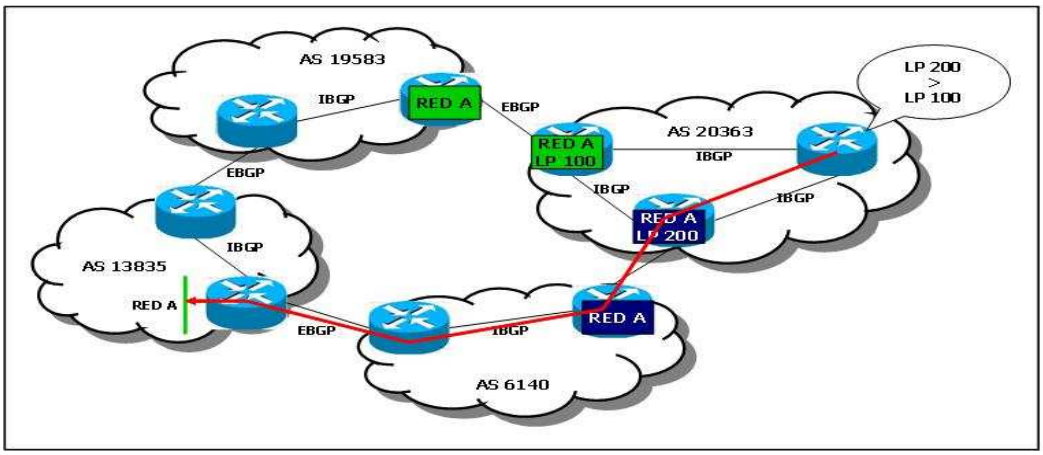


Fig. 2-36.- Atributo Local Preference

Atomic-aggregate: cuando un router hace una sumarización de prefijos aprendidos por BGP, probablemente se pierda información del AS-Path. Cada vez que esto ocurre, este atributo debe ser adjuntado a los updates de dicha ruta sumarizada.

Aggregator: opcionalmente también se puede adjuntar la dirección IP y el número de AS del router que realizó la sumarización.

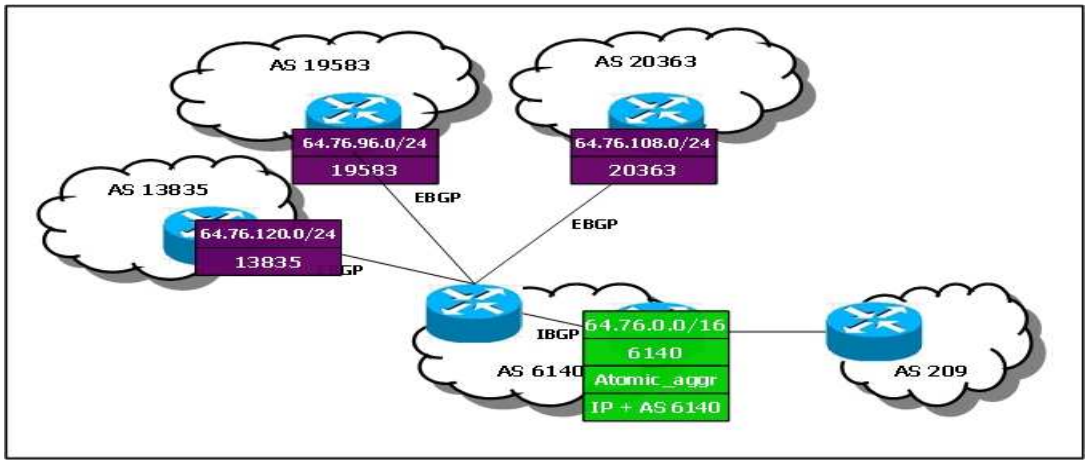


FIG. 2-37.- Aggregator

Community: Sirve para agrupar prefijos que comparten alguna característica en común, para luego clasificarlos según la comunidad a la que pertenecen y cambiar sus atributos según sea necesario. El atributo es original de Cisco pero luego fue estandarizado en la RFC 1997, con el formato de 4 octetos AA:NN, donde AA en el número de AS y NN es un identificador definido administrativamente. Existen 4 comunidades predefinidas:

VALOR	DESCRIPCIÓN
INTERNET	Comunidad por defecto, las rutas recibidas en esta comunidad son publicadas con normalidad
NO_EXPORT	Las rutas recibidas en esta comunidad no se propagarán a vecinos EBGP que no pertenezcan a la confederación.
NO_ADVERTISE	Las rutas recibidas en esta comunidad no se propagarán a ningún tipo de vecino.
LOCAL_AS	Las rutas recibidas en esta comunidad no se propagarán a vecinos EBGP así estos pertenezcan a una confederación.

Tabla 2-3.- Valores del atributo Community

MED: Sirve para influenciar el tráfico que ingresa al AS, siendo el menor valor el preferido. Este valor pasa de un AS a otro directamente conectado, pero no es propagado a un tercer AS.

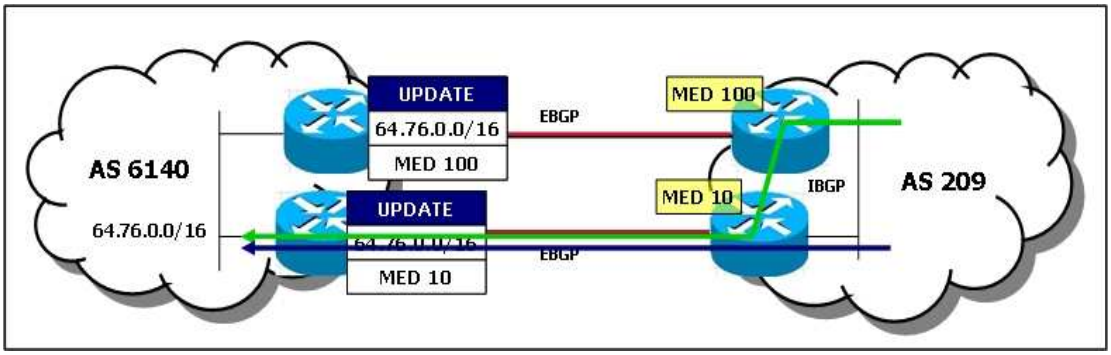


Fig. 2-38.- Atributo MED

La influencia de MED no siempre funcionará, ya que el AS vecino puede tener otros atributos de salida preferidos sobre el MED, como por ejemplo, Local Preference. Otro dato importante acerca de este atributo es que el MED sólo es comparado en rutas que vienen del mismo AS, no de ASs distintos.

Los siguientes atributos son utilizados en Route-Reflectors, tema que se verá más adelante.

Cluster-list: Es una lista de Cluster IDs por los cuales la ruta ha pasado. Si un Route-Reflector ve su cluster-ID en un update, lo descarta, al tratarse de un loop.

Originator ID: Es un valor de 32-bits creado por un Route-Reflector, igual al Router ID del originador de la ruta. Si el originador ve su propio ID como Originator ID en un update, lo descarta, al tratarse de un loop.

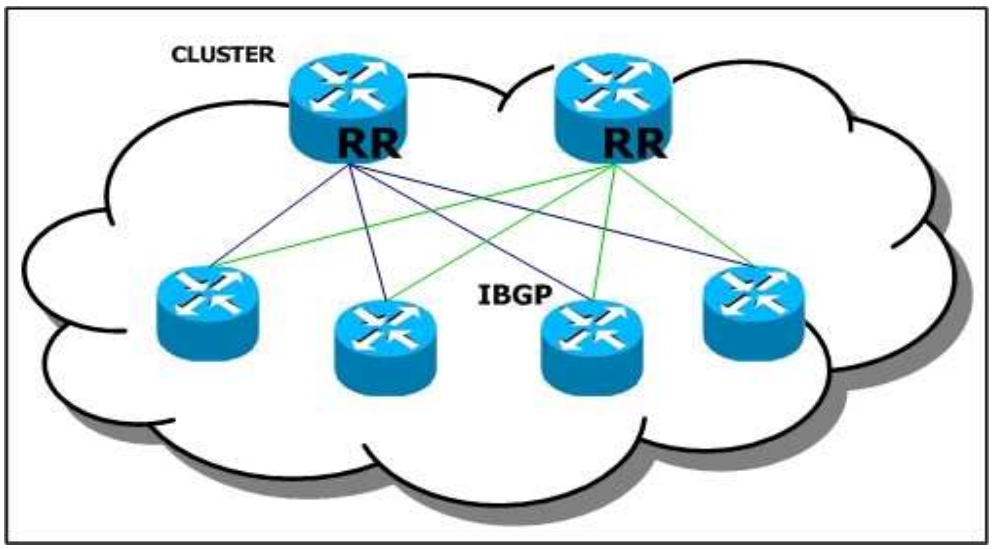


Fig. 2-39.- Configuración con Route-Reflector

2.7.2.4 Criterios de Selección de rutas e Influencias de Tráfico.

Cuando se reciba más de una ruta al mismo destino, se escogerá una según el siguiente criterio:

1. Se preferirán las rutas con mayor **Weight**, este parámetro es sólo usado por Cisco y es de significado local al router, no es propagado a ningún vecino.
2. Rutas con mayor valor de **Local Preference**.
3. Rutas que el propio router originó, es decir, de **origen local**.

4. Rutas con **AS-Path** más corto.
5. Rutas cuyo atributo **Origin** sea del menor tipo (IGP < EGP <Incomplete).
6. Rutas con menor valor de **MED**.
7. **EBGP** sobre IBGP.
8. Rutas anunciadas por el **vecino más cercano** (sólo en IBGP).
9. Ruta de mayor **antigüedad** (sólo en EBGP).
10. Rutas anunciadas por el vecino con el menor **Router ID**.

Para que una ruta sea válida y tomada en cuenta en la selección, su atributo NEXT-HOP debe ser alcanzable por algún IGP o ruta estática.

Existen dos formas de influenciar el camino que el tráfico toma para ingresar al AS:

1. Utilizando MED: se publican valores de MED distintos por cada camino, de acuerdo a lo explicado anteriormente.

2. Utilizando AS-Path Prepend: se añade el último número de AS varias veces en las rutas propagadas por el enlace menos preferido.

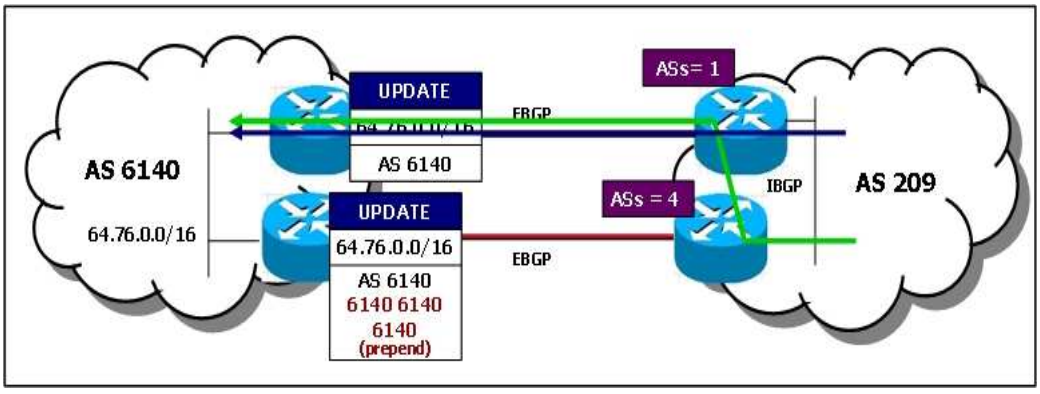


Fig. 2-40.- Influencia del tráfico entrante

Existen dos formas de influenciar el camino que el tráfico toma para salir del AS:

1. Utilizando Weight (sólo Cisco): se marca la ruta preferida con un mayor valor de Weight, sólo se influenciará la decisión del router donde se aplica.

2. Utilizando Local Preference: se marca la ruta preferida con un mayor valor de LP, se influenciarán las decisiones de todos los routers en el AS.

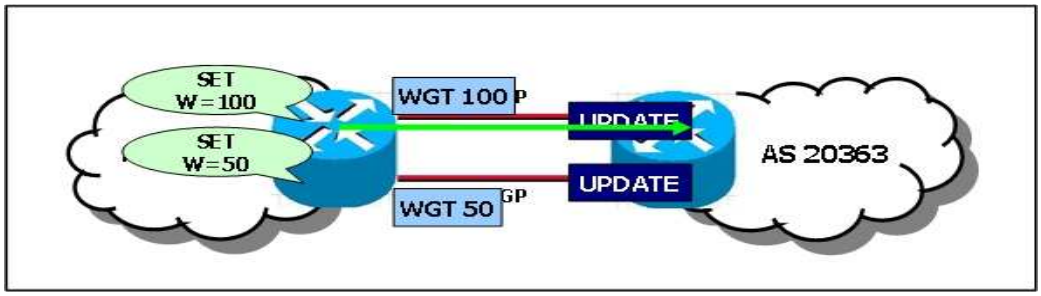


Fig. 2-41.- Influencia de tráfico saliente mediante WEIGHT

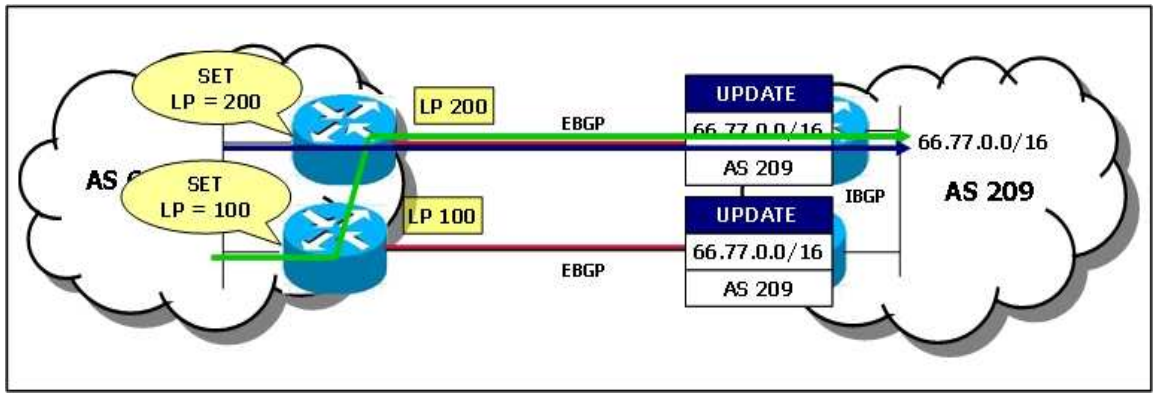


Fig. 2-42.- Influencia de tráfico saliente mediante LOCAL PREFERENCE

2.7.2.5 Filtros BGP

Normalmente en cualquier implementación de BGP se puede permitir o denegar rutas recibidas o enviadas en base a diversos parámetros. Los filtros más comunes son:

- Filtros por red IP: se filtran las rutas por la red o subred a la cual pertenecen.
- Filtros por prefijo IP y máscara: se filtran las rutas por la red a la que pertenecen y además por la máscara de red.
- Filtros por AS-Path: se filtran las rutas según su atributo AS-Path utilizando ***expresiones regulares***.
- Filtros por comunidad: se filtran las rutas por la comunidad a la que pertenecen.
- Filtros por Next-hop: se filtran las rutas según qué router las publicó.

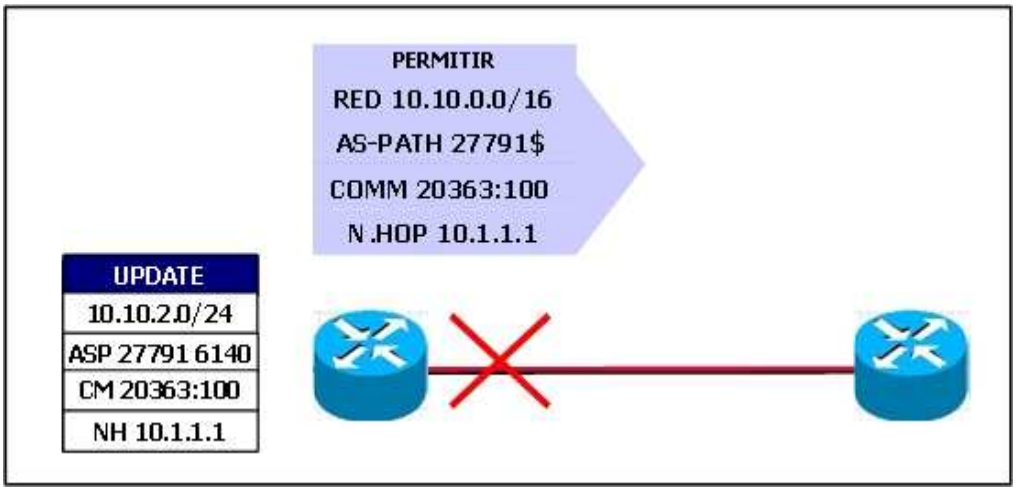


Fig. 2-43.- Filtros BGP

Después de aplicar filtros o aplicar alguna configuración que remarca atributos, es necesario volver a recibir o enviar la tabla BGP según sea el caso, debido a que esta no se reenvía sola, sólo se actualiza ante cambios de topología. Una alternativa es reiniciar la sesión BGP, pero normalmente esto no es posible en redes en producción, por lo que existen las siguientes alternativas:

- ✓ Reenvío de la tabla (outbound soft-reconfiguration): el router vuelve a enviar la tabla a su vecino sin bajar la sesión.
- ✓ Reingreso local de la tabla vecina (inbound soft reconfiguration): el router mantiene una copia de la tabla de su vecino, para volverla a pasar por los filtros cuando sea necesario (consume más memoria)
- ✓ Route Refresh: el router solicita a su vecino un reenvío de su tabla BGP.

2.7.3 Internal BGP - IBGP

IBGP es principalmente utilizado para propagar rutas en un sistema autónomo de tránsito. Se requiere BGP porque ningún IGP puede manejar la cantidad de rutas que puede llegar a tener BGP, además, si se redistribuye BGP en un IGP se pueden perder atributos indispensables.

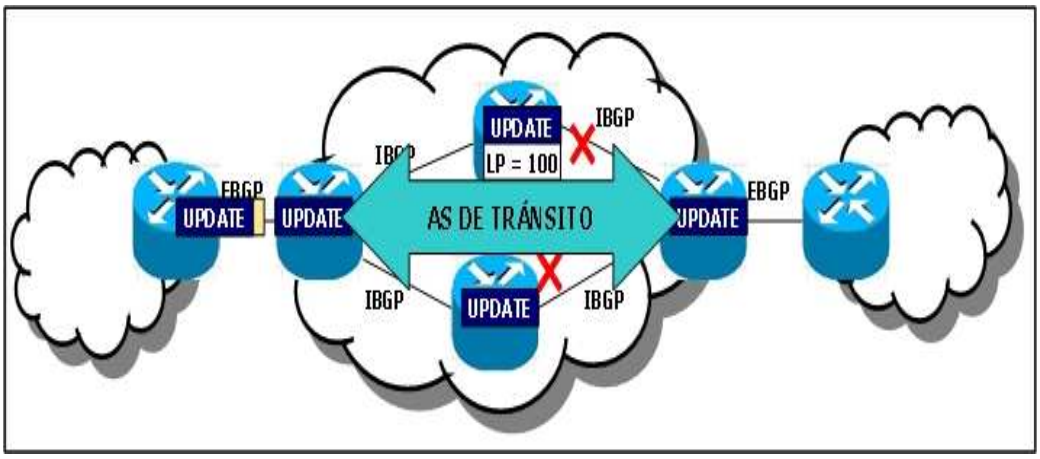


Fig. 2-44.- Internal Border Gateway Protocol

Vale la pena mencionar ciertas características que se presentan en la operación de este protocolo:

- Utiliza split-horizon para evitar loops, por lo cual ningún update recibido en IBGP es propagado a otros vecinos IBGP. Para mantener la misma información de rutas en todo el AS de manera que el tránsito funcione correctamente, se deben levantar sesiones IBGP entre todos los routers del domino → Full Mesh IBGP.
- Los atributos de las rutas no cambian conforme se propagan en updates IBGP, es decir, el valor de next-hop se mantiene.
- El atributo Local Preference es removido en los updates que egresan el AS (sesiones EBGP), pues sólo es utilizado dentro del AS.

2.7.3.1 Route-Reflectors (Reflectores de ruta) y Confederaciones

Como hemos visto en el apartado anterior, se requiere levantar redes FULL MESH IBGP para poder tener completa conectividad entre todos los nodos de la red; sin embargo, actualmente se cuenta con técnicas que permiten realizar esta función sin necesidad de levantar la red a full mesh así evitando los problemas que esta presentan.

Los Route-Reflectors cambian las reglas de split-horizon propias de IBGP, para evitar el full-mesh. La implementación está formada por routers que actúan como Route-Reflectors y sus clientes, formando un 'cluster'. Un AS puede estar formado por uno o varios 'clusters' , y cada uno de ellos por uno o varios RR redundantes.

Los clientes sólo necesitan tener sesiones con sus RRs. Si existen routers que no son ni clientes ni RRs en el AS, estos deben formar un full-mesh con todos los RRs.

ROUTER BGP CLÁSICO O CLIENTE	
UPDATE DE	SE ENVÍA A
Vecino EBGP	TODOS los vecinos
Vecino IBGP	Vecinos EBGP

ROUTER BGP ROUTE-REFLECTOR	
UPDATE DE	SE ENVÍA A
Vecino EBGP	TODOS los vecinos
NO-Cliente IBGP	Vecinos EBGP y Clientes
Cliente IBGP	TODOS menos el cliente

Tabla 2-4.- Router Clásico y Router con Route-Reflector

Las confederaciones evitan la configuración de full-mesh IBGP, subdividiendo un AS en dos o más AS que pueden ser privados o públicos.

Entre los AS internos a la confederación se matienen sesiones similares a EBGP (Intraconfederation EBGP), la diferencia es que en éstas sí se mantiene el valor de LP, MED y NEXT-HOP en los updates.

El AS de cada miembro es incluido en el AS-Path de sus updates, sin embargo, es excluido en el momento en que este update egresa la confederación. De esta forma desde afuera de la confederación sólo se conoce el AS global.

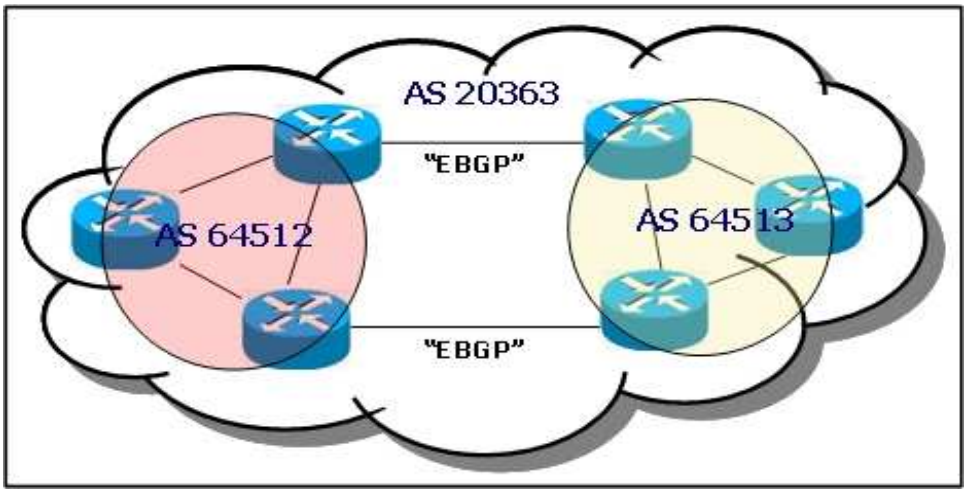


Fig. 2-45.- Confederaciones

Para concluir este apartado, es preciso indicar las siguientes anotaciones:

1. Las sesiones eBGP generalmente se forman entre routers directamente conectados, si estos no lo están, hay que especificarlo en la configuración (eBGP Multihop).

2. Las sesiones iBGP pueden formarse entre router que no están directamente conectados, pero que se conocen por un IGP o ruta estática, sin necesidad de configuración adicional.

3. Un router BGP no puede originar la publicación de una ruta si ésta no existe previamente en su tabla de rutas, aprendida por algún IGP o ruta estática.

4. En implementaciones anteriores una ruta BGP no podía ser propagada a través de un AS de tránsito sin que todos los routers dentro del AS conocieran previamente la ruta mediante algún IGP. En eso consistía la regla de sincronización, que dependía de la redistribución de BGP en el IGP utilizado. Esta regla ya no aplica pues ahora se utiliza IBGP en un AS de tránsito.

5. Si bien en IBGP el atributo next-hop de una ruta se mantiene con el mismo valor conforme ésta se propaga por el AS, en cualquier implementación se puede hacer que un router en el AS se declare a sí mismo como next-hop para todas las rutas anunciadas a algún vecino en particular.

6. Normalmente en una configuración BGP existen varios vecinos que comparten los mismos parámetros y filtros. En la mayoría de implementaciones se pueden colocar

estos vecinos en un grupo y aplicar los filtros y parámetros al grupo en lugar de a cada vecino individualmente, disminuyendo así los envíos y filtrados redundantes (Peer-Groups).

2.8 Ventajas y Diferencias frente a redes "tradicionales"

Llegado a este punto donde se ha compartido los conceptos más importantes de la tecnología MPLS, de los protocolos OSPF y BGP, ciertamente necesarios para la implementación de redes de alto rendimiento y escalabilidad; aunque de forma sucinta dada la amplitud teórica de los temas, procederemos en este apartado a enlistar brevemente las ventajas y diferencias más relevantes entre redes MPLS y redes IP tradicionales.

Diferencias

- Las redes IP tradicionales utilizan protocolos de enrutamiento para distribuir la información del protocolo enrutado seleccionado, en este caso IP.
- Las redes MPLS son independientes del protocolo enrutado seleccionado en la red, pudiendo ser IP, IPX, APPLETALK, etc.
- ❖ Las redes IP tradicionales realizan sus decisiones de reenvío de paquetes en base a la cabecera del paquete y su tabla de enrutamiento local.
- ❖ El mecanismo de reenvío de paquetes en redes MPLS es en base a "etiquetas".
- ✓ En redes IP tradicionales, cada router realiza consultas independientes a sus tablas de enrutamiento locales.
- ✓ En MPLS, los routers intermedios realizan consultas a las tablas con información de etiquetas y los siguientes saltos no en sus tablas de enrutamiento locales.

- Redes IP puras, no pueden ser utilizadas por proveedores de servicios de comunicaciones dado que podrían presentarse problemas de conflictos de redes privadas duplicadas. Quizás este problema se pueda solucionar de forma ineficiente mediante la asignación de IPs públicas a nivel WAN y la creación de túneles IP entre las sucursales.
- Redes MPLS, mediante la utilización de BGP extendido permiten eliminar los problemas de duplicidad de redes privadas mediante la asignación de VRFs y RD por cada VPN de clientes. (RFC 2547)

Ventajas

- Menor consumo de procesador y memoria.
- Independencia del protocolo enrutado (Capa 3). MPLS puede ser ejecutado con cualquier protocolo IP, IPX, Apple Talk.
- Independiente de la tecnología de transporte. (Capa 2). Esto mediante la habilitación de AToM (Any Transport Over MPLS).
- Permite la re-utilización de infraestructura: Solo se requiere realizar una actualización de IOS (Interworking Operation System) para que los equipos CISCO tengan características de MPLS, siempre y cuando el hardware soporte dicha actualización.
- La versatilidad de productos que se pueden ofrecer sobra una misma red: Voz, datos y video.
- Permite la clasificación y priorización de la data que transita por la red.
- Permite la comunicación entre redes MPLS con redes IP tradicionales sin problemas. Es decir, los equipos MPLS pueden conmutar etiquetas o enrutar paquetes IP con igual facilidad. Esta es de hecho la función de un Edge provider (PE).

- Soporta Ingeniería de tráfico.
- Permite la asignación dinámica de caudal, por ejemplo, cuando un caudal ORO no es utilizado puede ese ancho de banda ser utilizado por el caudal BRONCE hasta que se lo requiera de forma automática.

CAPITULO III

DISEÑO DE LA RED

DISEÑO DE LA RED FÍSICA

3.1 Visión General de la ruta del anillo

Básicamente este proyecto tienen como objetivo intercomunicar mediante una red óptica a tres de las ciudades más importantes de nuestro país como son: Guayaquil – Quito – Cuenca. Por las grandes distancias que tendremos que recorrer es recomendable dividir la ruta en tramos y cada tramo tendrá una estación que albergara un cuarto de equipos.

Fig. 3.1.- Recorrido del anillo De Fibra

Hemos considerado que nuestra red óptica, que será desplegada mediante una técnica de tendido con microzanjas, pase por todas las ciudades importantes que están en la ruta entre Guayaquil – Quito - Cuenca, ya que en estas ciudades se encontraran futuros clientes para la red.

Como es costumbre, se debe llevar a cabo un estudio detallado de la ruta, como situación física de las carreteras, clima en las ciudades donde se ubicaran los cuartos de equipos incluso en el momento de implementar proyectos como este se debe considerar el nivel delincuencial de la zona con finalidad de identificar todas las actividades que se deben efectuar antes de iniciar la instalación del cable de fibra y el levantamiento de los cuartos de equipos , tales como la preparación de la ruta en puentes, cruces bajo caminos o vías férreas. Además, es necesario determinar los sitios para los empalmes y las terminaciones de las secciones.

Es probable que se tenga que investigar la composición del subsuelo de la ruta, por ejemplo, el espesor del asfalto y los materiales del camino o de la banqueta, mediante perforaciones de prueba, como también es importante conocer si la zona es muy lluviosa y se producen continuas inundaciones con la finalidad ya que esta agua afectan las arquetan donde están localizados los empalmes.

Para Nuestro anillo de Fibra se ha considerado levantar 18 estaciones como nodos principales que contendrán el cuarto de equipos.

3.2 Recorrido de la Fibra

3.2.1. Tramo Quito - Guayaquil

RUTA	DISTANCIA
Quito – Aloag	65 Km.
Aloag –Tandapi	47 Km.
Tandapi – Santo Domingo	56 Km.
Santo Domingo – Quevedo	105 Km.
Quevedo – Ventanas	65 Km.
Ventanas - Babahoyo	50 Km
Babahoyo – Milagro	55 Km.
Milagro – Guayaquil	62 Km.
TOTAL DE LA RUTA	**505 KM**

Tabla 3.1 Distancias de la ruta Quito - Guayaquil

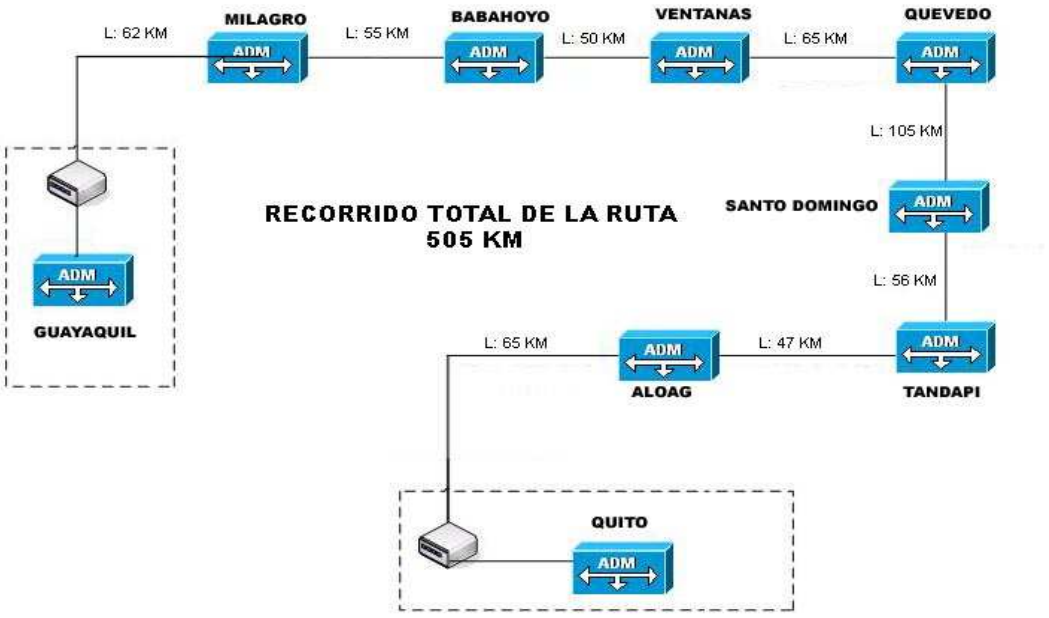


Fig. 3.2 Detalle de la Ruta Guayaquil – Quito

- **Sub.-tramo Quito - Aloag**

  Nodo Quito

  Coordenadas: 0° 07' 40.5" S - 78° 28' 18.3" W

  Distancia de Recorrido de la fibra al siguiente nodo: 65 Km.

  Numero de empalmes: 17

Fig. 3.3 Ruta principal Quito – Aloag

Comentarios de Ruta: a lo largo de esta se observan generalmente precipitaciones, la humedad esta entre 60% y 80 %. Por lo que se deben tomar precauciones con las arquetas para evitar posibles inundaciones o que la humedad afecte las fibras por medio de los empalmes.

- **Sub.-tramo Aloag – Tandapi**

  Nodo Aloag

  Coordenadas: 0° 27' 55.8" S - 78° 34' 49.3" W

  Distancia de Recorrido de la fibra al siguiente nodo: 47 Km.

  Numero de empalmes: 12

  Numero de conectores por fibra: 2

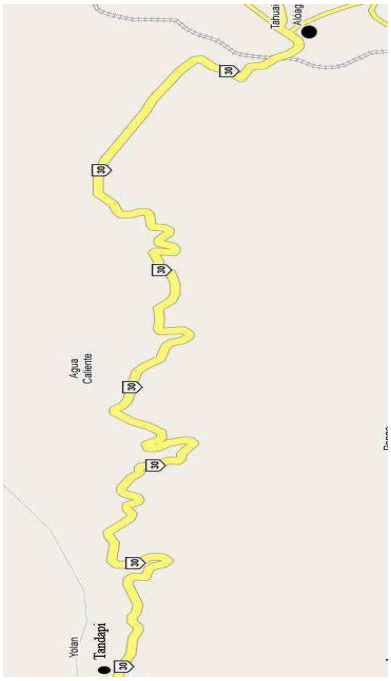


Fig. 3.4 Ruta Aloag - Tandapi

Comentarios de Ruta: La ruta Aloag - Tandapi es una de los tramos mas complicados para realizar el tendido de la fibra, pues es muy húmeda, y las precipitaciones son constantes, además, las curvas son muy pronunciadas por lo que se tienen que seguir las recomendaciones ITU – L.49 que especifica la técnica del tendido de la fibra en curvas pronunciadas.

- **Sub.-tramo Tandapi – Santo Domingo**

  Nodo Tandapi

  Coordenadas: 0° 24' 53.5" S 78° 47' 58" W

  Distancia de Recorrido de la fibra al siguiente nodo: 56 Km.

  Número de Empalmes: 14

  Numero de conectores por fibra: 2

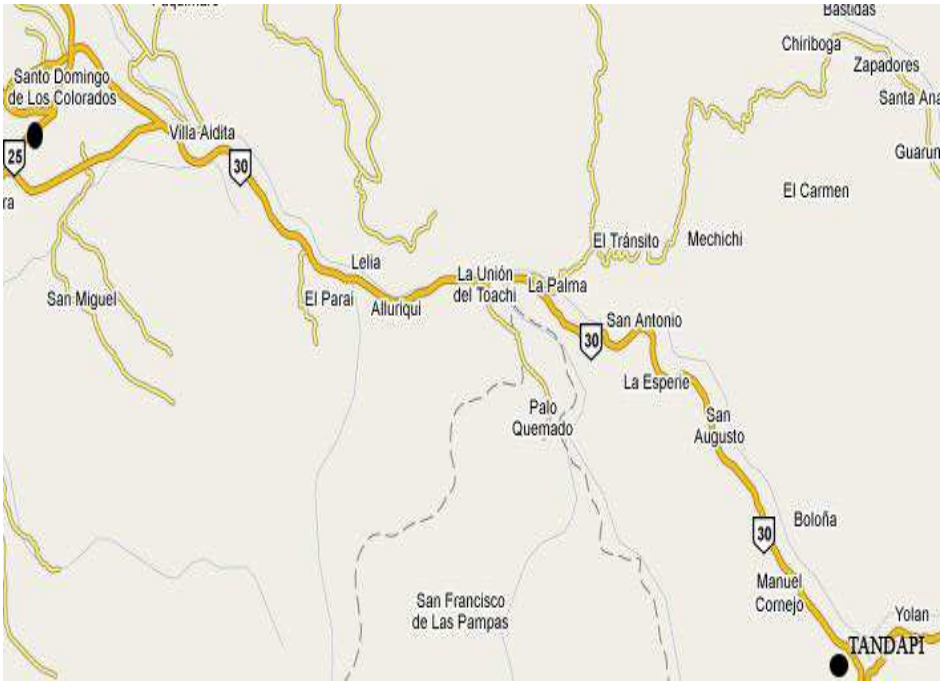


Fig. 3.5 Ruta Tandapi – Santo Domingo

Comentarios de Ruta:

Esta ruta nos presenta un mejor panorama para el tendido, sigue siendo húmeda pero no se presentan muchas curvas en el recorrido por lo que la instalación es más rápida.

- **Sub.-tramo Santo Domingo – Quevedo**

  Nodo Santo Domingo: 0° 15' 35" S 79° 10' 14" W

  Distancia de Recorrido de la fibra al siguiente nodo: 105 Km.

  Numero de empalmes: 27

  Numero de conectores por fibra: 2

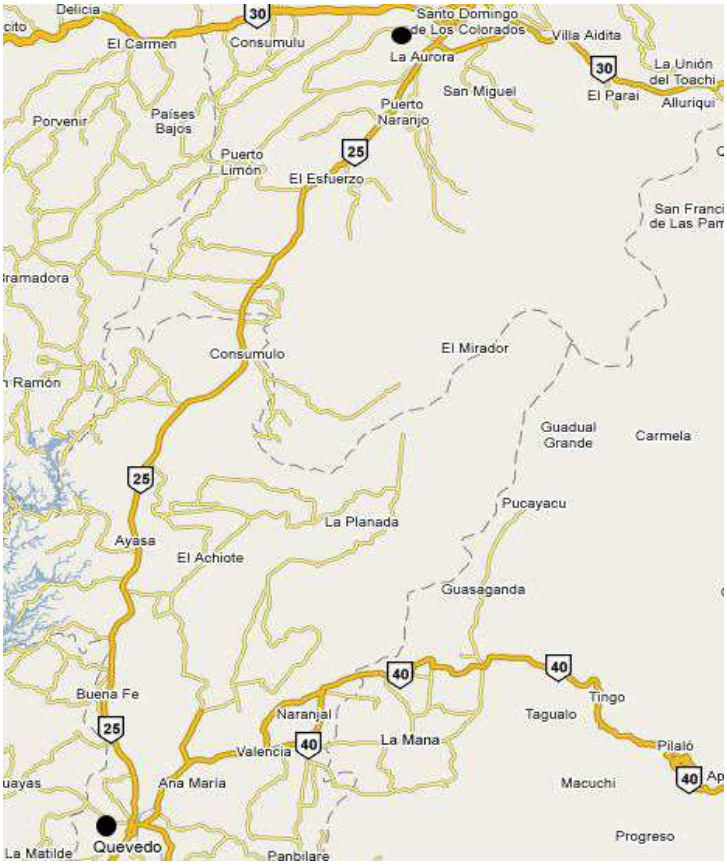


Fig.3.6 Ruta Santo Domingo Quevedo

Comentarios de Ruta: La ruta y el clima se presentan de la mejor manera técnicamente no deben presentarse mayores problemas en este tramo

- **Sub.-tramo Quevedo – Ventanas**

  Nodo Quevedo: 1° 1' 22" S 79° 27' 55" W

  Distancia de Recorrido de la fibra al siguiente nodo: 65 Km.

  Numero de empalmes: 17

  Numero de conectores por fibra: 2

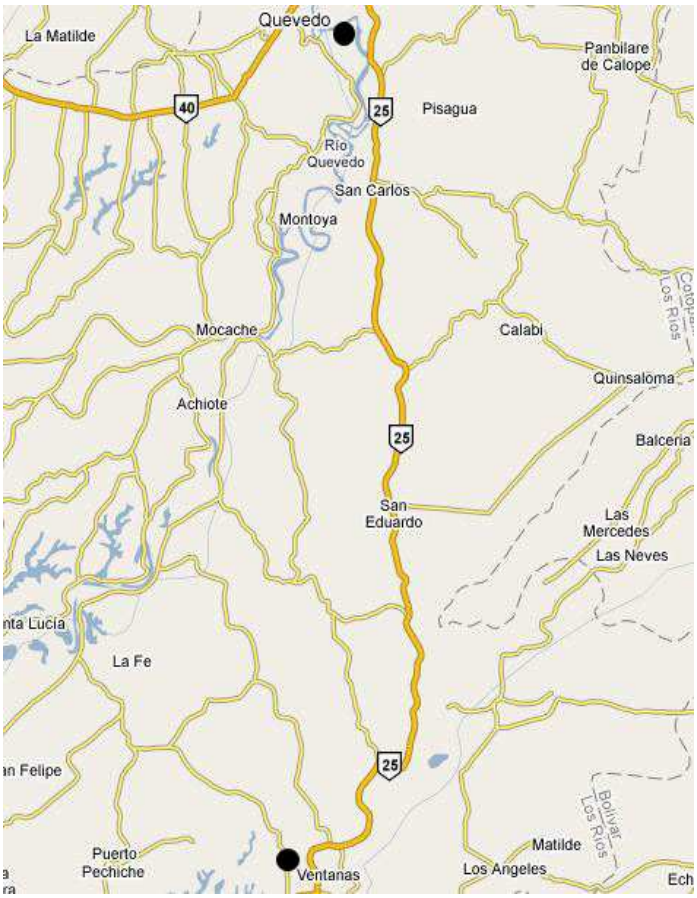


Fig. 3.7 Ruta Quevedo – Ventanas

Comentarios de Ruta: Igual que la anterior esta ruta no presenta ningún inconveniente con respecto al clima y curvas muy pronunciadas.

- **Sub.-tramo Ventanas – Babahoyo**

  Nodo Ventanas

  Coordenadas: 1° 26' 33.5" S 79° 27' 35.5" W

  Distancia de Recorrido de la fibra: 50 Km.

  Números de empalmes: 13

  Numero de conectores por fibra: 2

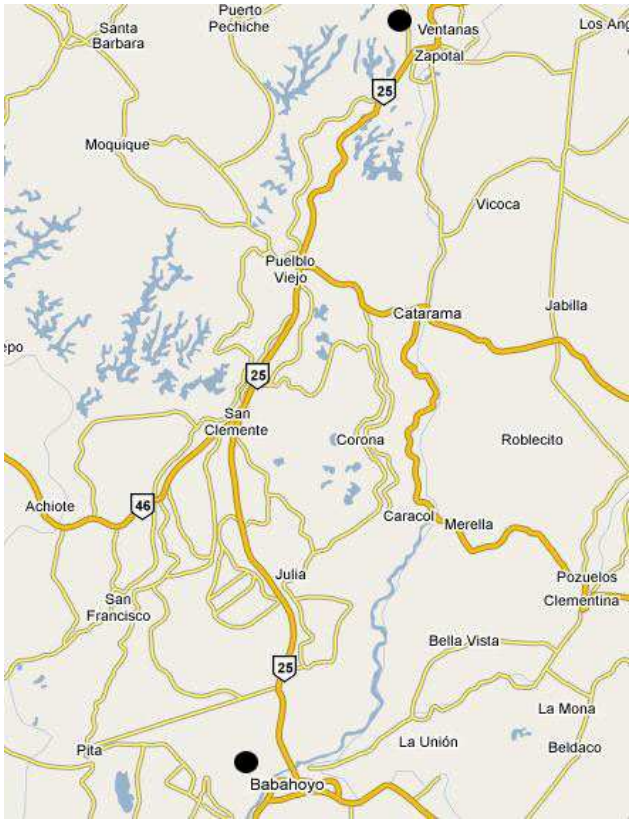


Fig. 3.8 Ruta Ventana - Babahoyo

Comentarios de Ruta. Este tramo presenta un pequeño intervalo que nos puede presentar problemas que es entre las ciudades Zapotal y Pueblo Viejo donde se presentan ciertas curvas pronunciadas.

- **Sub.-tramo Babahoyo – Milagro**

  Nodo Babahoyo

  Coordenadas: 1° 48' 6.5" S 79° 32' 7.2" W

  Distancia de Recorrido de la fibra: 55 Km

  Números de empalmes: 14

  Numero de conectores por fibra: 2

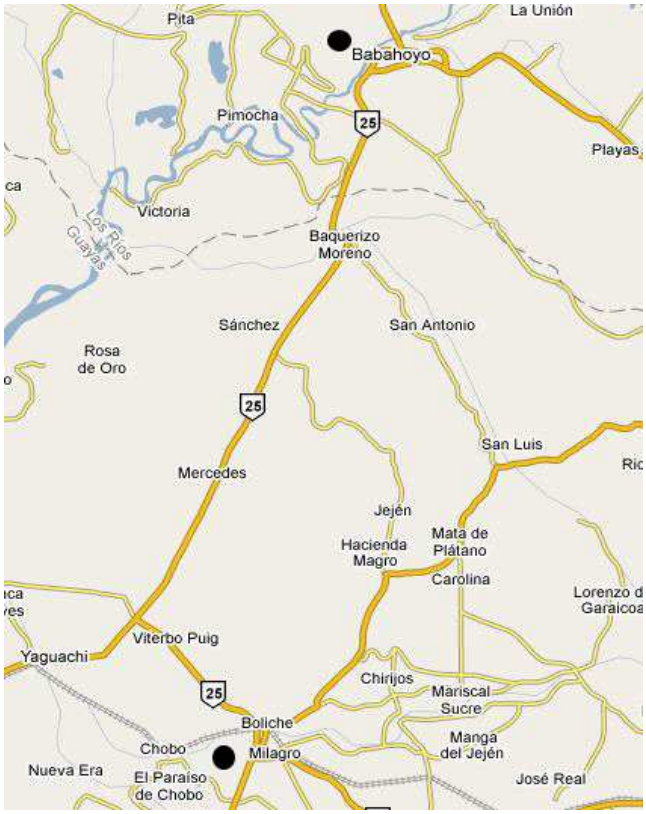


Fig. 3.9. Babahoyo - Milagro

Comentarios de Ruta: Una ruta en buenas condiciones, cabe acotar que no era necesario extenderse hasta milagro para llegar a guayaquil, sino que lo podíamos hacer por Yaguachi pero a lo largo de esa ruta solo se encuentra Yaguachi y por milagro encontramos más ciudades importantes.

- **Sub.-tramo Milagro – Guayaquil**

  Nodo Milagro

  Coordenadas: 2° 07' 43" S 79° 35' 39" W

  Distancia de Recorrido de la fibra: 62 Km.

  Números de empalmes: 16

  Numero de conectores por fibra: 2

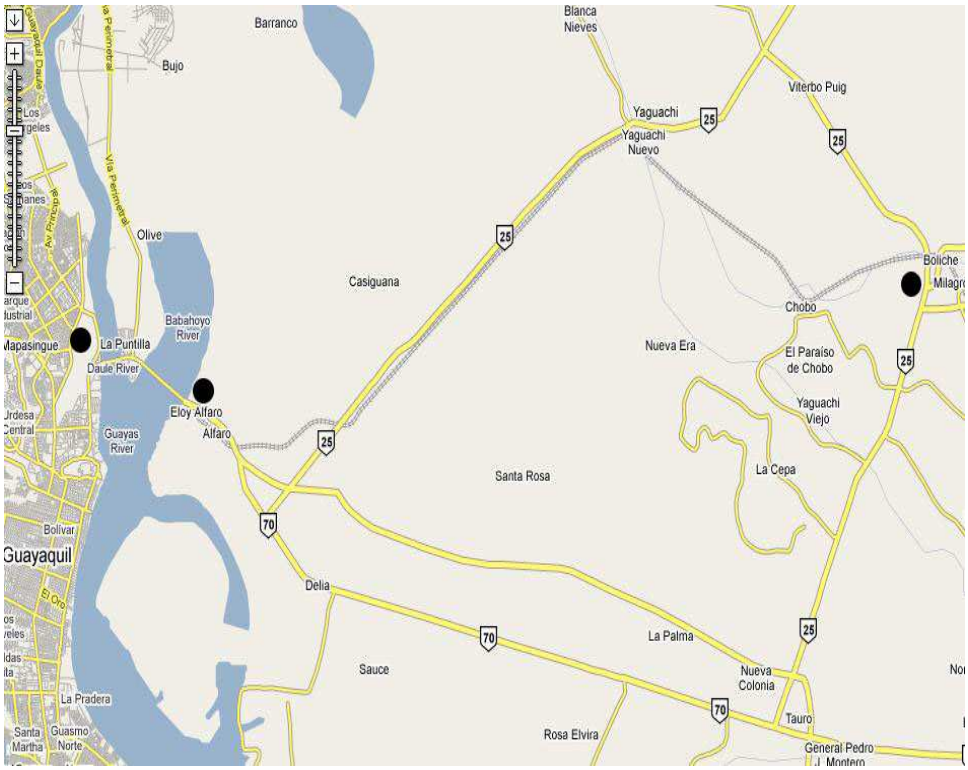


Fig.3.10 Ruta Milagro - Guayaquil

Comentarios de Ruta: Este tramo nos presenta un problema principal, que es el de el cruce en los puentes que unen Duran con Guayaquil.

3.2.2. TRAMO GUAYAQUIL - CUENCA

RUTA	DISTANCIA
Guayaquil – Naranjal	58 Km.
Naranjal – Machala	99 Km.
Machala – Santa Isabel	77 Km.
Santa Isabel – Cuenca	70 Km.
TOTAL DE LA RUTA	**304 KM**

Tabla 3.2 Distancia de la ruta Guayaquil - Cuenca

Fig.3.11 Esquema en detalle del recorrido de la fibra óptica GYE-CUE

- **Sub.-tramo Guayaquil – Naranjal**

  Nodo: Guayaquil

  Coordenadas: 2° 10' 37" S 79° 52' 43" W

  Distancia de Recorrido de la fibra próximo nodo: 58 Km.

  Números de empalmes: 15

Fig.3.12. Ruta Guayaquil - Naranjal

Comentarios de Ruta: Ruta en condiciones aceptables para el tendido de la fibra. Será necesario cubrir la carpeta asfáltica en ciertos tramos donde esta desgastada.

- **Sub.-tramo Naranjal – Machala**

  Nodo Naranjal.

  Coordenadas: 02º40´9.4´´S 79º36´54,8´´W

  Distancia de Recorrido de la fibra próximo nodo: 99 Km.

  Numero de empalmes: 25

Fig. 3.13. Naranjal Machala

Comentarios de Ruta: Ruta en condiciones aceptables para el tendido de la fibra .

- **Sub.-tramo Machala – Santa Isabel**

  Nodo Machala

  Coordenadas: 03º14´47,7´´S. 79º49´41,7´´W.

  Distancia de Recorrido de la fibra próximo nodo: 77 Km.

  Numero de empalmes: 20

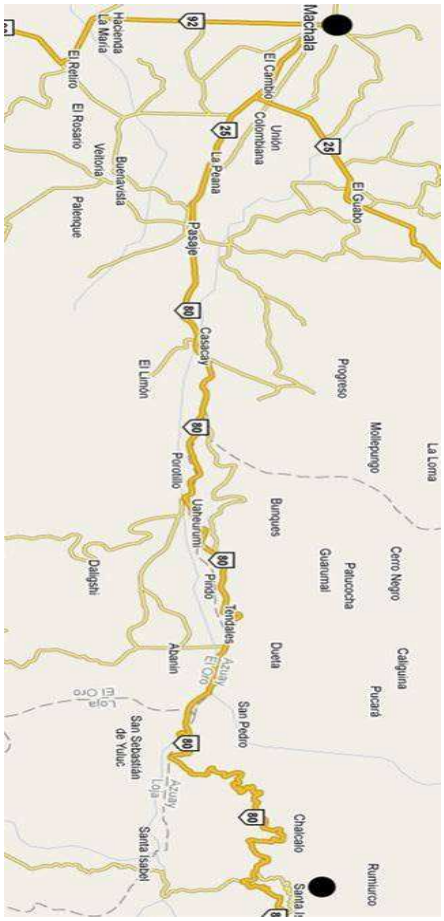


Fig. 3.14 Machala - Santa Isabel

Comentarios de Ruta. Ruta cuyos factores climáticos no son extremos, pero presenta muchas curvaturas desde aprox. 35 Km. antes de llegar a Santa Isabel.

- **Sub.-tramo Santa Isabel - Cuenca**

  Nodo Santa Isabel

  Coordenadas: 03º16´29´´S 79º18´50,4´´W

  Distancia de Recorrido de la fibra próximo nodo: 70 Km

  Numero de empalmes: 18

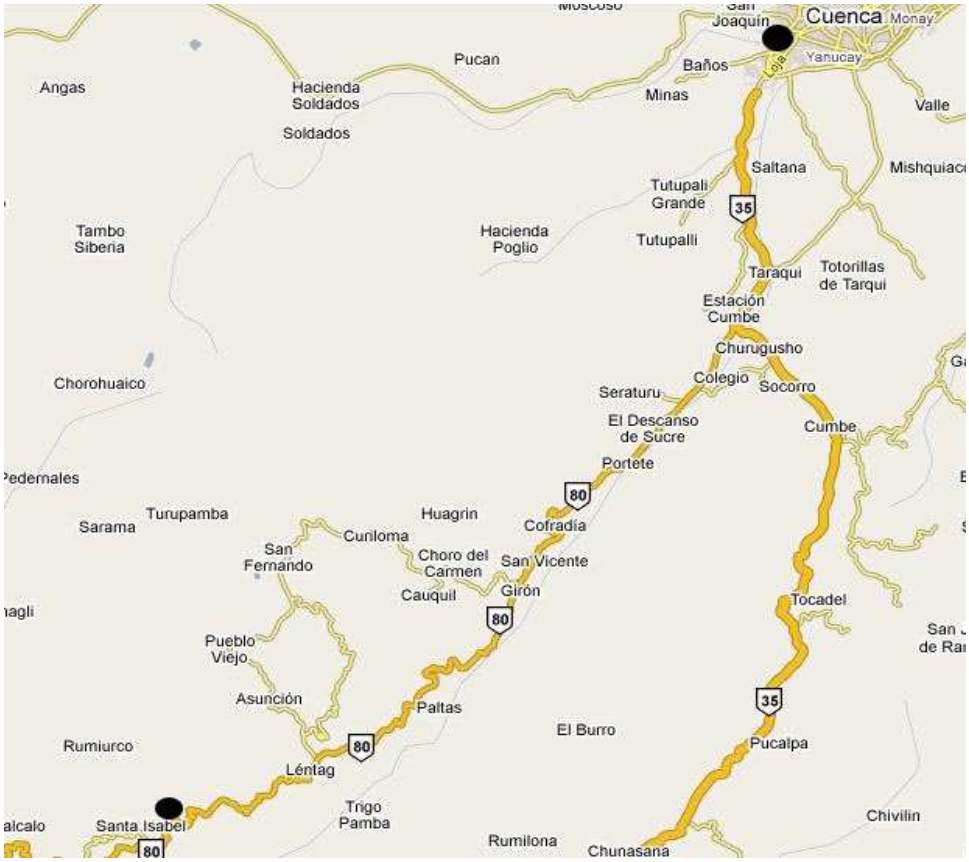


Fig. 3.15 Santa Isabel - Cuenca

Comentarios de Ruta. En esta ruta encontraremos inconvenientes en los primeros kilómetros ya que se presentan muchas curvas.

3.2.3 RUTA CUENCA – QUITO

SUB-RUTA	DISTANCIA
Cuenca - Zhud	93 Km
Zhud - Alausi	58 Km
Alausi - Riobamba	81 Km
Riobamba - Ambato	63 Km
Ambato - Latacunga	95 Km
Latacunga - Quito	90 Km
TOTAL	480 KM

Tabla 3.3.- Distancias del recorrido Cuenca - Quito

Fig.3.16 Esquema en detalle del recorrido de la fibra óptica UIO-GYE

- **Sub.-tramo Cuenca – Zhud**

  Nodo Cuenca

  Coordenadas: 02º53´49.10´´S 79º00´37,88´´W

  Distancia de Recorrido de la fibra próximo nodo: 93 Km

  Numero de empalmes: 24

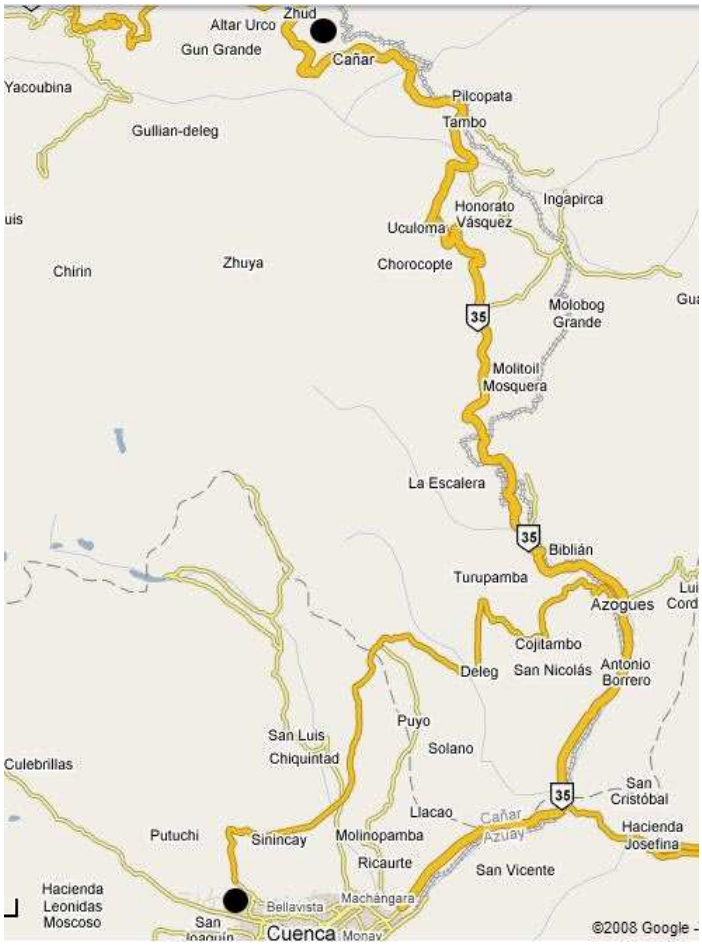


Fig. 3.17 Ruta Cuenca – Zhud.

Comentarios de Ruta. Esta Ruta se manifiesta muy humedad entre 70 % y 90 % y siempre se están presentando precipitaciones.

- **Sub.-tramo Zhud– Alausí**

  Nodo Zhud

  Coordenadas: 02º27´41,06´´S 79º00´18,73´´W

  Distancia de Recorrido de la fibra próximo nodo: 58 Km

  Numero de empalmes: 15

Fig. 3.18 Ruta Zhud. - Alausi

Comentarios de Ruta: Esta es una ruta muy difícil por sus curvas muy pronunciadas y su temperatura es muy baja 0 – 5 grados Celsius y una humedad del 90 % y se presentan muchas precipitaciones las condiciones extremas obligan a que las instalaciones deben ser realizados con mucho profesionalismo.

- **Sub.-tramo Alausí - Riobamba**

  Nodo Alausí

  Coordenadas: 02º11´36,43´´S 78º50´38,86´´W

  Distancia de Recorrido de la fibra próximo nodo: 81 Km

  Numero de empalmes: 21

Fig. 3.19 Ruta Alausí - Riobamba

Comentarios de Ruta: Esta es una ruta que no presenta muchas curvas pronunciadas pero su temperatura es muy baja 3 – 9 grados Celsius y una humedad del 90 % y se presentan muchas precipitaciones las condiciones extremas obligan a que las instalaciones deben ser realizados con mucho profesionalismo.

- **Sub.-tramo Riobamba – Ambato**

  Nodo Riobamba

  Coordenadas: 01º39´45,31´´S 78º50´38.86´´W

  Distancia de Recorrido de la fibra próximo nodo: 63 Km

  Numero de empalmes: 16

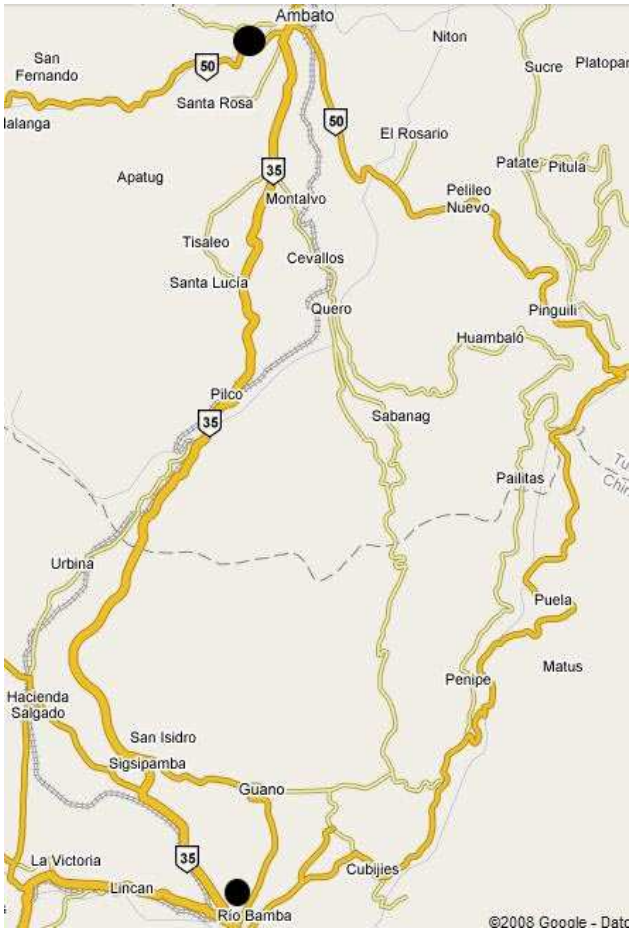


Fig. 3.20 Ruta Riobamba - Ambato

Comentarios de Ruta. –Esta ruta no presenta muchas dificultades con las calles, pero se siguen manteniendo las bajas temperaturas y las lluvias frecuentes.

- **Sub.-tramo Ambato - Latacunga**

Nodo Ambato

Coordenadas: 01º25´30,31´´S 78º61´22.86´´W

Distancia de Recorrido de la fibra próximo nodo: 95 Km.

Numero de empalmes: 24

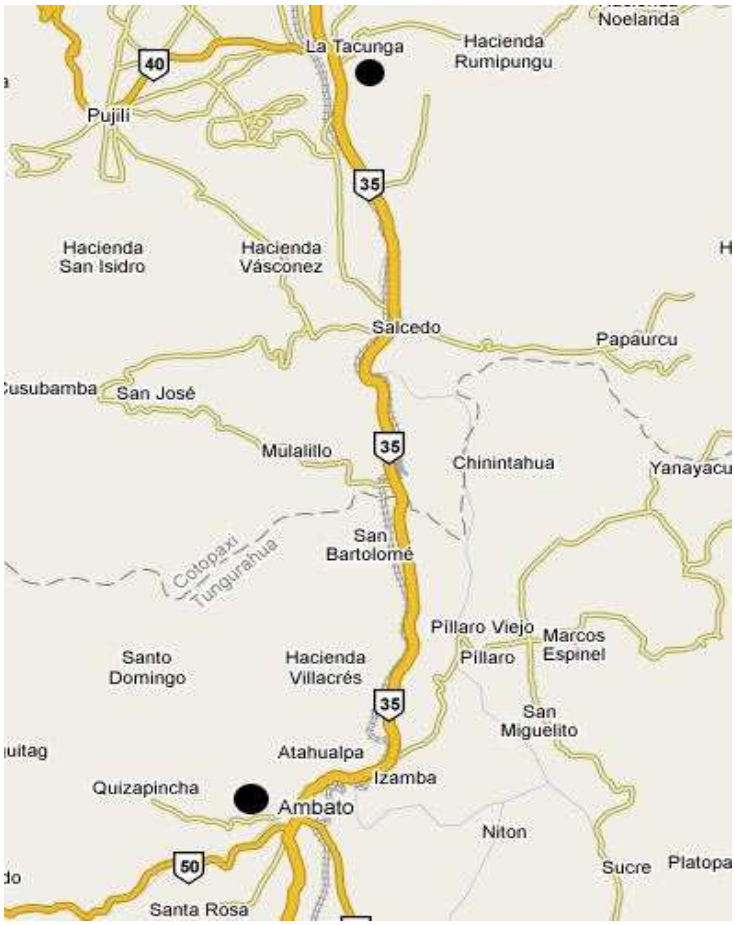


Fig. 3.21 Ruta Ambato – Latacunga

Comentarios de Ruta. –Esta ruta no presenta dificultades tanto en temperatura como en relieves de calles, pero las lluvias se presentan muy seguidas a lo largo de la ruta.

- **Sub.-tramo Latacunga - Quito**

  Nodo Latacunga

  Coordenadas:

  Distancia de Recorrido de la fibra próximo nodo: 90 Km.

  Numero de empalmes: 23

Fig. 3.22 Ruta Latacunga - Quito

Comentarios de Ruta. –Esta ruta no presenta dificultades tanto en temperatura como en relieves de calles, pero las lluvias se presentan muy seguidas a lo largo de la ruta. La humedad de la ruta promedia 80 %.

3.3 Cuartos de Equipos de los Nodos

El cuarto de equipo es un espacio de uso específico para equipo de telecomunicaciones tal como Equipos de red, central telefónica, equipo de cómputo, etc.

Un cuarto de equipos debe proveer las siguientes funciones:

- ✓ Un ambiente controlado para los contenedores de los equipos de telecomunicaciones.
- ✓ El hardware de conexión.
- ✓ Las cajas de uniones.
- ✓ Las instalaciones de aterrizaje
- ✓ Los aparatos de protección, dónde se necesiten.
- ✓ Generadores

El espacio del cuarto de equipos no debe ser compartido Equipos que generan vibraciones fuertes y las instalaciones eléctricas de equipos que demanden gran energía no deben ser las mismas que las de los equipos de telecomunicaciones. Además, el cuarto de equipo debe ser capaz de albergar equipo de telecomunicaciones, terminaciones de cable y cableado de interconexión asociado.

3.3.1 Características Generales

Todos los cuartos de Equipos deberán tener lo siguiente.

Descripción	**Característica**
Dimensiones recomendadas	4.5 x 4 mt área 3 mt. altura
Alimentación de energía	220 v – 110 v
Sistema de Tierra	0-4 ohm
Rectificador DC -48 V	60 Amp
Cajas de Breaker	2
Breaker	2x 50 Amp - 4 x 25 Amp
Generador	12 KVA
Aire Acondicionado	18000 BTU
Baterías	2x100 Amp /hora
Rack	2.2 mts Pintura Electrostática
Gabinete para ADM	2.2 mts Pintura Electrostática
Bandejas Metálicas canalizado	4 mts * 0.5 mt

Tabla 3.4 Características de los Cuartos de Equipos

3.3.2. Plano del Cuarto

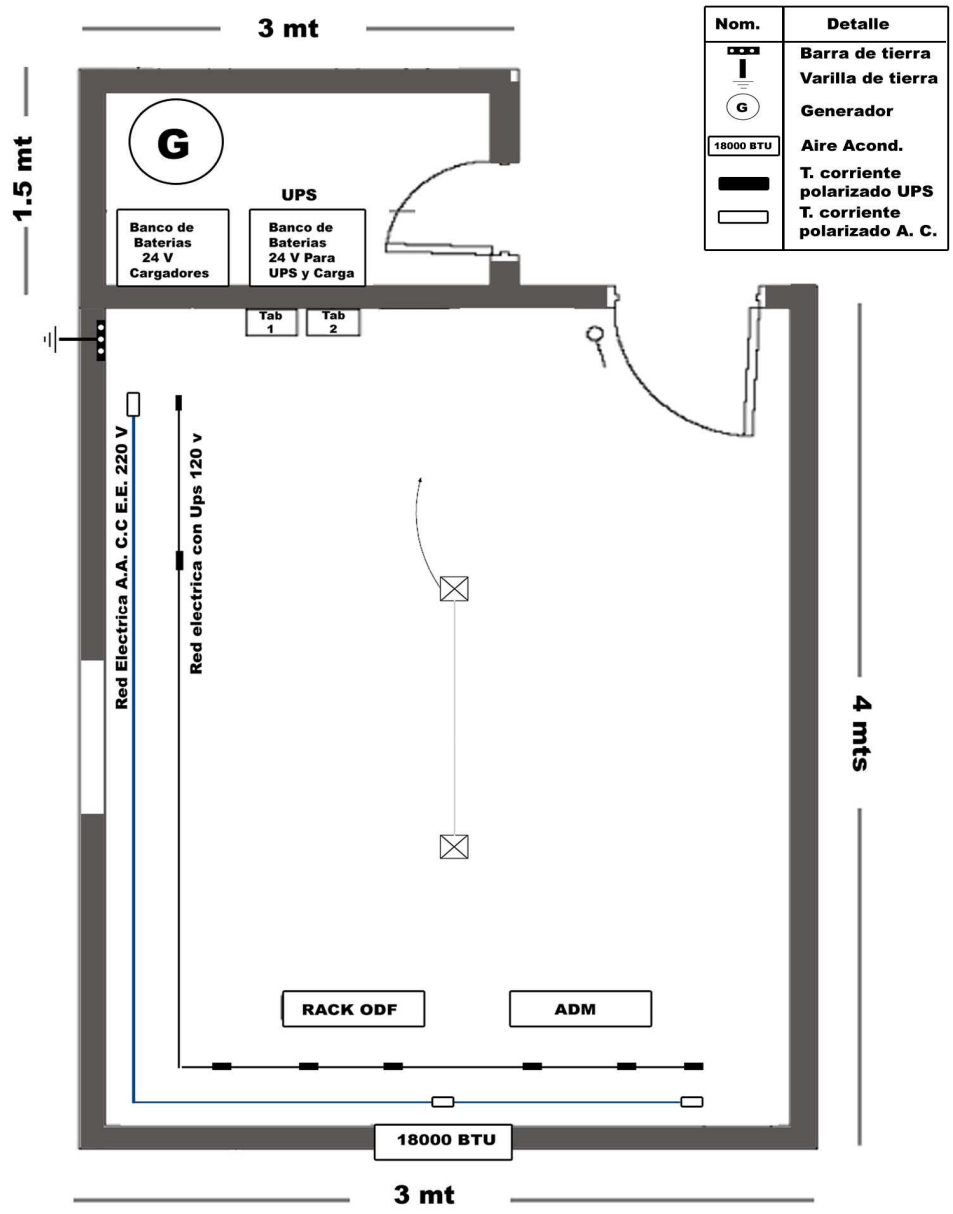


Fig. 3.23 Plano del cuarto de equipos

3.4 Diagrama Esquemático bajo dimensionamiento y especificaciones Técnicas.

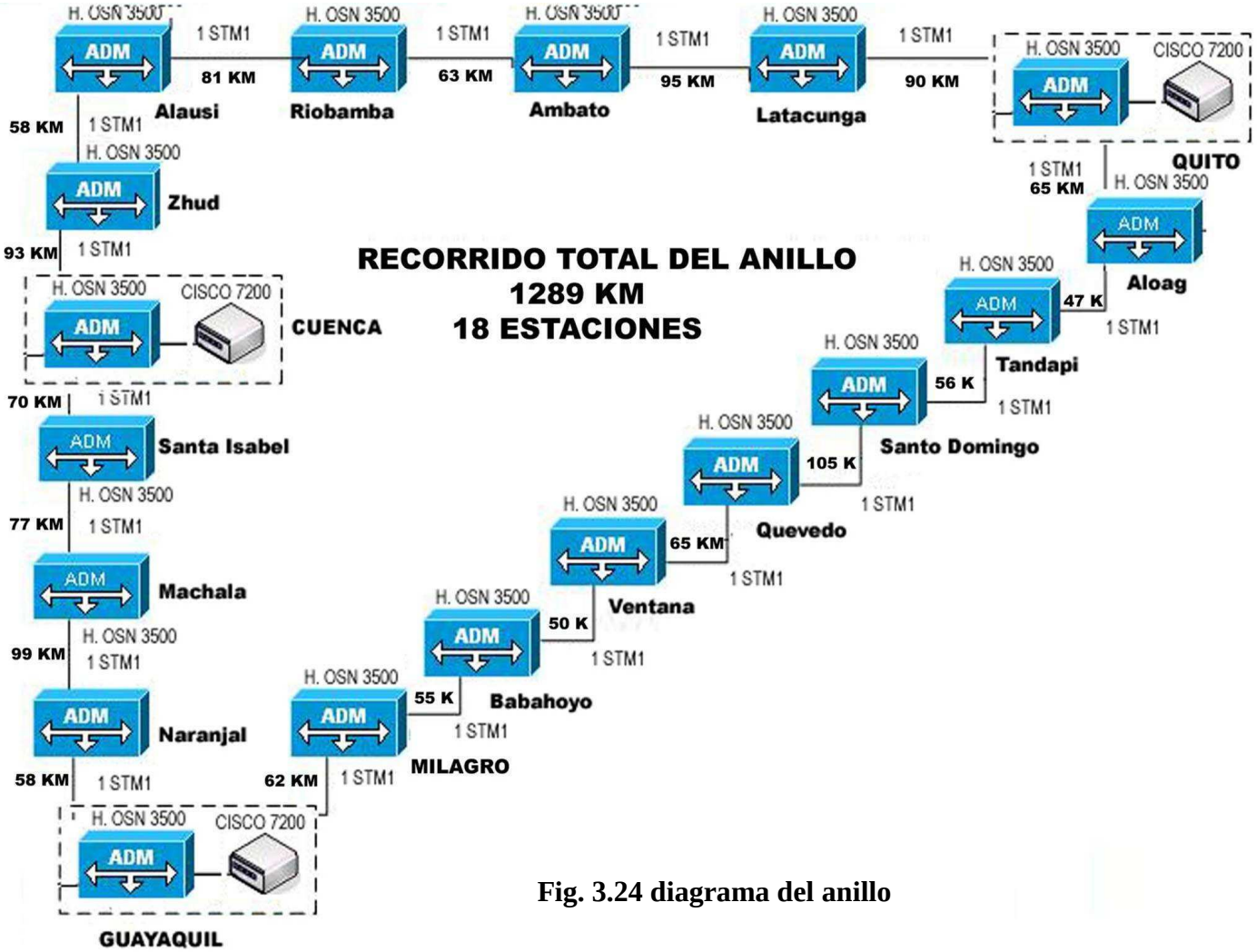


Fig. 3.24 diagrama del anillo

CAPITULO IV

Diseño de la red

IMPLEMENTACIÓN DE LA RUTA Y DIMENSIONAMIENTO DE LOS EQUIPOS.

4.1. Descripción del diseño

Para la realización del diseño de nuestra red se ha considerado el levantamiento de 3 nodos principales que estarán ubicados dentro de las tres ciudades que deseamos intercomunicar (Guayaquil, Quito, Cuenca), los cuales se implementarán con equipos de marca Cisco modelos 72006VXR que nos permiten manejar hasta un ancho de banda de 1 STM - 4 sin realizar cambios importantes en el hardware. La red estará basada en una topología en anillo que dará redundancia al sistema con una ruta alternativa en caso de problemas con el trayecto original. Debido a la gran distancia que existe entre los puntos a comunicar se ha procedido a dividir la ruta en tramos, mencionados en el Capitulo anterior. En cada una de las ciudades importantes que se encuentran en la ruta se montará un cuarto de Equipos el cual alojara un RACK central con los equipos ADM que permitirán la regeneración de señal (Huawei Optix OSN 3500) y conjuntamente con otro hardware darán acceso a la red a futuros clientes. Cabe mencionar que cada cuarto de equipos deberá estar acondicionado con todos los sistemas de seguridad para garantizar optimo funcionamiento del los equipos. Para el tendido de la fibra óptica se utilizara una nueva técnica por medio de microzanjas basada en la recomendación UIT-T L.49, una técnica que a inicios fue desarrollada para los anillos internos urbanos por su versatilidad de despliegue y su menor costo, pero ahora este concepto es utilizado para redes de larga distancia .

4.1.1. Procedimiento para el diseño de un enlace por fibra óptica.

Para realización del diseño del enlace es importante considerar los siguientes pasos:

1. Escoja la ruta adecuada y conozca las distancias de cada tramo
2. Determinar el ancho de banda con el que va a trabajar la Red
3. Determine la distancia del enlace, esto es, la distancia entre el transmisor y el receptor, en nuestro caso la distancias entre tramos.
4. Seleccione una fibra basada en los niveles atenuación necesaria.
5. Calcule el ancho de banda de la fibra del sistema. Esto se logra midiendo el factor de ancho de banda en Mhz. / Km., para la distancia del enlace, el factor de ancho de banda esta dado en tablas del fabricante.
6. Determine el margen de potencia. Esto es, la diferencia entre potencia de salida de la fuente de luz y la sensibilidad del receptor.
7. Determine la perdida total multiplicando la pérdida de la fibra en dB/Km. por la longitud del enlace en Km.
8. Identifique el número de conectores, multiplique la pérdida del conector (dado por el fabricante), por el número de empalmes. Multiplique la pérdida de empalme (dado por el fabricante), por el número de ramas.
9. Identifique el número de empalmes. Multiplique la pérdida de empalme (dado por el fabricante), por el número de ramas.
10. Haga 1dB para la perdida de acoplamiento del detector.
11. Ponga 3dB para la degradación de la temperatura.
12. Ponga 3dB para la degradación del tiempo.
13. Sume las perdidas y compare con las del fabricante del cable de fibra

14. Tome decisiones con respecto a la localización de los amplificadores

Los pasos 10, 11, 12, son consideraciones que hay que seguir para un diseño completo y altamente eficiente

4.1.2 Procedimiento para el diseño interior en los nodos

El cuarto de equipo es el espacio que utilizaremos para el uso específico de los equipos de comunicaciones tales como Optix Osn 3500, equipo de cómputo, Etc. Los cuartos de equipo incluyen espacio de trabajo para personal de telecomunicaciones. Los requerimientos del cuarto de equipo están basados en los estándares ANSI/TIA/EIA-568-A y ANSI/TIA/EIA-569.

- El Área mínima de acuerdo a la recomendación para el cuarto de equipos es 14 m2. para nuestros cuartos de equipos se considera 18 m2 de área.
- La Altura Mínima será de 3 Mt.
- Se debe considerar una altura adecuada del piso para evitar inundaciones, este estudio será basado por el tipo y ubicación del terreno.
- Los cuartos deben tener 2 divisiones una sola destinada para los equipos de telecomunicaciones y otra para los equipos de alimentación de energía como generadores, baterías, etc. Y se recomienda un área de 6 mt2 para estos equipos.
- El cuarto de equipos debe ser diseñado considerando una entrada de aire externo como por ejemplo ventanas.
- La puerta del cuarto de equipos debe tener mínimo un ancho de 0,9 m y 2,4 m de alto y abrir hacia fuera o ambos lados.
- Colocar mínimo dos tomas eléctricas en circuitos separados

- Colocar tomas auxiliares cada 1.8 m alrededor del perímetro del cuarto, a una altura de 15 cm. sobre el suelo.
- Deberán albergar 1 Rack donde estarán localizados los ODF y un Gabinete que deberá albergar al OSN 3500
- Todos los cables de energía y de comunicaciones deben pasar por bandejas porta cables tipo escalera sin sobrepasar el 40 % de llenado por la parte superior del cuarto. Cuando pasan por la misma canaleta deben estar separados por barreras entre el cableado lógico y el eléctrico; incluso dentro de cajas o compartimentos de tomas, debe haber separación física total entre los cableados.
- Las bandejas porta cables y canaletas metálicas deben estar debidamente aterrizadas.
- Equipos no relacionados a la entrada de servicio de telecomunicaciones, como cañerías, bombas hidráulicas, etc., no se deben instalar ni deben pasar a través de la sala.

Fig. 4.1.- Instalación de de Rack y Gabinetes

Fig. 4.2.- Bandeja para tendido del cable en el interior del cuarto de equipos

4.2. Configuración del sistema

- ✓ En el Rack se colocaran los ODF, deben estar perfectamente identificado a que nodo corresponden. Nombre del nodo donde provienen y nodo de localización actual
- ✓ Las fibras que llegan desde un nodo se alojaran en el ODF que llevara el nodo de donde proviene.
- ✓ Los dos hilos de fibras con los que se realiza la comunicación pasan de la salida del ODF hasta el ADM (Optix OSN 3500).
- ✓ Los otros 22 hilos de fibras deben quedar conectados en el ODF de donde provienen.
- ✓ La salida del Optix OSN 3500 de los dos hilos de fibra Salen hacia el ODF que deberá llevar el nombre del nodo de posición actual.
- ✓ Los otros 22 hilos de fibra salen del ODF de posición actual para seguir el recorrido.
- ✓ Todas las conexiones para la alimentación deben realizarse desde las tomas de energía que se encuentran en el Rack.
- ✓ Las tomas de corriente del rack y gabinete deben estar conectadas a los UPS general del cuarto de Equipo

- ✓ EL UPS del Cuarto de Equipos deben estar conectadas a la red de distribución que en caso de fallar debe alternar con el generador.

4.3. Consideraciones técnicas sobre el diseño

El diseño que se presenta en este proyecto de tesis depende de muchas consideraciones que deben tomarse en cuenta para escoger los equipos y materiales con que se va a formar la red.

1. Determinación de una fibra óptica con las características adecuadas de tal manera que resista, tensiones adecuadas, el ambiente donde va a residir la fibra.
2. Identificación de la trayectoria exacta del cable. Al momento de tender la fibra óptica. Se deben cumplir con las normas que rigen los sistemas de fibra, es importante considerar que se debe obtener el debido permiso para la utilización de los postes y vías por las cuales se realizara el tendido de la fibra.
3. Las perdidas totales a lo largo del trayecto
4. El numero de empalmes y conectores requeridos para el trayecto.
5. Verificar que todos los empalmes, conectorizacion fueron correctamente realizados con la finalidad de garantizar la fiabilidad de transmisión y poder considerar los valores normalizados que necesitamos para los cálculos.
6. Que las reflectancias máximas de los componentes (conectores, empalmes, atenuadores, etc.) entre los puntos Transmisor - Receptor no sobrepasan los limites establecidos por la interface.
7. Que las perdidas por flexión, envejecimiento, tracción, microcurvaturas, etc. Estén incluidos en el peor caso de diseño.
8. Que al momento del tendido de la fibra no se exceda los valores dados como limites tanto en tracción, curvatura, temperatura, etc.

9. Que el tendido de la fibra se lo realice a un costado de la carretera y buscando las menos transitadas. Esto ayudara mucho a la vida de la fibra una vez enterrada
10. Que la longitud de onda del sistema es mayor a la longitud de onda de corte para el tramo más pequeño, garantizando de esta manera el desempeño monomodo.
11. Que los empalmes se colocan cada 4 Km. debido a que las bobinas de fibra óptica vienen de esa medida. Esto es muy importante en el momento del cálculo de las pérdidas.

4.3.1. Elementos Activos y Pasivos a utilizar

4.3.1.1. Características técnicas de los elementos activos

Para el diseño de la red, en lo referente a los equipos de networking hemos tomado en consideración las siguientes premisas:

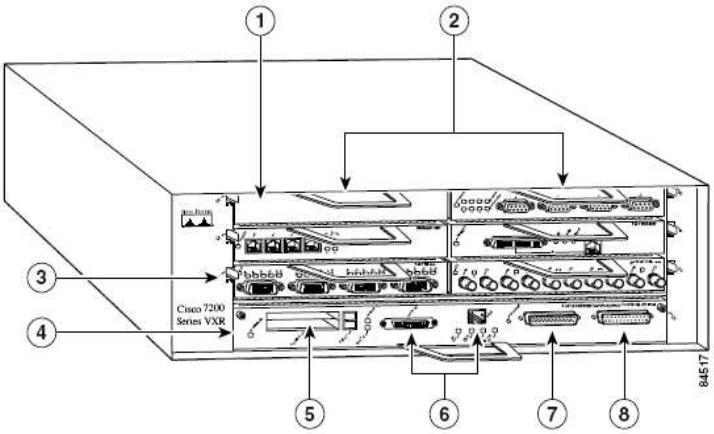
1. Escalabilidad: Equipos que soporten incrementos en demanda de consumo de memoria y procesamiento y que mediante un sistema modular permitan realizar crecimiento que no impacten de forma significativa el presupuesto operacional de la red.
2. Durabilidad: Equipos que ofrezcan un amplio reconocimiento en el mercado en cuanto a la calidad de sus productos desarrollados.
3. Soporte: Equipos cuyos fabricantes acrediten un amplio reconocimiento en el mercado en cuanto a su esquema de soporte y repuestos.
4. Estandarización: Equipos que permitan una aceptable interoperabilidad entre equipos de otras marcas.
5. Costos: Equipos que permitan poder operar la red según el ancho de banda inicial de 1SMT-1 con crecimientos futuros de hasta 1 STM-4 sin necesidad de cambios importantes de hardware al menor costo posible.

En base a los criterios expuestos, se optó por equipos de la marca CISCO, específicamente el modelo Cisco 7206VXR para que sea el equipo CORE de nuestra red y se proceda en la implementación de los equipos:

- ✓ P Quito – P01 UIO
- ✓ P Guayaquil – P01GYE
- ✓ P Cuenca – P01CUE
- ✓ PE Quito – PE01UIO
- ✓ PE Guayaquil – PE01GYE
- ✓ PE Cuenca – PE01CUE

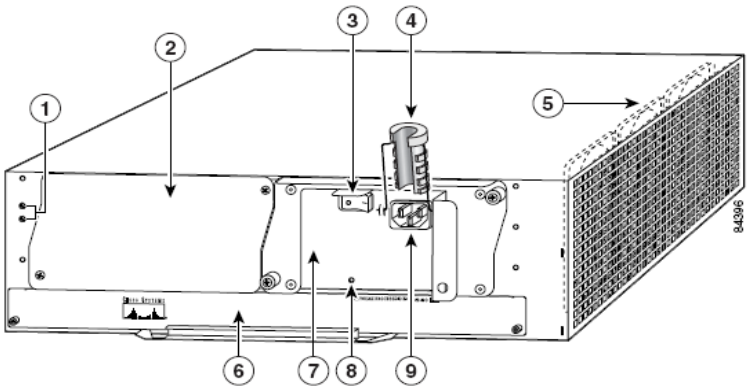
Equipo Cisco 7206VXR

El equipo Cisco 7200VXR pertenece a la familia de los equipos multiservicios de Cisco enfocados a las grandes empresas proveedoras de servicios de comunicación. Estos equipos están diseñados para soportar capacidad de Gigabit y para mejorar la integración de los servicios de transmisión de datos, voz y video en ambientes de redes de proveedores e incluso empresariales.



1	Blank port adapter	5	PC Card slots
2	Port adapters	6	Optional Fast Ethernet interface (MII port and RJ-45 port)
3	Port adapter lever	7	Auxiliary port
4	I/O controller	8	Console port

Fig. 4-3.- Equipo Cisco 7206VXR – Vista Frontal



1	Chassis grounding receptacles	6	Network processing engine or network services engine
2	Power supply filler plate	7	AC-input power supply
3	Power switch	8	PWR OK LED
4	AC power cable-retention clip	9	AC power supply receptacle
5	Internal fans		

Fig. 4-4.- Equipo Cisco 7206VXR – Vista Trasera

Este tipo de equipos ofrecen una amplia gamma de interfaces de conexión que van desde interfaces eléctricas de conexiones LAN y WAN hasta puertos para conexiones ópticas, además

este equipo incluye soporte para la tecnología NPE (Network Processing Engine) y NSE (Network Service Engine).

Ranuras de Expansión.-

Este equipo cuenta con 6 ranuras de expansión, distribuidas de la siguiente forma:

- 4 para adaptadores de puerto. (Interfaces)
- 1 para una controladora de I/O.
- 1 para una tarjeta NPE o NSE.

A continuación, se resume en un cuadro (tomado del data sheet de Cisco) todas las características físicas del equipo Cisco 7206VXR

Description	Specification
Midplane	Two primary PCI buses, and one secondary PCI bus • With an NPE-G2 or NPE-G1 and an I/O controller installed, the I/O controller does not use bandwidth points, and the NPE-G2 or NPE-G1 does use bandwidth points. The NPE-G2 or NPE-G1 does not use bandwidth points if installed without the I/O controller. • With an NSE-1, NPE-400, or NPE-300 installed: aggregate bandwidth of 900 Mbps[1] • With n NPE-100, NPE-150, or NPE-200 installed: aggregate bandwidth of 600 Mbps Three primary PCI buses—With the NPE-G2 or NPE-G1 installed, no I/O controller, and the Port Adapter Jacket Card installed, three PCI buses are available. Aggregate bandwidth of the PCI buses is 900 Mbps. The third PCI bus goes to the Port Adapter Jacket Card and provides unlimited bandwidth for one port adapter.
Dimensions (H x W x D)	5.25 in. x 16.8 in. x 17 in. (13.34 cm x 42.67 cm x 43.18 cm)
Weight	Chassis fully configured with a network processing engine or network services engine, I/O controller, maximum number of port adapters, 2 power supplies, and a fan tray: ~ 50 lb (22.7 kg)
Heat dissipation	370W (1262 BTU[2])
Chassis fan noise levels—single speed fan	Tested: • Front (I/O controller and port adapter side) 44.2 dB • Back (power supply side) 43.7 dB • Left (fan side) 47.2 dB • Right 44.8 dB
	Maximum: 65 dB
Airflow	~80 cfm[3]
Temperature	32 to 104°F (0 to 40°C) operating; –4 to 149°F (–20 to 65°C) nonoperating
Humidity	10 to 90% noncondensing
Power Specifications	
AC-input voltage rating	100–240 VAC[4] wide input with power factor correction
AC-input current rating	5A[5] at 100–240 VAC with the chassis fully configured
AC-input frequency rating	50/60 Hz[6]
AC-input cable	18 AWG[7] three-wire cable, with a three-lead IEC-320 receptacle on the power supply end, and a country-dependent plug on the power source end
DC-output power	280W maximum (with either a single or dual power supply configuration)
DC-input voltage rating	–48 VDC[8] nominal in North America –60 VDC nominal in the European Community

Fig. 4-5.-Especificaciones Físicas Cisco 7206VXR

A nivel de IOS (Sistema operativo Cisco) el fabricante recomienda el siguiente listado de IOS mínimos que deben ser ejecutados por este dispositivo:

- Cisco IOS Release 12.0(2)XE2 or later releases of 12.0XE
- Cisco IOS Release 12.1(1)E or later releases of 12.1E
- Cisco IOS Release 12.0(5)S or later releases of 12.0S
- Cisco IOS Release 12.0(3)T or later releases of 12.0T
- Cisco IOS Release 12.2(1) or later releases of 12.2
- Cisco IOS Release 12.2(4)B or later releases of 12.2B
- Cisco IOS Release 12.4(7)
- Cisco IOS Release 12.4(4)XD

Este proyecto de tesis se ha considerado desarrollar el laboratorio en base al IOS –c7200-js-mz.124-7e para uso de proveedores, mismo que soporta protocolo MPLS y las aplicaciones QoS, VPN y TE.

Equipo Huawei OPTIX OSN 3500

Estos equipos provienen de la serie Optix proporcionados por el fabricante HUAWEI y funcionan como multiplexores, sistemas Add Drop y como Cross connect.

Este equipo permite transmisión integrado a velocidades de 2.5G (STM-16) y 10G (STM-64) como interfaces de línea.

Es una plataforma de transmisión multiservicios, compatible con las tradicionales redes SDH e integra además, muchas y variadas tecnologías, tales como PDH, Ethernet, WDW, ATM y MPLS , entre otras tecnologías.

Características Optix OSN 3500

a) Plataforma económicamente eficiente:

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

b) Configuración flexible: -Compatibilidad con STM-64/16

Soporta actualización on-line de 2.5G a 10G, esto es muy importante para nuestro proyecto ya que inicialmente se empieza con STM-1, pero luego va a surgir la necesidad de migrar a mayores anchos de banda.

c) Alta capacidad en la planificación:

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

d) Provisión multiservicio

1) Interfaces

-STM-1 (O/E);

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

-E1/T1/E3/T3/E4;

-ATM

-IMA, SAN y otros

Utiliza la protección de trayectoria virtual de fibra compartida (fiber – share virtual protection)
Una sola ranura puede acomodar directamente hasta seis interfaces ópticas 40 STM-1, 16 STM 4, STM 16 o alguna combinación de estas.

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

a) Alta integración

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

b) Robusto

Soporta incorporación dinámica de nodos a la red enmallada y permite actualización y expansión en línea. Cada subrack puede habilitar anillos 1xSTM-64 de cuatro fibras o anillos 2xSTM-16 de cuatro fibras o anillos 4xSTM-16 de dos fibras

c) Tecnología WDM incorporada

Provee dos canales ópticos para tarjetas ADM

d) Completos mecanismos de protección de red

-Recuperación de mallas

-Mecanismos distribuidos de recuperación de rutas de protección

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

-Protección SDH

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

e) Protección de servicio de datos

Soporta protección en anillo RPR y STP spanning tree protection;

Soporta protección de anillo VP-RING para servicios ATM

f) Completos mecanismos de protección de equipo

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

-Protección de energía y térmico (TPS)

g) Características físicas

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

Fig. 4-6.- Equipo OptiX OSN 3500

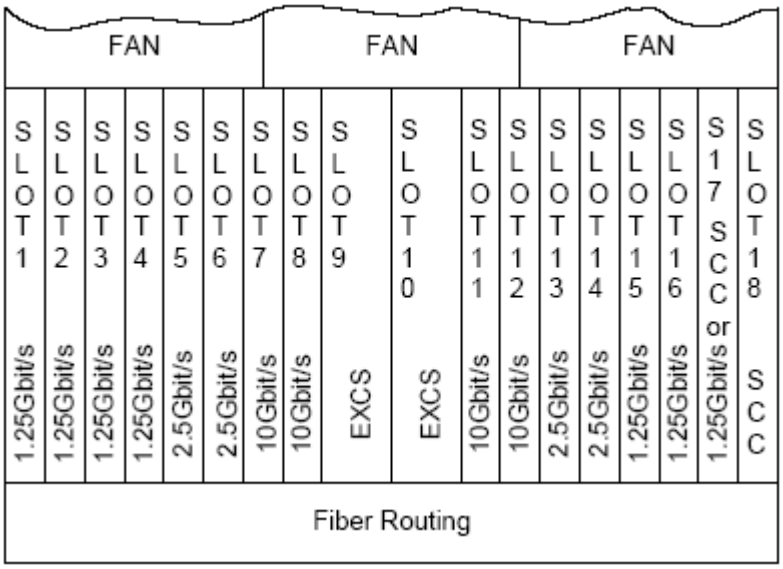


Fig. 4-7.- esquema de acceso en chasis inferior

4.3.1.2. Características técnicas de los equipos pasivos

Los conectores utilizados son de tipo FC con pulido PC de acuerdo a la normativa IEC 61754-13. Sus características deberán ajustarse a las determinadas en la siguiente tabla:

PROPIEDADES ÓPTICAS DE LOS CONECTORES FC/PC		
Parámetro	**Condiciones**	**Valor**
Pérdidas de inserción a 1.310 y 1.550 nm [dB]	IEC 60874-1	≤ 0,20 (valor típico) ≤ 0,50 (valor máximo)
Pérdidas de retorno a 1.310 y 1.550 nm [dB]	IEC 60874-1	≥ 45,0

Tabla 4.1.- Propiedades ópticas de los conectores FC

Parámetro	Condición	Valor
Tracción. Incremento de las pérdidas de inserción a 1.550 nm [dB]	IEC 60874-1 Tensión: 70 N (tensión máxima aplicada en 15 s) Punto de aplicación: 500 mm desde el conector Duración: 1 minuto Ancho de banda del detector: 0-1.500 Hz	≤ 0,50 (durante el test) ≤ 0,20 (tras el test)
Tracción. Incremento de las pérdidas de retorno a 1.310 y 1.550 nm [dB]	IEC 60874-1 Tensión: 70 N (tensión máxima aplicada en 15 s) Punto de aplicación: 500 mm desde el conector Duración: 1 minuto	≤ 5,0 (durante y tras el test)
Ciclos de conexión – desconexión. Incremento de las pérdidas de inserción a 1.310 y 1.550 nm [dB]	IEC 60874-1 500 ciclos	≤ 0,30 (durante el test) ≤ 0,20 (tras el test)
Ciclos de conexión – desconexión. Pérdidas de retorno a 1.310 y 1.550 nm tras el test [dB]	IEC 60874-1 500 ciclos	≥ 45

Tabla 4.2.- Propiedades mecánicas de los conectores FC

PROPIEDADES AMBIENTALES DE LOS CONECTORES FC/PC		
Parámetro	**Condición**	**Valor**
Temperatura de almacenamiento [ºC]		-30 a +60
Temperatura de operación [ºC]		-5 a +45
Máxima humedad relativa soportada en almacenamiento [%]		≥ 93
Ciclos térmicos. Incremento de las pérdidas de inserción a 1.310 y 1.550 nm [dB]	IEC 60874-1, IEC 60068-2-14 Temperatura mínima: (-40±2) ºC Temperatura máxima: (+70±2) ºC Número de ciclos: 20 Tiempo de aplicación: 2 horas Tiempo de transición: 2 horas	≤ 0,30 (durante el test) ≤ 0,20 (tras el test)
Ciclos térmicos. Incremento de las pérdidas de retorno a 1.310 y 1.550 nm [dB]	IEC 60874-1, IEC 60068-2-14 Temperatura mínima: (-40±2) ºC Temperatura máxima: (+70±2) ºC Número de ciclos: 20 Tiempo de aplicación: 2 horas Tiempo de transición: 2 horas	≤ 5,0 (durante y tras el test)
Ciclos térmicos con condensación. Incremento de las pérdidas de inserción a 1.310 y 1.550 nm [dB]	IEC 60874-1, IEC 60068-2-38 Total de ciclos: 10, alternando ciclos B y A *Ciclo A:* Temperatura mínima: (+25±2) ºC Temperatura máxima: (+65±2) ºC Humedad relativa: (93±3) % Duración: 24 horas *Ciclo B:* Temperatura mínima: (-10±2) ºC Temperatura máxima: (+65±2) ºC Humedad relativa: (93±3) % Duración: 24 horas	≤ 0,30 (durante el test) ≤ 0,20 (tras el test)

Tabla. 4.3.- Propiedades ambientales de los conectores FC

Cajas de empalmes

Para proteger los empalmes de humedad y suciedad, estos se alojaran en cajas de empalmes montadas en arquetas. En el interior de las cajas de empalmes se encuentran las bandejas de empalmes con organizadores para distribuir las fibras fusionadas y espacio para situar la reserva de fibra desnuda. Muy importante acotar que las fibras organizadas en las bandejas deberán de estar debidamente identificadas.

El cable de fibra se mantendrá sujeto mediante los elementos de tracción de los cables al soporte de la caja. Las cajas de empalmes se instalaran en las arquetas, situándose en el lugar más alto posible para pretejerlas de las posibles inundaciones de las arquetas.

Las cajas de empalmes deberán estar debidamente identificadas

Fig. 4-8.- Caja de empalme situada en arqueta

Paneles de conexión o Distribuidores de fibras ODF.

Se utilizara paneles de conexión o distribuidores ópticos, instalados en rack de 2.2 mts, para fibra óptica tanto en el punto de regeneración como en los extremos de la instalación del tendido de fibra óptica. Quito , Guayaquil, Cuenca.

La utilización de los paneles de conexión facilitara la organización de las fibras y la conexión con los sistemas de transmisión y recepción que se instalaran posteriormente.

Los empalmes quedaran pretejidos en una bandeja de empalmes tipo rack, los conectores estarán organizados en la parte frontal de la bandeja, de forma que sean fácilmente identificables.

La entrada de las fibras se realiza por la parte trasera de la bandeja. El ordenamiento de las fibras y los empalmes se lleva a cabo sobre la unidad organizadora, los cuáles puede alojar los protectores de empalme. La cantidad de fibra que se puede almacenar en la unidad organizadora varía dependiendo del nº de vueltas de diferente radio que se dé a la fibra. El radio mínimo de curvatura de la fibra óptica está limitado, en cualquier parte de la unidad organizadora, a 35 mm, asegurándose la buena transmisión a 1550 mm para las fibras ópticas monomodo. El recorrido de la fibra por toda la bandeja está determinado por el diseño de la misma, facilitando las labores de instalación e imposibilitando al operario una mala organización de la fibra en el interior de la bandeja. Cabe acotar que la unidad organizadora debe llevar una tapa de protección transparente.

Rack y Gabinetes utilizados

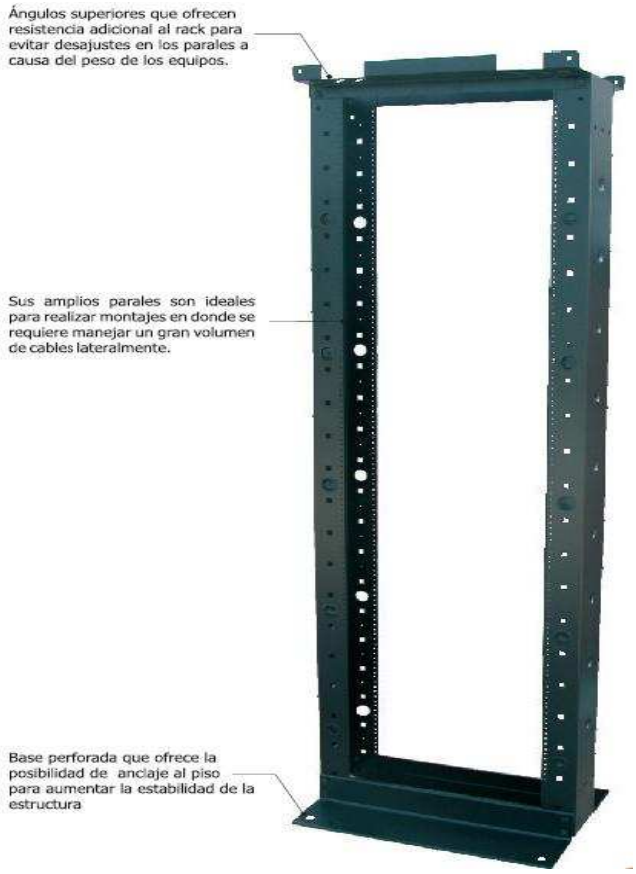


Fig. 4.9.- Modelo del Rack a Utilizar

4.3.1.2.1 Fibra óptica utilizada

Para este proyecto se ha escogido un cable de fibra denominado Headrow, este es un producto diseñado para soportar las condiciones más severas reduciendo notablemente los costes de los tendidos de fibra óptica.

Los componentes del minicable son:

Fig. 4.10.- Morfología del cable de fibra utilizada

Es un tipo de cable de fibras ópticas formado por uno o varios tubos en los que de forma holgada donde se alojan las fibras con un gel bloqueante del agua y taponante. Sobre esta composición un

tubo de aluminio que asegura alta protección al cable frente a las agresiones más diversas. Y finalmente una cubierta exterior que proporciona una superficie de alta deslizabilidad para su instalación en conductos

El cable Headrow está concebido para poder instalarse directamente enterrado, en entornos agresivos como industrias, cloacas, canalizaciones de agua, cruces de ríos, cortas y largas distancias.

Las grandes ventajas del cable Headrow

- Utilizar cable Headrow supone instalaciones de alta calidad con un notable ahorro de costes (Aprox. 1/3 respecto a las obras tradicionales) por los siguientes motivos:
- Zanjado menos profundo por su elevada resistencia al aplastamiento (tres veces superior a cables con armadura de acero corrugado).
- Elevada hermeticidad: el tubo de aluminio extruido es la mejor barrera frente a la penetración radial del agua. Los cables dieléctricos o los de acero corrugado estándar no presentan los niveles de estanqueidad del Headrow.

Sistemas de instalación más simples y económicos debido a.

- Elevada resistencia mecánica del cable
- Diámetro hasta el 30% inferior a los cables con fleje de acero corrugado
- Flexibilidad: similar a otros cables con armadura metálica
- Alta deslizabilidad en conductos
- Fácil cortado del tubo de aluminio
- Resistencia al ataque de roedores
- Menor coste de mantenimiento

- Utilizable en todo tipo de instalaciones de exterior de corta y largas distancias incluso en entornos agresivos (industrias, cloacas, cruces de ríos, paralelo a canalizaciones de agua, gaseoductos u oleoductos, torrentes, puertos marítimos, entornos con maquinaria pesada móvil, autopistas, túneles.

El minicable Headrow contiene 48 fibras ópticas es del tipo monomodo y en la siguiente tabla se especifican las propiedades.

PROPIEDADES GENERALES DEL MINICABLE	
Parámetro	**Valor**
Diámetro [mm]	2,4 3,0
Radio de curvatura [mm]	≤ 30,0
Tracción máxima [N]	≥ 70

Tabla 4.4.- Propiedades Generales del minicable

PROPIEDADES ÓPTICAS DE LA FIBRA MONOMODO ESTÁNDAR		
Parámetro	**Condiciones**	**Valor**
Diámetro del campo modal [μm]	λ = 1.310 nm	9,1 ± 0,5
	λ = 1.550 nm	10,2 ± 1,0
Coeficiente de atenuación [dB/Km]	λ = 1.310 nm	≤ 0,40
	λ = 1.550 nm	≤ 0,27
Variación de la atenuación a 1.310 y 1.550 nm al enrollar en mandril [dB]	75 vueltas, 75 mm de diámetro	≤ 0,10

Tabla 4.5.- Propiedades ópticas de la fibra

PROPIEDADES GEOMÉTRICAS DE LA FIBRA MONOMODO	
Parámetro	**Valor**
Diámetro del revestimiento [μm]	125 ± 1,0
Diámetro del recubrimiento primario [μm]	242 ± 7,0

Tabla 4.6.- Propiedades geométricas de la fibra monomodo

PROPIEDADES MECÁNICAS DE LA FIBRA MONOMODO	
Parámetro	**Valor**
Tensión de carga de prueba [kpsi]	≥ 100 (0,7 GN/m²)
Resistencia a la fatiga	≥ 20

Tabla 4.7.- Propiedades mecánicas de la fibra monomodo

4.3.2. Características de Alimentación de Potencia

El Cuarto de equipos debe tener alimentación eléctrica de la compañía de distribución y adicionalmente generadores de energía (es recomendable que los generadores de energía no se encuentren en el mismo piso que el cuarto), estas distribuciones deben ir directamente al cuadro de alimentación eléctrica para el cuarto de equipo, del otro lado debe estar conectado a UPS's donde en condiciones normales el voltaje alterno de la Red, rica en fluctuaciones, entra al rectificador /cargador donde es convertida para CC y usada para accionar el inversor para cargar y mantener la fluctuación en un banco de acumuladores eléctricos, el inversor convierte el voltaje de CC en AC modula su forma de onda y regula su voltaje la cual es entregada a la carga critica.

Es importante poseer un tablero principal de alimentación con 2 breaker de 50 Am. Y un Tablero de distribución con breaker de 32 Am. o 20 Am.

Fig. 4.11.- Tablero Principal de alimentación y tablero de distribución

El banco de baterías normalmente queda en fluctuación, la cual no absorbe ni genera energía. Pero en caso de falla de energía, el banco de baterías pasa a dar la corriente solicitada por el inversor y la carga critica continua a ser alimentada por un lapso de tiempo dependiendo de la capacidad del(los) UPS's hasta que los generadores alternos de energía se activen.

Para dar servicios al cuarto eléctrico de la caseta deberá crearse una acometida desde la línea de tensión. Deberá ejecutarse una canalización formada por un conducto de PVC de 160 mm de diámetro por el cual deberán tenderse los conductores de 50 mm2 de sección de aluminio desde el centro de transformación hasta el armario de protección que se instalara en el exterior de la caseta

4.3.3. Protecciones

Protección

- Se debe instalar protección contra voltajes inducidos por líneas de energía de alta tensión y por líneas de energía de corriente alterna, en caso de cortos circuitos, de conformidad con las normas existentes.
- La protección de los cables de alimentación se debe realizar con funda sellada BX, para disminuir riesgos por ejemplo cortocircuitos.
- Se deben de instalar todas las protecciones de sobrecorrientes y mala calidad de la energía, que pueden presentarse como fluctuaciones y cortes bruscos de energía, por tal motivo es importante la colocación de un UPS que regule y atenúe estos problemas.
- El sistema puesta a tierra debe estar en el orden de 0 hasta 3 ohm. El sistema se detalla en le siguiente literal.

4.3.3.1. Sistema puesta a tierra

Todas las partes de las instalaciones eléctricas, deben ser proyectadas e ejecutadas de modo que sea posible prevenir por medios seguros, los peligros de choques eléctricos y todos los otros tipos de accidentes. El conductor de tierra debe ser una malla unipolar, sin ninguna derivación.

Todas las partes de las instalaciones eléctricas sujetas a acumulación de electricidad estática deben ponerse a tierra.

Los gabinetes interconectados por cables de datos, necesitan tener sus tierras lógicas también conectadas.

Si por algún motivo cualquier gabinete quede en un potencial de tierra diferente a los demás, comenzara a circular corriente por los circuitos de tierra, esta diferencia de potencial entre los gabinetes no necesita ser grande para causar la circulación de grandes corrientes. Como la impedancia de los circuitos de aterramiento es en la orden de los mili-ohms, cualquier diferencia de potencial en el orden de milivoltios causara una circulación de corriente en el orden de Amperes.

Este aterramiento debe ser el básico y su resistencia no debe superar a 5 ohms. En caso de superar los 5 ohms deben hacerse otros puntos de aterramiento hasta bajar la resistencia de tierra, estos puntos de aterramiento deben ser efectuados en cámaras de cemento para su verificación futura.

Aterramiento en punto único

El sistema de tierra debe tener como origen un único punto, este punto único es una placa de cobre instalada por lo general en la pared y debe estar conectado directamente a la malla aislada de tierra, unidos a esta placa deben estar todos los cables de tierra de cada equipo, uno de los principales motivos por el cual es necesario que la malla de tierra de alimentación en el cuadro tenga un único punto de conexión con tierra es el de facilitar el mantenimiento correctivo.

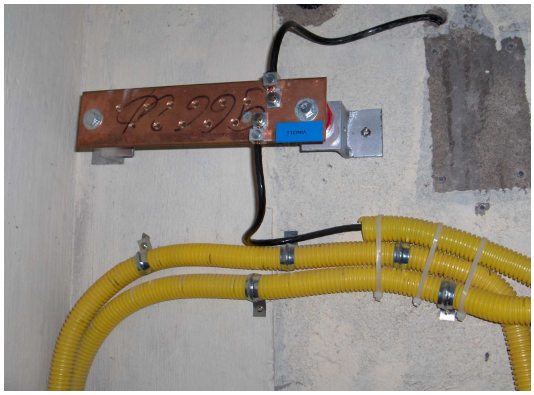


Fig. 4.12.- Modelo de un punto único de Tierra

Malla a tierra

La malla a tierra estará formada por 4 varillas de cobres de 2 mts de longitud, que se deben enterrar a una distancia de 2 mts entre ellas y unidas mediante un cable de cobre 2/0. Esta unión Cable – Varilla se la debe realizar con soldadura exotérmica de alto punto de fusión mediante moldes que utilizan oxido de cobre (CU_2O), oxido de aluminio (AL_2O_3) y pólvora que genera una pequeña explosión dejando como resultado un solo cuerpo entre varilla y cable

Es recomendable que en los huecos donde se enterraran las varillas se coloquen soluciones salinas, gracias a estas soluciones salinas se mejora la conectividad de tierra.

4.3.4 Equipos de climatización

La sala de un cuarto de equipos requiere de un sistema de aire acondicionado capaz de mantener las especificaciones básicas del ambiente.

El sistema de aire acondicionado en la sala debe ser dedicado, totalmente independiente de cualquier otro sistema, no debe tener ambientes compartidos con otros cuartos. Debe tener capacidad de filtrar, enfriar, calentar, humidificar y des humidificar el aire, montado de tal forma que sea incapaz de producir vibraciones.

Las especificaciones del ambiente son generales básicas.

- Temperatura: 18-24 C (21 C Nominal)
- Variación máxima de temperatura: 3 C/ hora
- Humedad relativa: 40 a 60% (50% nominal)
- Variación máxima de humedad: 6 % / hora
- Compensación de altura Todos las especificaciones referentes a la temperatura deben ser reducidas de 1 grado centígrado por cada 1000 mt. de altitud.

La dirección del flujo del aire debe ser mayor parte los equipos de red y es recomendable que sea de abajo para arriba, por lo que son mejor refrigerados cuando usan la inyección del aire acondicionado por el piso falso. El retorno del aire caliente por el techo permite que el calor generado por los equipos sea absorbido.

Ventilación y aire externo

Para que exista presión positiva y para que el aire no se torne viciado, una cierta cantidad de aire externo es necesario inyectarlo a la sala del cuarto de equipos.. Por otro lado es aconsejable el uso

de cortinas de aire instaladas en la puerta de acceso al cuarto, para evitar fugas de aire y eliminar impurezas transportadas por las personas en el momento del ingreso.

4.4 Cálculos

Después de haberse realizado el estudio de cuantos kilómetros tienen las tres rutas, cuantos empalmes se van a utilizar, y en que ventana óptica se va a trabajar, se realiza el cálculo de cada sub. - ruta tomándose en consideración las perdidas en cada empalme, conectores y la atenuación de la fibra por kilómetros, la suma de todo esto da como resultado la perdidas de la potencia de luz en la fibra óptica que es importante en el diseño; ya que con estos valores podemos dimensionar los equipos, el cable de fibra, y demás accesorios que se utilizan según los requerimientos del sistema.

Para poder saber si el equipo ADM esta bien dimensionado es importante considerar sus características de Potencia máxima transmitida, potencia mínima de transmisión, potencia mínima de recepción. Se deben conocer las características de la fibra óptica con respecto a las perdidas por kilómetros que se tiene y las perdidas por empalmes y las perdidas por acople con los conectores.

4.4.1 Cálculos de Atenuación y Determinación del número de repetidores

DATOS:

- ✓ **Longitud del cable de fibra por bobina** n = 4 Km.
- ✓ **Potencia del Transmisor** 09= 3 dB
- ✓ **Potencia mínima del Receptor** P_{mr} . = - 28 dB
- ✓ **Perdida en la fibra / Km**. α1 = 0.19 Km.
- ✓ **Perdidas en cada empalme.** α2 = 0.2 dB

✓ **Perdida en los conectores** α3= 0.25 dB

La Formula de las perdidas esta dada por.

$$\text{Per} = \sum_{n=1}^{m} (\alpha 1 \times L_n) + (\alpha 2 \times E) + (\alpha 3 \times C)$$

Potencia Promedio de transmisión

$$P_{pro} = \frac{P_{\max} + P_{\min}}{2}$$

Formula de Potencia Recibida en el receptor

$$P_r = P_{pro} - Per$$

TRAMO QUITO - GUAYAQUIL

- **Sub-tramo Quito – Aloag**

  Perdidas en el sub.-tramo

  $\text{Per} = (0.19 \times 65) + (0.25 \times 17) + (0.25 \times 2)$

  Per = 16.**38 dB**

  Potencia recibida en el receptor

  P_r = P_{pro} - Per

  P_r = 0.5 – 15.65

  P_r = - 15.88 dB

Conclusión: Comparamos P_r = -15.88 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM.

- **Sub.-tramo Aloag – Tandapi**

  Perdidas en el sub.-tramo

  Per = $(0.19\times 47)+(0.25\times 12)+(0.25\times 2)$

  Per = 11.92 dB

  Potencia recibida en el receptor

  P_r = P_{pro} - Per

  P_r = 0.5 – 11.92

  P_r = - 11.42 dB

Conclusión: Comparamos P_r = - 11.42 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM.

- **Sub.-tramo Tandapi – Santo Domingo**

  Perdidas en el sub.-tramo

  Per = $(0.19\times 56)+(0.25\times 14)+(0.25\times 2)$

  Per = 14.052 dB

  Potencia recibida en el receptor

  P_r = P_{pro} - Per

  P_r = 0.5 – 14.052

  P_r = - 13.55 dB

Conclusión: Comparamos P_r = - 13.55 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM.

- **Sub.-tramo Santo Domingo – Quevedo**

  Perdidas en el sub.-tramo

  Per = $(0.19\times105)+(0.25\times27)+(0.25\times2)$

  Per = 26.06

  Potencia recibida en el receptor

  P_r = P_{pro} - Per

  P_r = 0.5 – 26.06

  P_r = - 25.56 dB

Conclusión: Comparamos P_r = - 25.56 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM.

- **Sub.-tramo Quevedo – Ventanas**

  Perdidas en el sub.-tramo

  Per = $(0.19\times65)+(0.25\times17)+(0.25\times2)$

  Per = 16.38

  Potencia recibida en el receptor

  P_r = P_{pro} - Per

  P_r = 0.5 – 16.38

  P_r = - 15.88 dB

Conclusión: Comparamos P_r = - 15.88 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM.

- **Sub-tramo Ventanas – Babahoyo**

  Perdidas en el sub.-tramo

  Per = $(0.19\times 50)+(0.25\times 13)+(0.25\times 2)$

  Per = 12.70

  Potencia recibida en el receptor

  P_r = P_{pro} - Per

  P_r = 0.5 – 12.70

  P_r = - 12.20 dB

Conclusión: Comparamos P_r = - 12.2. Comparamos la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM.

- **Sub-tramo Babahoyo – Milagro**

  Perdidas en el sub.-tramo

  Per = $(0.19\times 55)+(0.25\times 14)+(0.25\times 2)$

  Per = 13.86 dB

  Potencia recibida en el receptor

  P_r = P_{pro} - Per

  P_r = 0.5 – 13.86

  P_r = - 13.36 dB

Conclusión: Comparamos P_r = - 13.36 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM

- **Sub-tramo Milagro – Guayaquil**

Perdidas en el sub.-tramo

Per = $(0.19\times 62)+(0.25\times 16)+(0.25\times 2)$

Per = 15.604 dB

Potencia recibida en el receptor

P_r = P_{pro} - Per

P_r = 0.5 – 15.604

P_r = - 15.104 dB

Conclusión: Comparamos P_r = - 15.104 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM

TRAMO GUAYAQIL – CUENCA

- **Sub.-tramo Guayaquil – Naranjal**

Perdidas en el sub.-tramo

Per = $(0.19\times 58)+(0.25\times 15)+(0.25\times 2)$

Per = 14.64 dB

Potencia recibida en el receptor

P_r = P_{pro} - Per

P_r = 0.5 – 14.64

P_r = - 14.14 dB

Conclusión: Comparamos P_r = - 14.14 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM

- **Sub.-tramo Naranjal – Machala**

  Perdidas en el sub.-tramo

  Per = $(0.19\times 99)+(0.25\times 25)+(0.25\times 2)$

  Per = 24.508 dB

  Potencia recibida en el receptor

  P_r = P_{pro} - Per

  P_r = 0.5 – 24.508

  P_r = - 24.008 dB

Conclusión: Comparamos P_r = - 24.00 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM

- **Sub.-tramo Machala – Santa Isabel**

  Perdidas en el sub.-tramo

  Per = $(0.19\times 77)+(0.25\times 20)+(0.25\times 2)$

  Per = 19.3 dB

  Potencia recibida en el receptor

  P_r = P_{pro} - Per

  P_r = 0.5 – 19.3

  P_r = - 18.78 dB

Conclusión: Comparamos P_r = - 18.78 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM

- **Sub.-tramo Santa Isabel - Cuenca**

Perdidas en el sub.-tramo

Per = $(0.19\times 70)+(0.25\times 18)+(0.25\times 2)$

Per = 17.54 dB

Potencia recibida en el receptor

P_r = P_{pro} - Per

P_r = 0.5 – 17.54

P_r = - 17.04 dB

Conclusión: Comparamos P_r = - 17.04 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM

RUTA CUENCA – QUITO

- **Sub.-tramo Cuenca – Zhud**

Perdidas en el sub.-tramo

Per = $(0.19\times 93)+(0.25\times 24)+(0.25\times 2)$

Per = 23.16 dB

Potencia recibida en el receptor

P_r = P_{pro} - Per

P_r = 0.5 – 23.16

P_r = - 22.65 dB

Conclusión: Comparamos P_r = - 22.65 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM

- **Sub.-tramo Zhud– Alausí**

Perdidas en el sub.-tramo

Per = $(0.19\times58)+(0.25\times15)+(0.25\times2)$

Per = 14.63 dB

Potencia recibida en el receptor

P_r = P_{pro} - Per

P_r = 0.5 – 14.63

P_r = - 14.13 dB

Conclusión: Comparamos P_r = - 14.13 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM

- **Sub.-tramo Alausí - Riobamba**

Perdidas en el sub.-tramo

Per = $(0.19\times81)+(0.25\times21)+(0.25\times2)$

Per = 20.25 dB

Potencia recibida en el receptor

P_r = P_{pro} - Per

P_r = 0.5 – 20.25

P_r = - 19.75 dB

Conclusión: Comparamos P_r = - 19.75 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM

- **Sub.-tramo Riobamba – Ambato**

Perdidas en el sub.-tramo

Per = $(0.19\times 63)+(0.25\times 16)+(0.25\times 2)$

Per = 15.80 dB

Potencia recibida en el receptor

P_r = P_{pro} - Per

P_r = 0.5 – 15.80

P_r = - 15.30 dB

Conclusión: Comparamos P_r = - 15.30 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM

- **Subtramo Ambato – Latacunga**

Perdidas en el sub.-tramo

Per = $(0.19\times 95)+(0.25\times 24)+(0.25\times 2)$

Per = 23.54 dB

Potencia recibida en el receptor

P_r = P_{pro} - Per

P_r = 0.5 – 23.54

P_r = - 23.04 dB

Conclusión: Comparamos P_r = - 23.04 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM

- **Subtramo Latacunga – Quito**

Perdidas en el sub.-tramo

Per = $(0.19\times 90)+(0.25\times 23)+(0.25\times 2)$

Per = 22.38 dB

Potencia recibida en el receptor

P_r = P_{pro} - Per

P_r = 0.5 – 22.38

P_r = - 21.88 dB

Conclusión: Comparamos P_r = - 21.88 con la Potencia mínima de recepción. P_{mr} = -28 y estamos dentro de las potencias aceptadas por el Equipo ADM

Cálculo de Potencia Enlaces Interurbanos Ventana 1550 nm							Presupuesto Óptico 1550 nm						
Tramo	Distancia (Km)	Numero de Empalmes	Perdidas en la fibra (dB)	Perdidas en ODF's y patchords (dB)	Perdidas en empalmes (dB)	Atenua. del trayecto (dB)	Potencia TX max	Potencia TX Min	Potencia de Salida promedio	Sensibilidad Receptor STM-1	Nivel Rx en el MUX HUAWEI	Margen (dB)	conclusión
Guayaquil - Naranjal	**58.00**	15	-11.136	-0.5	-3	**-14.63**	3	-2	0.5	-28	-14.13	13.86	No repetidor
Naranjal - Machala	**99.00**	25	-19.008	-0.5	-5	**-24.50**	3	-2	0.5	-28	-24.00	3.99	No repetidor
Machala - Santa Isabel	**77.00**	20	-14.784	-0.5	-4	**-19.28**	3	-2	0.5	-28	-18.78	9.21	No repetidor
Santa Isabel - Cuenca	**70.00**	18	-13.44	-0.5	-3.6	**-17.54**	3	-2	0.5	-28	-17.04	10.9	No repetidor
Cuenca - Zhud	**93.00**	24	-17.856	-0.5	-4.8	**-23.15**	3	-2	0.5	-28	-22.65	5.34	No repetidor
Zhud - Alausí	**58.00**	15	-11.136	-0.5	-3	**-14.63**	3	-2	0.5	-28	-14.13	13.86	No repetidor
Alausí - Riobamba	**81.00**	21	-15.552	-0.5	-4.2	**-20.25**	3	-2	0.5	-28	-19.75	8.24	No repetidor
Riobamba - Ambato	**63.00**	16	-12.096	-0.5	-3.2	**-15.79**	3	-2	0.5	-28	-15.29	12.70	No repetidor
Amabato - Latacunga	**95.00**	24	-18.24	-0.5	-4.8	**-23.54**	3	-2	0.5	-28	-23.04	4.96	No repetidor
Latacunga - Quito	**90.00**	23	-17.28	-0.5	-4.6	**-22.38**	3	-2	0.5	-28	-21.88	6.12	No repetidor
Quito - Aloag	**65.00**	17	-12.48	-0.5	-3.4	**-16.38**	3	-2	0.5	-28	-15.88	12.12	No repetidor
Aloag - Tandapi	**47.00**	12	-9.024	-0.5	-2.4	**-11.92**	3	-2	0.5	-28	-11.42	16.57	No repetidor
Tandapi - Santo Domingo	**56.00**	14	-10.752	-0.5	-2.8	**-14.05**	3	-2	0.5	-28	-13.55	14.44	No repetidor
Santo Domingo - Quevedo	**105**	27	-20.16	-0.5	-5.4	**-26.06**	3	-2	0.5	-28	-25.56	2.44	No repetidor
Quevedo - Ventanas	**65.00**	17	-12.48	-0.5	-3.4	**-16.38**	3	-2	0.5	-28	-15.88	12.12	No repetidor
Ventanas- Babahoyo	**50.00**	13	-9.6	-0.5	-2.6	**-12.70**	3	-2	0.5	-28	-12.2	15.8	No repetidor
Babahoyo - Milagro	**55.00**	14	-10.56	-0.5	-2.8	**-13.86**	3	-2	0.5	-28	-13.36	14.64	No repetidor
Milagro - Guayaquil	**62.00**	16	-11.904	-0.5	-3.2	**-15.60**	3	-2	0.5	-28	-15.10	12.89	No repetidor

Tabla. 4.8.- Resultados de los Cálculos de Perdidas

4.5. Instalación y tendido de la fibra óptica

Para la instalación de la fibra nos basamos en la recomendación UIT-T L.49. En esta Recomendación se describe la técnica con microzanjas, que permite instalar cables subterráneos en pequeñas ranuras a una profundidad reducida. Las ventajas de esta técnica con relación a las tecnologías convencionales de tendido de cables estriban esencialmente en su mayor velocidad de ejecución, bajo costo, repercusión ambiental significativamente baja y una interrupción limitada del tráfico en los caminos, y como consecuencia, se expedita la obtención de los permisos para trabajar en zonas públicas o carreteras concesionadas.

El cable se puede instalar manualmente en la microzanja, depositándolo en el fondo de la ranura gradualmente desde el carrete y con la ayuda de la carretilla de éste. Aunque se permiten los cambios de dirección, se debe tener cuidado de no exceder los radios de curvatura mínimos especificados para el cable.

Esta técnica involucra una sencillez en la instalación de la fibra:

1. Con la maquinaria se procede a realizar la ranura a lo largo de la ruta

Fig. 4.13 Maquina para microzanjado

Fig. 4.14 Cierras de la maquina

Las microzanjas constituyen una nueva y ventajosa técnica de construcción para canalizaciones de cables ópticos en carreteras.

- Se trata de canalizaciones de tamaño muy reducido que se construyen sobre asfalto u hormigón de manera rápida y económica
- Su anchura puede variar entre 10 y 15 mm.
- Su profundidad puede variar entre 10 y 25 cm.
- Admiten diversas arquitecturas y permiten incorporar:

  a.- uno o varios cables de fibra óptica directamente enterrados

  b.- Uno o varios microductos vacíos disponibles para tender posteriormente fibra mediante técnicas de soplado.

Fig. 4.15 Tendido de fibra tradicional

Fig. 4.16 Tendido de Microducto

En la Figura observamos un tendido de cable subterráneo tradicional que a mas de ser muy costosa, causa muchas molestias a la vías y pueden afectar a otros servicios, mientras que en la fig. se observa un tendido por microcables ocasionan este tipo de molestias.

2. Se procede a realizar la limpieza de la microzanjas

Después de realizar el corte de la ranura se deben llevar a cabo las siguientes operaciones

- limpiar la ranura con agua a presión;
- secar la ranura utilizando aire comprimido;
- secar nuevamente la ranura (por ejemplo, calcinar) con aire caliente empleando una caña de soplar apropiada

Fig. 4.17 Limpieza de la microzanja

3. Luego de que la microzanja este en las condiciones adecuadas se procede a realizar el tendido del Microcable. El tendido ira desde una arqueta hasta la siguiente

Fig. 4.18 Ejemplo de colocación del cable de fibras en la microzanja

Fig. 4.19 Cable de fibras en la microzanja

4. Después de que se ha instalado el cable, se debe cerrar la ranura con asfalto liquido caliente

Fig. 4.20 sellado de la microzanja con asfalto liquido

Para garantizar que el asfalto se adhiere a los costados de las paredes de la ranura y crea un sello efectivo, primero se aplicará un agente ligador líquido (base) a toda la trayectoria y a los costados de la ranura.

El asfalto líquido se aplicará utilizando una boquilla de tamaño apropiado. Esta operación se debe ejecutar de tal manera que se asegure que la ranura se llena uniformemente hasta el nivel de la superficie del camino (por ejemplo, mediante dos pasadas consecutivas).

Tras seguir los pasos descritos, no habrá ejes disparejos, ni desniveles o irregularidades a lo largo de la ranura del cable resultantes del recubrimiento con el asfalto líquido (esto se podrá confirmar, por ejemplo, mediante un dispositivo sobre ruedas). Se deben mantener esas condiciones por un largo periodo de tiempo.

Arquetas

Las arquetas son las cajas que se utilizaran para proteger los empalmes que se realicen a lo largo del tendido del cable. Se tiene programado que necesitaremos una de estas arquetas cada 4 Km. Ya que las bobinas se comercializan con 4 Km. de fibras. La localización de las arquetas será a los costados de la carretera y se deberá buscar prioritariamente lugares de no circulación de automóviles. Se recomienda que las arquetas sean plásticas y con tapas de fundición.

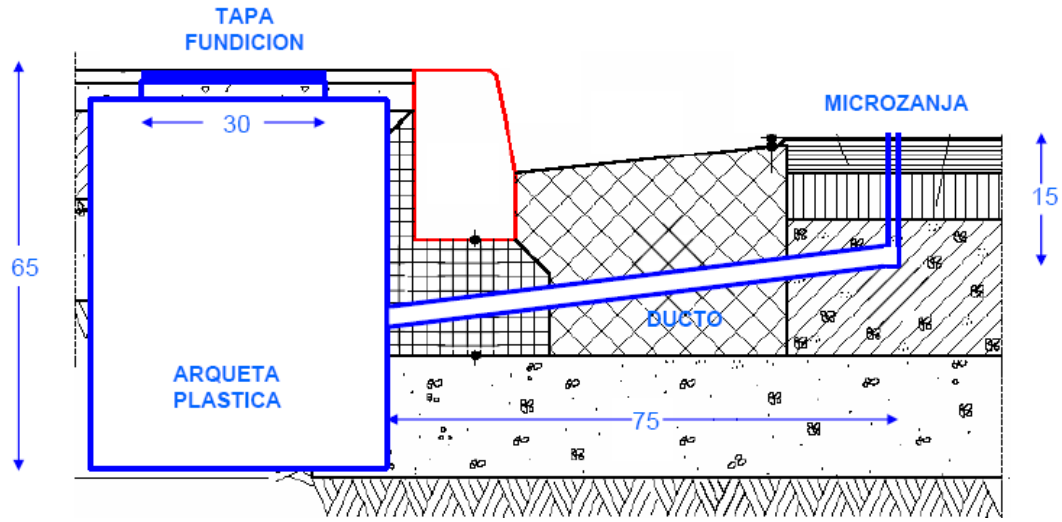


Fig. 4.21 Modelo para Arquetas que alojaran las cajas de empalmes

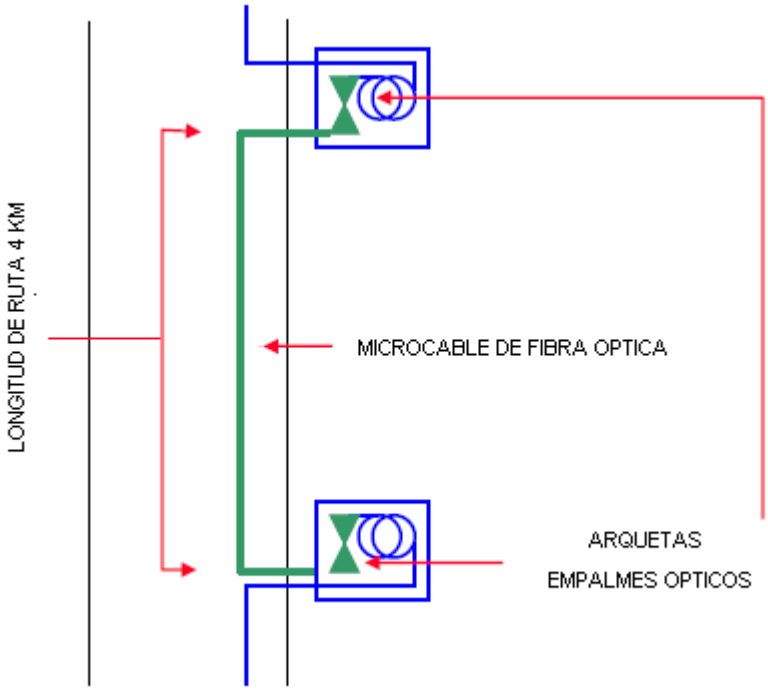


Fig. 4.22 Diagrama de localización de arquetas

Fig. 4.23 Tapa de Fundición de arquetas

4.5.1. Requisitos de Instalación

La tecnología de microzanjas se aplica en rutas con superficies de rodamiento asfaltadas como caminos o banquetas con una base de material compactado (asfalto u hormigón). Sus ventajas con relación a las tecnologías convencionales de tendido de cables estriban esencialmente en una

mayor velocidad de ejecución, una reducción importante de los costos de despliegue de la infraestructura, y un efecto ambiental sobre el tráfico en los caminos mucho menor.

Debido a las reducidas profundidades que se utilizan en las técnicas de microzanjas, no existe protección contra posibles daños causados por los trabajos de reparación de los caminos. Por consiguiente, es muy importante que se planifiquen cuidadosamente las rutas en las que se utilizan esas técnicas a fin de poder asegurar una estabilidad a largo plazo en las mismas. Normalmente, la microzanja se excava cortando una ranura en el asfalto a poca profundidad (máximo de 7 cm), pero sin penetrar toda la capa de asfalto. Se debe tener precaución de no cortar totalmente el asfalto, ya que esto podría provocar que se fracture o divida el pavimento a los lados de la ranura.

Se debe mantener en mente esta precaución particularmente en aquellos casos cuando no haya protección lateral, que podría evitar que la capa de asfalto se mueva, en uno o ambos lados de la ranura y sobre todo cuando la microzanja se construye a lo largo del borde de un camino sin berma o banqueta. En esos casos, la ranura se localizará normalmente a una distancia apropiada (por ejemplo, al menos un metro) del borde del camino.

El ancho de la ranura puede variar (por ejemplo, 10-15 mm) de conformidad con el diámetro del cable que se va a tender. El cable debe cumplir estrictamente con los requisitos de resistencia a la presión vehicular y, en particular, resistencia a la temperatura, necesaria cuando se sella el cable en la ranura con asfalto caliente. La temperatura del asfalto durante la operación de sellado puede variar entre 100º C y 170º C.

Es preferible que las fibras ópticas se introduzcan en un tubo metálico (por ejemplo cobre) relleno con un compuesto apropiado y revestido de una cubierta de polietileno (PE). Actualmente se

utilizan distintos tipos de cable, que contienen distintos números de fibras y con distintos diámetros exteriores. El cable se puede fabricar y suministrar en tramos largos; sin embargo, en las redes urbanas a menudo es conveniente utilizar tramos cortos o concordantes, particularmente para los cruces bajo los caminos o las vías férreas.

Cuando se realicen los empalmes se deben utilizar cajas apropiadas para unir o bifurcar el cable. Estos accesorios se instalan al nivel de la superficie del camino o banqueta y dispondrán de una cubierta muy resistente (que soporte el paso de vehículos). Estas cajas se deben instalar en orificios cortados en el asfalto con una barrena de diámetro apropiado para las dimensiones de la caja.

Al tender el cable, debe tenerse en cuenta si se va a instalar posteriormente la caja de empalme. En el sitio de instalación de la caja de empalme, se dejará una holgura en el cable que se tiende provisionalmente en ranuras prefabricadas debidamente cubiertas.

Cuando se instale la caja de empalme, primero se debe descubrir el cable y a continuación se debe perforar un orificio con una barrena si no se efectúo durante el tendido del cable. Después de la perforación del orificio, se debe insertar la caja de empalme provisionalmente para determinar las dimensiones de los extremos del cable que se han de desnudar. Para garantizar la colocación correcta, se determinará la profundidad del orificio en base a la altura de la caja de empalme. Una vez concluidas las operaciones de empalme, la caja se asegurará y sellará con asfalto líquido. Se debe garantizar la hermeticidad al aire y al agua utilizando accesorios apropiados (por ejemplo, tubos termorretractables) en el exterior de todas las toberas por las que pasa el cable. Cuando el cable instalado en la microzanja deba unirse con un cable instalado convencionalmente utilizando una caja de empalme existente no instalada al nivel de la superficie, se utilizarán accesorios

apropiados a fin de garantizar un sellado neumático efectivo en los orificios de entrada de la caja de empalmes

4.5.2 Protección del cable de fibra

Se debe instalar sobre el cable una tira de retención [por ejemplo, una tira de polietileno (PE, *polyethylene*) ensanchada], para fijarlo en su lugar dentro de la ranura. La tira de retención se cubrirá a su vez con materiales de relleno altamente repelentes al agua (por ejemplo una tira de hule) cuya dimensión será ligeramente mayor que la sección transversal de la ranura. Cada tira se fijará en su sitio utilizando un rodillo apropiado. Además de asegurar el cable al fondo de la ranura, la función principal de estos materiales de relleno es proteger mecánicamente al cable. La tira de hule proporciona además protección térmica.

Después de que se han instalado el cable y las tiras protectoras, se debe cerrar la ranura con asfalto líquido caliente. Para garantizar que el asfalto se adhiere a los costados de las paredes de la ranura y crea un sello efectivo, primero se aplicará un agente ligador líquido (base) a toda la trayectoria y a los costados de la ranura El asfalto líquido se aplicará utilizando una boquilla de tamaño apropiado. Esta operación se debe ejecutar de tal manera que se asegure que la ranura se llena uniformemente hasta el nivel de la superficie del camino (por ejemplo, mediante dos pasadas consecutivas). Tras seguir los pasos descritos, no habrá ejes disparejos, ni desniveles o irregularidades a lo largo de la ranura del cable resultantes del recubrimiento con el asfalto líquido (esto se podrá confirmar, por ejemplo, mediante un dispositivo sobre ruedas). Se deben mantener esas condiciones por un largo periodo de tiempo.

Para asegurar que la ranura está correctamente rellenada y sellada, el material de base y el asfalto deben ser compatibles

4.5.3 Mantenimiento del cable

En caso de fallo del cable, será necesario reemplazar la sección donde se localizó el problema, instalando un nuevo cable. Una vez localizado el fallo, se removerá el asfalto de la ranura utilizando una herramienta apropiada (por ejemplo, un gancho) en una longitud de aproximadamente 3 m a ambos lados (véase la figura 2a). Después de retirar las tiras de protección, se debe cortar el cable antiguo y extraer una longitud suficiente de las fibras que se van a unir con las del nuevo cable. La unión de los dos cables se lleva a cabo utilizando dos cajas de empalme, que se instalarán en ambos extremos de la sección reparada (véanse la figura 4.24). Por lo que se refiere a la instalación de la caja de empalme y del nuevo cable véanse las

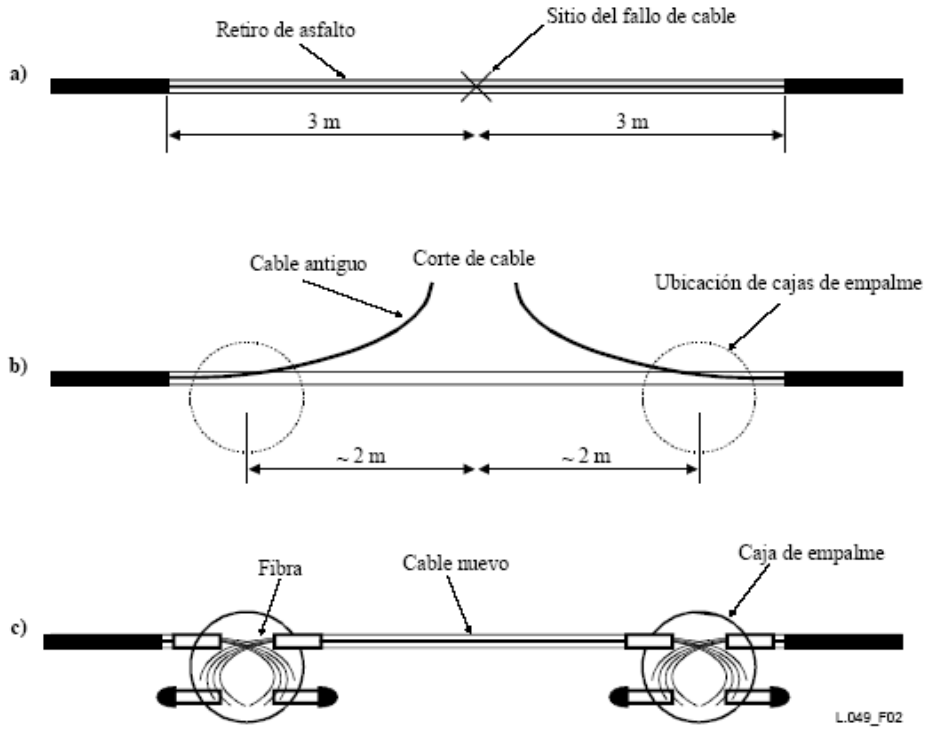


Fig. 4.24 Proceso para el cambio de fibra

4.5.4 Equipos Necesarios para la instalación

- Maquinas para realizar las microzanjas, con este método se pueden realizar tendidos de hasta 2 Km. por día, por lo que es importante no solo contar con un solo frente de trabajo sino con varios si se desea terminar a la brevedad
- Es muy importante contar con fusionadoras para la realización de los empalmes que se nos presentaran cada 4 Km
- Kit especializados para conectorizacion de las fibras.
- conectores, patch de fibras, bobina de fibra
- Accesorios indispensables para poder trabajar en clima adversos,.
- Adicionalmente se deben tener tarjetas de respaldos para los enlaces principales de fibra, para la capacidad suministrada y así tener siempre el respaldo a nivel de interfases ópticas.
- Todos los cuartos de Equipos deben contar con una bodega con equipos de respaldo por si se presentan daños en los que se utilizan a diario.

4.5.5 Normas y Estándares Internacionales

Para nuestro proyecto es muy importante considerar las normas y recomendaciones internacionales, estas ayudaran y nos guiaran de gran forma en el momento del levantamiento del sistema troncal.

UIT – T L.49: CONSTRUCCIÓN, INSTALACIÓN Y PROTECCIÓN DE LOS CABLES Y OTROS ELEMENTOS DE PLANTA EXTERIOR

- Técnica de instalación con microzanjas

UIT – T G52: SERIE G: SISTEMAS Y MEDIOS DE TRANSMISIÓN, SISTEMAS Y REDES DIGITALES

- Características de los medios de transmisión – Cables de fibra óptica**.**

EIA/TIA 607. SISTEMAS PUESTAS A TIERRA

- Define al sistema de tierra física y el de alimentación bajo las cuales se deberán de operar y Proteger los elementos del sistema estructurado.

ANSI/TIA/EIA-569-A: **RUTAS Y ESPACIOS DE TELECOMUNICACIONES PARA EDIFICIOS COMERCIALES**.

- Define La infraestructura del cableado de telecomunicaciones, a través de tubería, registros, pozos, trincheras, canal, entre otros, para su buen funcionamiento y desarrollo del futuro

CAPITULO V

Diseño de la red

Diseño Lógico de la Red basado en enrutamiento IP – MPLS

5.1 Criterios de Diseño

En este apartado se presenta la red en anillo que se esta diseñando introducido desde la perspectiva de los equipos de red. Como se puede apreciar, se logra un alto nivel de disponibilidad al lograr una redundancia de medio gracias al diseño en anillo del tendido de fibra óptica y como veremos más adelante una redundancia a nivel lógico de la red.

Las premisas básicas que nuestra red debe cumplir utilizados durante esta fase de diseño de nuestra red MPLS fueron los siguientes:

- ✓ Robustez
- ✓ Convergencia
- ✓ Flexibilidad de Servicios

Para el diseño de nuestra red de servicios basada en protocolo MPLS y a fin de procurar la consecución de las premisas planteadas, hemos divido la estructura lógica de nuestra red en 3 grandes áreas que se presenta en la siguiente figura (Fig. 5-1)

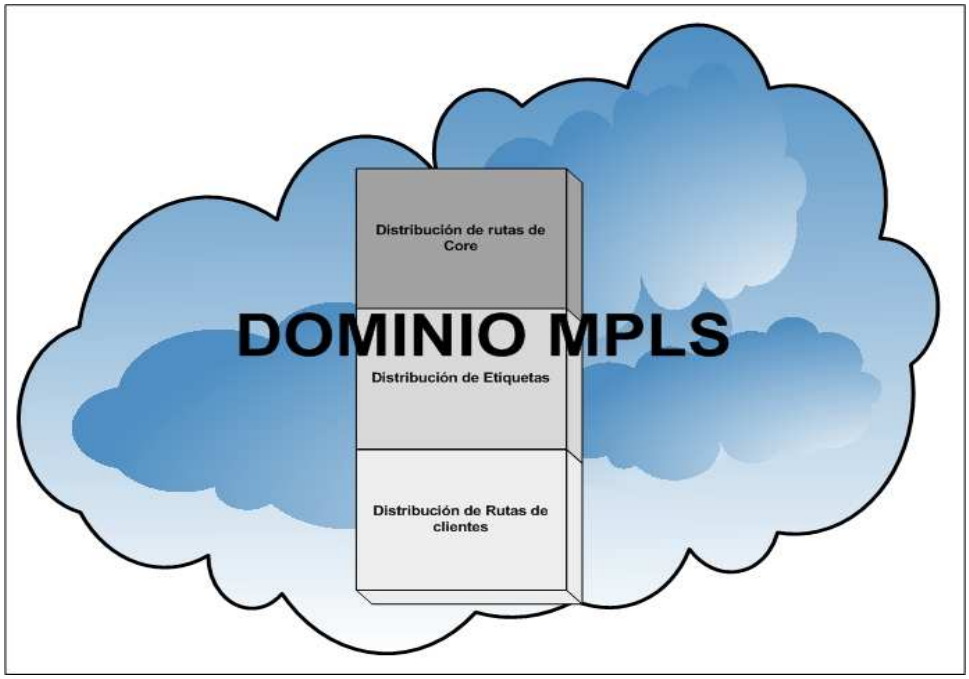


Fig. 5.1.- Estructura Red MPLS

Distribución de Rutas de Core:

Cuando se desarrollan redes de proveedores de servicios es de vital importancia el poder lograr una conectividad total permitiendo que todos se vean contra todos. Estas redes “Full Mesh” (malla completa) se logran implementando un protocolo de enrutamiento dinámico para que todos los routers miembros de la comunidad puedan aprender las redes de cada unos de sus vecinos.

¿Porque OSPF?

1.- Protocolo de estado enlace de gran difusión.

2.- Permite a futuro aplicaciones como Ingeniería de Tráfico.

3.- Protocolo robusto menos propenso a fallas. (Envío de información incorrecta)

4.- Protocolo de rápida convergencia.

Distribución de Etiquetas

Actualmente se cuentan con 2 opciones en cuanto al protocolo para la distribución de rutas, el LDP y el TDP. LDP es de estándar publicado por la IETF y ampliamente utilizado en el mercado mientras que el protocolo propietario de Cisco TDP encuentra restringido su ambiente de aplicación a equipos únicamente CISCO lo cual sin dudas representa una limitante seria.

En el presente trabajo, a pesar de que la red se desarrollará en un ambiente completamente CISCO, se ha optado por el uso del protocolo LDP por su carácter de estándar.

Distribución de las Rutas de Clientes

Sin este apartado, simplemente no tendría sentido tener como negocio una red de prestación de servicio de comunicaciones. Según la RFC 1918, se ha asignado bloques de IPs para que las empresas puedan utilizarlas para su direccionamiento privado. Que ocurre si algunos clientes que utilizarían nuestra red para sus comunicaciones WAN usara el mismo direccionamiento interno? Simplemente no se pudieran comunicar y tocaría IMPONER a los clientes el direccionamiento que deben utilizar.

MP-BGP permite gracias a la riqueza de atributos del protocolo BGP “marcar” como únicas a las redes del cliente con esto permitir que nuestra red pueda ser utilizada por varios clientes sin restricción de direccionamiento interno y adicional este protocolo permite la propagación de las rutas entre todos los equipos PE (equipos de borde) a fin de que el cliente pueda alcanzar todos los sitios pertenecientes a su red.

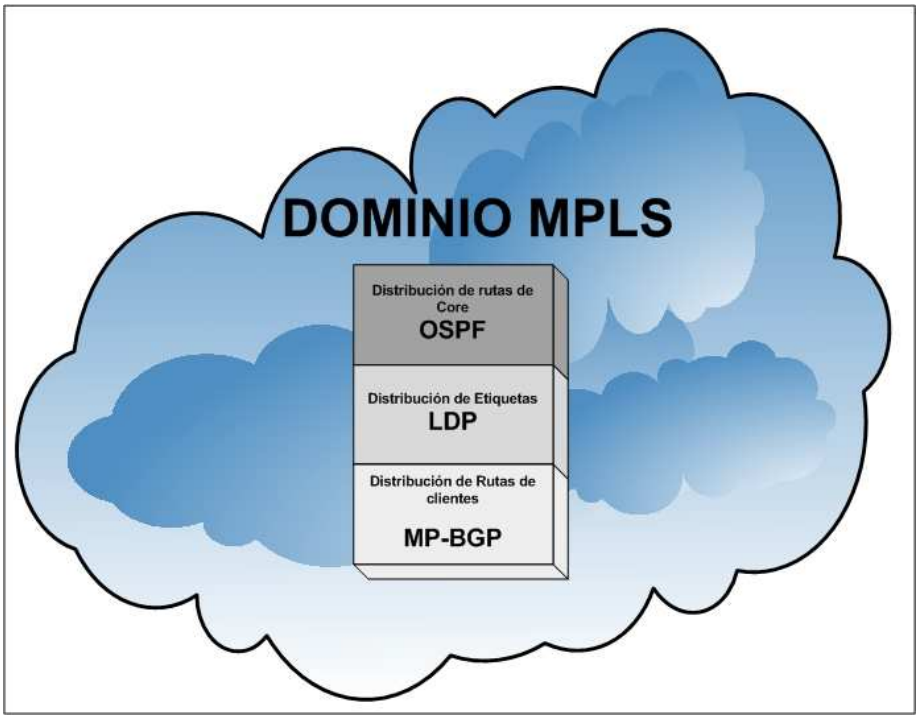


Fig. 5.2.- Protocolos Seleccionados

De forma adicional, en ambientes que tengan conexión al Internet, BGP es el único protocolo capaz de poder aprender la cantidad de rutas disponibles en el Internet, es por ello que su utilización para la comunicación entre grandes redes (sistemas autónomos) es de muy extensa utilización.

5.2 Diagrama de Red

A continuación se presenta el diagrama físico del diseño propuesta para la red nacional IP – MPLS:

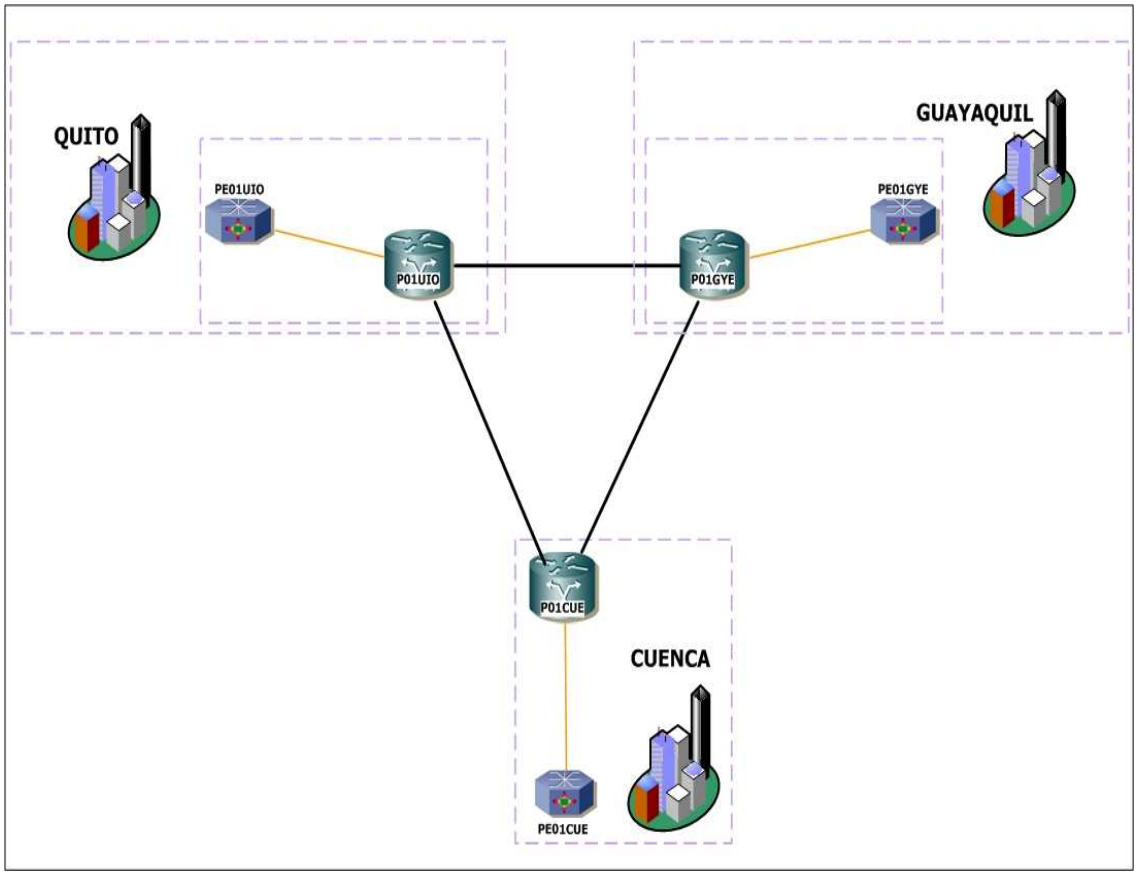


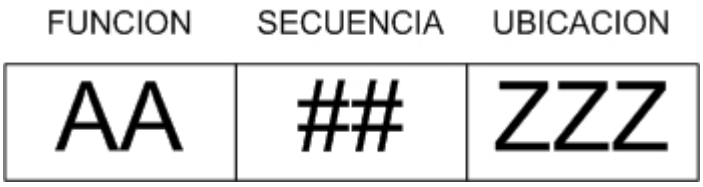
Fig. 5.3.- Diagrama Físico de la Red.

Para una mejor comprensión de este y futuros diagramas, presentamos la siguiente figura de convenciones:

Fig. 5.4 Convenciones

De la Nomenclatura:

La forma de nombrar a los equipos CORE de nuestra nos basamos en la siguiente formula:



Por lo que el equipo PE01GYE significa que el es un equipo PE (Provider Edge o E-LSR), siendo el primer equipo en ser instalado y esta ubicado geográficamente en Guayaquil.

5.3 Definición de los Servicios a Brindar

Conforme a los criterios de diseños inicialmente planteados y los protocolos seleccionados para el desarrollo del presente trabajo, la red en una fase inicial estará habilitada para poder soportar los siguientes servicios ejecutándose en su backbone MPLS:

1. VPNs peer to peer.
2. Calidad de Servicio.

Quedando para desarrollos futuros configuraciones y aplicaciones mucho más complejas como lo es implementar Traffic Engineering (Ingeniería de Tráfico) y AToM (Any Transport over MPLS) sobre la presente red de estudio.

5.3.1 Calidad de Servicio (QoS)

En la época actual donde la mayoría de las empresas (muy pronto será todas) están optando por redes que permitan la integración de todo tipo de datos: Datos realtime (tiempo real) o sensibles al retardo como lo son la voz y el video y los datos no sensibles al retardo como lo son correo electrónico y el http. Esta integración provoca que de no existir una configuración adicional, los datos de una empresa llegado un momento de congestión lucharán de igual a igual por la utilización del canal contratado. Esto sin lugar a dudas resulta perjudicial para los clientes dado que en esa lucha es muy probable que se pierdan datos importantes como lo son los paquetes de voz o de alguna aplicación financiera crítica para el desempeño normal del cliente.

Es por ello que se recurre a la configuración de Calidad del Servicio, donde básicamente lo que se hace es marcar el tráfico del cliente en la etiqueta MPLS que indique que tan importante es para el cliente para que en caso de congestión, los paquetes de mayor importancia sean los primeros en ser reenviados.

En nuestro proyecto hemos definido básicamente 5 categorías de priorización de tráfico:

- Tráfico Video – Muy sensible a la latencia* y jitter**.
- Tráfico Voz – Sensible a la latencia y jitter.
- Tráfico Datos Críticos – Son los datos que el cliente considera muy importantes para el normal desempeño de sus funciones, por lo general se relacionan con ERPs. (Aplicaciones Gerenciales y financieras).
- Tráfico de Datos No Críticos – Son los datos que no son de relevancia alta para el normal desempeño del negocio.

- Tráfico Best Efford – Cualquier tráfico generado por la empresa y que no este en las otras categorías.

Estas clasificaciones por lo general representan cargos extras a la tarifa que cancela el cliente por los enlaces contratados.

5.4 Direccionamiento Lógico de la Red.

Para el presente proyecto se ha considerado el siguiente direccionamiento lógico:

Direcciones Loopback

Nombre	Dirección	Máscara
PE01GYE	10.116.254.21	255.255.255.255
P01GYE	10.116.254.20	255.255.255.255
PE01UIO	10.116.254.11	255.255.255.255
P01UIO	10.116.254.10	255.255.255.255
PE01CUE	10.116.254.31	255.255.255.255
P01CUE	10.116.254.30	255.255.255.255

Tabla 5.1 Direcciones Loopback

Direccionamiento WAN

WAN	Dirección	Máscara
P01GYE - PE01GYE	10.116.253.160	255.255.255.252
P01GYE - P01UI0	10.116.253.0	255.255.255.252
P01UIO - PE01UI0	10.116.253.96	255.255.255.252
P01GYE - P01CUE	10.116.253.8	255.255.255.252
P01UI0 - P01CUE	10.116.253.4	255.255.255.252
P01CUE - PE01CUE	10.116.253.224	255.255.255.252

Tabla 5.2 Direccionamiento WAN

* Latencia: Tiempo que tarde un paquete en llegar a un destino medido desde que abandona su origen.

** Jitter: Es la variación en la latencia que se presentan en los paquetes recibidos.

Estas redes son las redes del core será propagadas mediante el IGP y de ninguna forma podrán ser conocidas por los clientes finales. A continuación, presentamos un esquema con el direccionamiento y la interfaz utilizada.

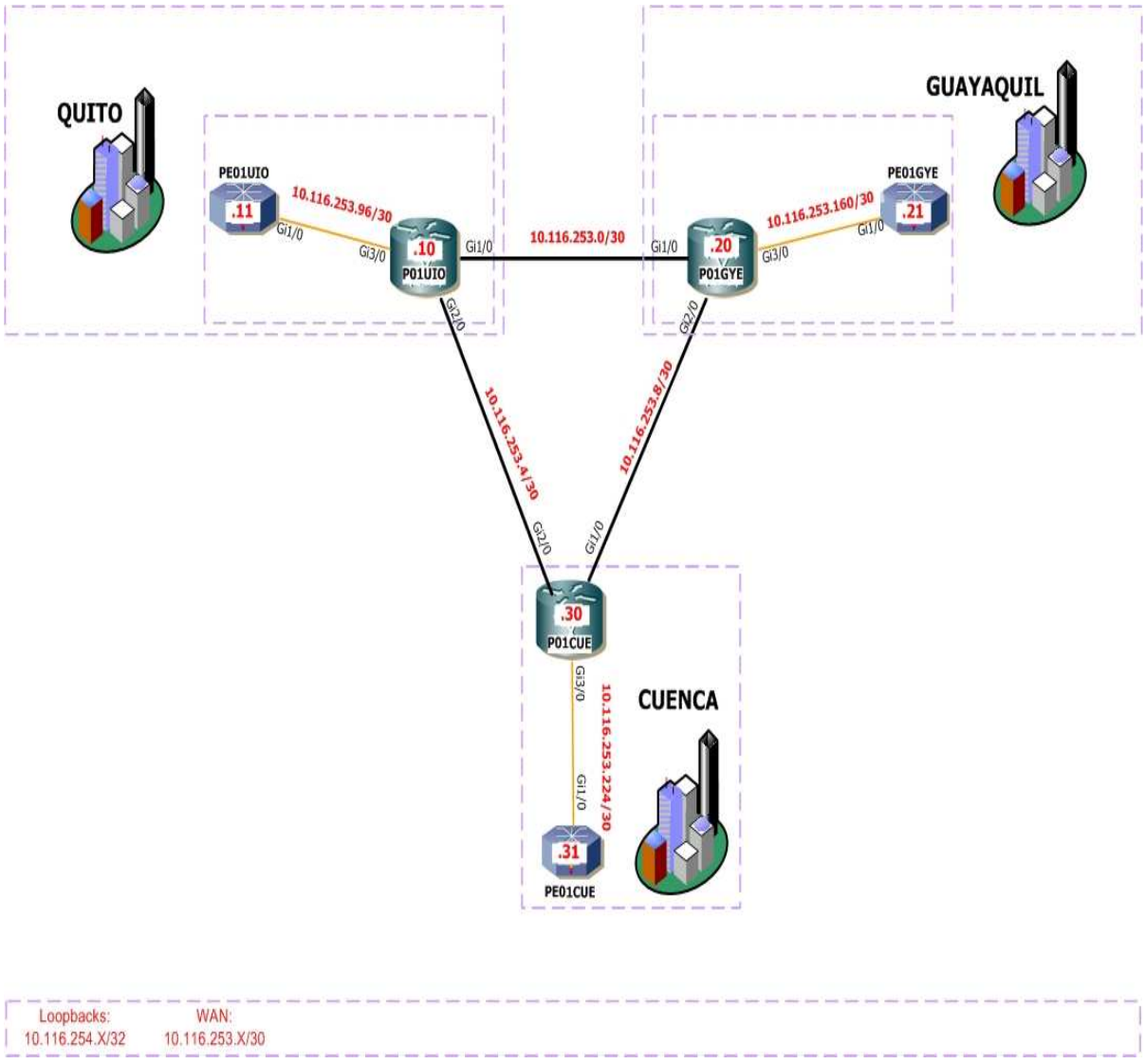


Fig. 5-5.- Direccionamiento de la Red

5.5 Configuración de los Equipos P (LSR)

El equipo P en nuestro diseño de red MPLS, su función primaría es la de realizar el reenvío de paquetes en base al intercambio de etiquetas. Adicional a esta función, hemos decidido en lugar de iniciar sesiones iBGP de todos contra todos hemos decidido implementar el esquema de Route Reflectors (RR) aplicándolo en los equipos P de Quito, Guayaquil y Cuenca a fin de que poder ejecutar MP-BGP contra los equipos PE y de esta forma poder propagar las rutas de los clientes.

Con esas acotaciones, el trabajo de configuración se dividirá en 4 bloques básicos:

1.- Habilitar MPLS – LDP.

2.- Configuración de la Calidad de Servicio.

3.- Configurar OSPF como protocolo IGP.

4.- Configurar BGP.

A continuación presentamos los comandos más relevantes que se ejecutarán sobre el router a fin de obtener la habilitación de los servicios.

5.5.1 Configuración MPLS – LDP

Habilitando MPLS - LDP
P01GYE(config)# ip cef
Este comando activa la función CEF en el router
P01GYE(config)# mpls ldp
Este comando habilita a LDP como protocolo de reenvío de etiquetas.
P01GYE(config)# mpls ldp router-id (loopback) force
Este comando obliga al LDP a utilizar como ID a la loopback
P01GYE(config-if)# mpls ip
Habilita a esta interfaz para poder reenviar etiquetas

5.5.2 Configuración de la Calidad de Servicio:

Para la configuración del QoS lo hemos dividido en 3 etapas:

- Creación de las Clases de Tráfico.
- Creación de las Políticas que tendrán esas clases de tráfico.
- Aplicación de las políticas sobre las interfaces.

Creación Clases de Tráfico

P01GYE(config)# class-map match-any CM-VoIP
Este comando crea la clase CM-VoIP
P01GYE(config-cmap)# match mpls experimental topmost 5
Este comando realiza un match con los paquetes MPLS con el bit experimental en 5.
P01GYE(config-cmap)# match ip precedence 5
Este comando realiza un match con los paquetes IP con precedence 5
P01GYE(config)# class-map match-any CM-Controlred
P01GYE(config-cmap)# match mpls experimental topmost 6 7
P01GYE(config-cmap)# match ip precedence 6 7
P01GYE(config)# class-map match-any CM-Video
P01GYE(config-cmap)# match mpls experimental topmost 4
P01GYE(config-cmap)# match ip precedence 4
P01GYE(config)# class-map match-any CM-Datoscriticos
P01GYE(config-cmap)# match mpls experimental topmost 2 3
P01GYE(config-cmap)# match ip precedence 2 3
P01GYE(config)# class-map match-any CM-Datosnocriticos
P01GYE(config-cmap)# match mpls experimental topmost 1
P01GYE(config-cmap)# match ip precedence 1

Creación de las Políticas

P01GYE(config)# policy-map PM-QoSBB
Este comando nombra a la política que se aplicará a las clases de tráfico creadas.
P01GYE(config-pmap)# class CM-VoIP

Este comando ingresa a la clase VoIP dentro de la politica QoSBB
P01GYE(config-pmap-c)# police rate percent 15
Este comando define un porcentaje de AB del 15% a la clase VoIP
P01GYE(config-pmap-c)# conform-action transmit
P01GYE(config-pmap-c)# exceed-action drop
P01GYE(config-pmap)# class CM-Video
P01GYE(config-pmap-c)# bandwidth percent 20
P01GYE(config-pmap-c)# queue-limit 20
Este comando indica la cantidad de paquetes que puede colectar antes de descartar
P01GYE(config-pmap)# class CM-Controlred
P01GYE(config-pmap-c)# bandwidth percent 3
P01GYE(config-pmap)# class CM-Datoscriticos
P01GYE(config-pmap-c)# bandwidth percent 20
P01GYE(config-pmap-c)# random-detect
P01GYE(config-pmap-c)# random-detect 2 20 50
P01GYE(config-pmap-c)# random-detect 3 30 60
Estos 2 comandos definen el rango de paquetes min y max antes de descartar.
P01GYE(config-pmap)# class CM-Datosnocriticos
P01GYE(config-pmap-c)# bandwidth percent 15
P01GYE(config-pmap-c)# random-detect
P01GYE(config-pmap-c)# random-detect 1 40 70
P01GYE(config-pmap)# class class-default
P01GYE(config-pmap-c)# random-detect
P01GYE(config-pmap-c)# random-detect 0 80 200

Aplicación de la Política en las Interfaces

P01GYE(config-if)# service-policy output PM-QoSBB
Este comando aplica la política definida para el tráfico de salida en la interfaz

5.5.3 Configuración OSPF

Configuración Loopback

P01GYE(config)# interface loopback 199
Este comando crea la interfaz de loopback
P01GYE(config-if)# ip address 10.116.254.20 255.255.255.255
Esta línea de comando asigna la IP a la loopback
P01GYE(config-if)# ip ospf network point-to-point
Habilita a la interfaz loopback para comunicar mediante OSPF.

Configuración OSPF

P01GYE(config)# router ospf 1
Este comando habilita la instancia ospf en el router
P01GYE(config-router)# router id 10.116.254.20
Declara como router ID a la dirección de loopback
P01GYE(config-router)# auto-cost reference-bandwidth 10000
Este comando se aplica cuando tenemos interfaces de mayor velocidad, por ejemplo Gigabit
P01GYE(config-router)# redistribute connected
Esta línea de comando permite redistribuir las redes directamente conectadas por las interfaces habilitadas.
P01GYE(config-router)# network 10.116.253.2 0.0.0.0 area 0
P01GYE(config-router)# network 10.116.253.9 0.0.0.0 area 0
P01GYE(config-router)# network 10.116.253.161 0.0.0.0 area 0
P01GYE(config-router)# network 10.116.254.20 0.0.0.0 area 0
Estos comandos declara las interfaces donde estará habilitado OSPF

5.5.4Configuración BGP – MP-BGP

Habilitando BGP en el equipo P01GYE

P01GYE(config)# router bgp 666
Este comando habilita la sesión BGP en este router.
P01GYE(config-router)# bgp router id 10.116.254.20
Este comando habilita a la loopback como identificador del router
P01GYE(config-router)# neighbor 10.116.254.10 remote-as 666
Este comando declara al router vecino con quien se establecerá la sesión BGP
P01GYE(config-router)# neighbor 10.116.254.10 description P01UIO
Este comando permite describir al vecino
P01GYE(config-router)# neighbor 10.116.254.10 update-source Loopback199
Este comando declara la IP de la interfaz que servira para recibir los updates BGP.

Habilitando MP-BGP en el equipo P01GYE

P01GYE(config-router)# address-family vpnv4
Este comando activa la sesión MP-BGP
P01GYE(config-router)# no bgp default ipv4-unicast
Este comando impide la propágación de rutas IPv4 entre los vecinos BGP
P01GYE(config-router-af)# neighbor 10.116.254.10 activate
Este comando activa a ese vecino para intercambiar rutas VPNv4
P01GYE(config-router-af)# neighbor 10.116.254.10 send-community both
Este comando se activa para permitir el atributos en los updates BGP
P01GYE(config-router-af)# neighbor 10.116.254.10 route-reflector-client
Este comando indica que este vecino será cliente de este RR.

En las últimas 2 tablas se han indica los comandos ingresados para configurar el P01GYE de Guayaquil con sesión BGP contra el P01UIO de Quito, habilitándolo a su vez para comunicar

VPNv4. El número escogido en nuestro proyecto como Sistema Autónomo es el 666. Esta configuración se repite contra los equipos: PE01GYE, PE01CUE, P01CUE, PE01UIO.

En resumen, esta es la configuración básica necesaria en los routers P de nuestra red MPLS. Para observar la configuración completa referirse al apéndice de configuraciones.

5.6 Configuración de los Equipos PE (Edge - LSR)

Los equipos PE en nuestro diseño de red MPLS, cumplen las siguientes funciones:

1.- Agregar o remover etiquetas a los paquetes IP.

2.- Conmutar paquetes etiquetados.

3.- Conmutar paquetes IP.

4.- Aplicar la política de servicio a los paquetes IP entrantes.

5.- Conocer y propagar las redes de los clientes.

En base a esas funciones, el trabajo de configuración se dividirá en 5 bloques básicos:

1.- Habilitar MPLS – LDP.

2.- Configuración de la Calidad de Servicio.

3.- Configurar OSPF como protocolo IGP.

4.- Configurar BGP.

5.- Configurar las VRFs de los clientes. (En nuestro caso haremos una prueba montando el cliente ESPOL con una VPN entre las ciudades de Guayaquil y Quito.)

En las siguientes tablas presentaremos los comandos más relevantes a utilizar para la configuración en los equipos PE.

5.6.1 Habilitación MPLS - LDP

Habilitando MPLS - LDP

PE01GYE(config)# ip cef
Este comando activa la función CEF en el router
PE01GYE(config)# mpls label protocol ldp
Este comando habilita a LDP como protocolo de reenvío de etiquetas.
PE01GYE(config)# mpls ldp router-id (loopback) force
Este comando forza al LDP a utilizar como ID a la loopback
PE01GYE(config)# mpls ldp label range 16 800000
Este comando indica el rango de valores de las etiquetas
PE01GYE(config-if)# mpls ip
Habilita a esta interfaz para poder reenviar etiquetas

5.6.2 Configuración de la Calidad de Servicio

Para la configuración del QoS lo hemos dividido en 3 etapas:

- Creación de las Clases de Tráfico.
- Creación de las Políticas que tendrán esas clases de tráfico.
- Aplicación de las políticas sobre las interfaces.

Creación Clases de Tráfico

PE01GYE(config)# class-map match-any CM-VoIP
Este comando crea la clase CM-VoIP

PE01GYE(config-cmap)#	**match mpls experimental topmost 5**
Este comando realiza un match con los paquetes MPLS con el bit experimental en 5.	
PE01GYE(config-cmap)#	**match ip precedence 5**
Este comando realiza un match con los paquetes IP con precedence 5	
PE01GYE(config)#	**class-map match-any CM-Controlred**
PE01GYE(config-cmap)#	**match mpls experimental topmost 6 7**
PE01GYE(config-cmap)#	**match ip precedence 6 7**
PE01GYE(config)#	**class-map match-any CM-Video**
PE01GYE(config-cmap)#	**match mpls experimental topmost 4**
PE01GYE(config-cmap)#	**match ip precedence 4**
PE01GYE(config)#	**class-map match-any CM-Datoscriticos**
PE01GYE(config-cmap)#	**match mpls experimental topmost 2 3**
PE01GYE(config-cmap)#	**match ip precedence 2 3**
PE01GYE(config)#	**class-map match-any CM-Datosnocriticos**
PE01GYE(config-cmap)#	**match mpls experimental topmost 1**
PE01GYE(config-cmap)#	**match ip precedence 1**

Dado que los equipos PE son los equipos frontera en nuestra red MPLS, son los llamados a limitar el tráfico asignado para cada cliente. Esto lo hacemos mediante la configuración de Traffic Policies que se presenta en los siguientes comandos, hemos creado políticas para los caudales: 1280K, 256K y 128K mismas que luego serán aplicadas a las interfaces que conecten a los usuarios.

Creación Políticas ancho de banda clientes	
PE01GYE(config)#	**policy-map 1280Kbps**
Este comando crea la politica 1280Kbps para anchos de banda de clientes	
P01GYE(config-pmap)#	**class class-default**
Este comando asocia la politica creada anteriormente con la clase default	
P01GYE(config-pmap-c)#	**police cir 1280000 bc 40000 be 40000**
Este comando indica el AB comprometido en esta clase, el exceso permitido y el exceso antes de descartar paquetes	

P01GYE(config-pmap-c)#	**exceed-action drop**
Aquí se aplica la acción que se ejecutará según la regla anterior.	
PE01GYE(config)#	**policy-map 128Kbps**
PE01GYE(config-pmap)#	**class class-default**
PE01GYE(config-pmap-c)#	**police cir 128000 bc 4000 be 4000**
PE01GYE(config-pmap-c)#	**exceed-action drop**
PE01GYE(config)#	**policy-map 256Kbps**
PE01GYE(config-pmap)#	**class class-default**
PE01GYE(config-pmap-c)#	**police cir 256000 bc 8000 be 8000**
PE01GYE(config-pmap-c)#	**exceed-action drop**

Políticas QoS de Backbone

PE01GYE(config)#	**policy-map PM-QoSBB**
Este comando nombra a la política que se aplicará a las clases de tráfico creadas.	
PE01GYE(config-pmap)#	**class CM-VoIP**
Este comando ingresa a la clase VoIP dentro de la política QoSBB	
PE01GYE(config-pmap-c)#	**police rate percent 15**
Este comando define un porcentaje de AB del 15% a la clase VoIP	
PE01GYE(config-pmap-c)#	**conform-action transmit**
PE01GYE(config-pmap-c)#	**exceed-action drop**
PE01GYE(config-pmap)#	**class CM-Video**
PE01GYE(config-pmap-c)#	**bandwidth percent 20**
PE01GYE(config-pmap-c)#	**queue-limit 20**
Este comando indica la cantidad de paquetes que puede colectar antes de descartar	
PE01GYE(config-pmap)#	**class CM-Controlred**
PE01GYE(config-pmap-c)#	**bandwidth percent 3**
PE01GYE(config-pmap)#	**class CM-Datoscriticos**
PE01GYE(config-pmap-c)#	**bandwidth percent 20**
PE01GYE(config-pmap-c)#	**random-detect**
PE01GYE(config-pmap-c)#	**random-detect 2 20 50**
PE01GYE(config-pmap-c)#	**random-detect 3 30 60**

Estos 2 comandos definen el rango de paquetes min y max antes de descartar.
PE01GYE(config-pmap)# class CM-Datosnocriticos
PE01GYE(config-pmap-c)# bandwidth percent 15
PE01GYE(config-pmap-c)# random-detect
PE01GYE(config-pmap-c)# random-detect 1 40 70
PE01GYE(config-pmap)# class class-default
PE01GYE(config-pmap-c)# random-detect
PE01GYE(config-pmap-c)# random-detect 0 80 200

5.6.3 Configuración de OSPF

Configuración Loopback

PE01GYE(config)# interface loopback 199
Este comando crea la interfaz de loopback
PE01GYE(config-if)# ip address 10.116.254.21 255.255.255.255
Esta línea de comando asigna la IP a la loopback
PE01GYE(config-if)# ip ospf network point-to-point
Habilita a la interfaz loopback para comunicar mediante OSPF.

Configuración OSPF

PE01GYE(config)# router ospf 1
Este comando habilita la instancia ospf en el router
PE01GYE(config)# router id 10.116.254.21
Declara como router ID a la dirección de loopback
PE01GYE(config-router)# auto-cost reference-bandwidth 10000
Este comando se aplica cuando tenemos interfaces de mayor velocidad, por ejemplo Gigabit.
PE01GYE(config-router)# network 10.116.253.162 0.0.0.0 area 0
PE01GYE(config-router)# network 10.116.254.21 0.0.0.0 area 0
Estos comandos declara las interfaces donde estará habilitado OSPF

5.6.4 Configuración BGP – MP-BGP

Habilitando BGP en el equipo PE01GYE

PE01GYE(config)# router bgp 666
Este comando habilita la sesión BGP en este router.
PE01GYE(config-router)# bgp router id 10.116.254.21
Este comando habilita a la loopback como identificador del router
PE01GYE(config-router)# neighbor 10.116.254.10 remote-as 666
Este comando declara al router vecino con quien se establecerá la sesión BGP
PE01GYE(config-router)# neighbor 10.116.254.10 description P01UIO
Este comando permite describir al vecino
PE01GYE(config-router)# neighbor 10.116.254.10 update-source Loopback199
Este comando declara la IP de la interfaz que servirá para recibir los updates BGP.

Habilitando MP-BGP en el equipo PE01GYE

PE01GYE(config-router)# address-family vpnv4
Este comando activa la sesión MP-BGP
PE01GYE(config-router)# no bgp default ipv4-unicast
Este comando impide la propágación de rutas IPv4 entre los vecinos BGP
PE01GYE(config-router-af)# neighbor 10.116.254.10 activate
Este comando activa a ese vecino para intercambiar rutas VPNv4
PE01GYE(config-router-af)# neighbor 10.116.254.10 send-community both
Este comando se activa para permitir el atributos en los updates BGP
PE01GYE(config-router-af)# neighbor 10.116.254.10 next-hop-self
Este comando impide que se propague al nodo del cliente como next hop dentro de la red MPLS en caso de que se inicie una instancia eBGP con los clientes.

Esta configuración se ha realizado para iniciar la sesión BGP con el P01UIO, esta deberá replicarse para los otros 2 Ps: P01GYE y P01CUE quienes serán RR. La configuración completa de todos los PE podrá ser consultada en la sección de apéndices.

5.6.5 Configuración EIGRP contra el cliente.

Se ha escogido como protocolo de enrutamiento para aprender las rutas del cliente el protocolo EIGRP, a continuación se detallan los comandos necesarios para la configuración.

Configuración EIGRP
PE01GYE(config)# router eigrp 100
Este comando habilita la instancia eigrp en el router
PE01GYE(config-router)# address-family ipv4 vrf espol
Aquí habilitamos que EIGRP alimente la tabla de enrutamiento de la vrf espol.
PE01GYE(config-router)# redistribute bgp 666 metric 128000 10 255 1 1500
Este comando habilita la redistribución de las rutas eigrp hacia el protocolo bgp
PE01GYE(config-router)# network 192.168.1.0 0.0.0.3
Este comando identifica la red eigrp
PE01GYE(config-router)# network 192.168.1.0 0.0.0.3
Este comando evita la sumarización.

5.7 Configuración de los equipos CE - Costumer Equipment

Para efectos de realizar pruebas y comprobar el funcionamiento de nuestra red MPLS, desde el punto de vista de la calidad de servicio (marcado de paquetes) y del servicio de VPN peer to peer, planteamos el siguiente escenario:

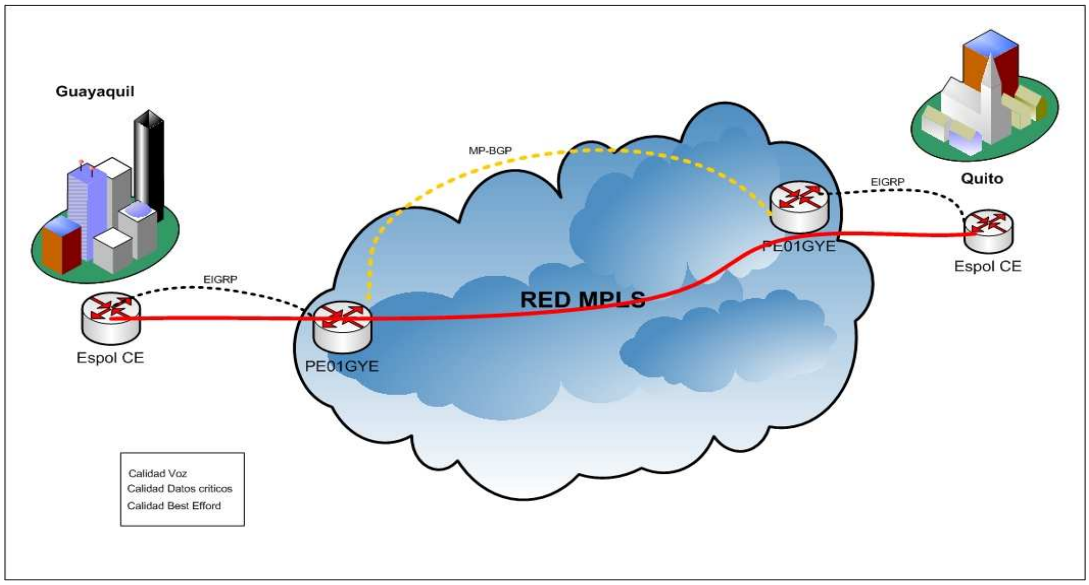


Fig. 5-7.- Red de pruebas – VPN Espol

Para estas pruebas, se considera la siguiente necesidad: Cliente Espol tiene una matriz en Guayaquil y una sucursal en la ciudad de Quito. Desea interconectarlas utilizando la red MPLS que se ha diseñado. El tráfico que cursará por la red tendrá 3 tipos de priorización: Voz, Datos Críticos y Best Efford. Para efecto de pruebas, el tipo de datos críticos se ha definido como ICMP solo para validar el marcado.

Para la comunicación entre el CE y el PE, se ha escogido el protocolo de enrutamiento dinámico EIGRP, pero esto es en realidad a conveniencia y acuerdo con el cliente dado que se puede implementar RIP, IGRP, OSPF, IS – IS o el protocolo externo BGP e incluso las simples rutas estáticas.

Con estas premisas, el procedimiento para el enrutamiento se dividió en las siguientes tareas:

1.- Configurar las clases de servicio del cliente.

2.- Configurar EIGRP contra el router PE.

5.7.1 Configuración QoS

Creación Clases de Tráfico

espol(config)# class-map match-all voz
Este comando crea la clase voz
espol(config-cmap)# match ip precedence 5
Este comando realiza un match con los paquetes IP con precedence 5
espol(config)# class-map match-all datoscriticos
espol(config-cmap)# match ip precedence 3
espol(config)# class-map match-all best_efford
espol(config-cmap)# match ip precedence 1

Creación Política clientes Espol
espol(config)# policy-map QoS_out
Este comando crea la politica QoS_out
P01GYE(config-pmap)# class voz
Este comando asocia la política creada anteriormente con la clase voz
P01GYE(config-pmap-c)# set ip precedence 5
Este comando indica que a los paquetes de la clase voz les seteará el IP precedence en 5
espol(config)# policy-map QoS_out
espol(config-pmap)# class datoscriticos
espol(config-pmap-c)# set ip precedence 3
espol(config)# policy-map QoS_out
espol(config-pmap)# class best_efford
espol(config-pmap-c)# set ip precedence 1

Aplicación de la Política en las Interfaces

espol(config-if)# service-policy output QoS_out
Este comando aplica la política definida para el tráfico de salida en la interfaz

5.7.2 Configuración EIGRP

Configuración EIGRP

espol(config)# router eigrp 100
Este comando habilita la instancia eigrp en el router
espol(config-router)# network network 10.6.0.0 0.0.255.255
Este comando identifica la red de la sucursal en Quito
espol(config-router)# network 192.168.1.0 0.0.0.3
Este comando identifica la red conectada en Guayaquil
espol(config-router)# no auto-summary
Este comando evita la sumarización.

Capítulo 6

Diseño de la Red

Protocolo de Pruebas de la red utilizando Dynamips

6.1 Generalidades Simulador

Antes de validar la configuración realizada en cada uno de los equipos que forman parte del diseño de la red MPLS, es necesario que detallemos las características del simulador que utilizaremos para levantar nuestro laboratorio.

GNS3 (Graphical Network Simulator) es un simulador gráfico de redes que permite la simulación de redes complejas.

Para una completa simulación, GNS3 esta fuertemente ligado con:

- Dynamips, este es el núcleo que permite la simulación de las imágenes de Cisco.
- Dynagen, es el frente al usuario de Dynamips pero basado en texto.

El programa GNS3 es un desarrollo de código abierto, es decir que puede ser modificado, mejorado o cambiado por los usuarios y que puede ser ejecutado sobre plataforma Windows, Mac o Linux.

Antes de la aparición de GSN3 en el 2007, la utilización de Dynamips de cierta forma era compleja pues se debía realizar primero la topología de la red mediante texto, es decir, había que

indicar línea por línea en el archivo de configuración los routers, switches y la forma en que esos equipos de red se interconectaban e indicar las interfaces.

Dynamips, que es el motor de simulación que utiliza GNS3, es el más avanzado simulador existente actualmente en el mundo académico dado que a diferencia de simuladores como Bosom o Simulink, Dynamips no simula routers a nivel de software sino que utilizando el hardware de una PC ejecuta el IOS (sistema operativo de los equipos Cisco) para simular físicamente a un router real. Es decir, Dynamips no es simulador de software sino que simula un router real ejecutándose en una computadora (PC) y utilizando su procesador y tarjetas para el reenvío de paquetes.

Por supuesto que es difícil obtener el "perfomance" o desempeño de un router real que puede obtener operaciones de reenvío de paquetes de 100 Kpps (kilo packets per second) en los antiguos NPE-100 a diferencia de una PC robusta, con excelente tarjeta madre y procesador que puede obtener un promedio de 1Kpps.

Entre las cosas que se pueden realizar sobre GNS3 – Dynamips están:

- ✓ Diseñar redes de alta complejidad topológica.
- ✓ Emular las plataformas de Routers Cisco y Cortafuegos PIX. En la actualidad, Dynamips soporta IOS de equipos Cisco 36XX y 72XX, estos últimos fueron los escogidos para el desarrollo de este trabajo.
- ✓ Simular switches Ethernet, ATM y Frame relay.
- ✓ Conectar la red "simulada" al mundo real, mediante la utilización de las tarjetas NICs de la o las PCs.
- ✓ Capturar los paquetes mediante sniffers o capturadotes de tráfico como WireShark.

6.1.1 Validación de Hardware del PC e Instalación del simulador

La instalación y posterior operación del aplicativo GNS3 es relativamente sencilla pues al estar en ambiente Windows no genera mayor problema con su ambiente gráfico. Mayor información acerca de su operación puede ser consultada en el Web del creador: www.gns3.net y en el siguiente link encontrarán un manual muy completo para su total comprensión: http://ufpr.dl.sourceforge.net/sourceforge/gns-3/GNS3-0.5-tutorial.pdf

Las características de la PC que utilizamos para el procedimiento de simulación de la red y sus posteriores pruebas son las siguientes:

a. Tarjeta madre INTEL DG31PR LGA775 (SON/VID/LAN)
b. Procesador INTEL Intel Core2Duo E7200 2.53Ghz 3M 1066Mhz.
c. 3 Gb de Memoria RAM*
d. OS: Windows XP Edición Profesional
e. 2 Tarjetas de Red adicional 10/100 Mbps Rj 45.

* La tarjeta madre tiene capacidad máxima de 4Gb de memoria RAM, pero al llegar a esta capacidad notamos demasiada instabilidad en el sistema.

Durante la fase de pruebas, notamos que al arrancar el simulador el consumo del procesador se eleva al 100% durante la fase de descompresión del IOS en cada uno de los routers y durante la fase en la que las sesiones OSPF, BGP y LDP se están iniciando. Luego de alrededor de 10 minutos el simulador esta consumiendo alrededor del 40% del procesador y estamos listos para realizar la configuración y posterior pruebas de este laboratorio.

6.2 Revisión de las configuraciones y validación de funcionamiento

El objetivo de esta sección es validar la correcta operación y funcionamiento de la configuración realizada en el capítulo anterior, para lo cual nos valdremos del comando “SHOW”. Este comando, aplicado según la necesidad nos permitirá verificar desde el estado de las interfaces hasta conocer si los routers están aprendiendo las rutas de sus vecinos y clientes mediante los protocolos que se configuraron.

6.2.1 Interfaces

En esta primera parte de la revisión validaremos el estado de las interfaces mediante el comando “show ip interface brief” que nos presenta un resumen acerca de la configuración básica impuesta sobre las interfaces (IP address) y si estas están activas o no. En los siguientes gráficos se muestra el resultado de este comando aplicado en los routers PE y P de Guayaquil.

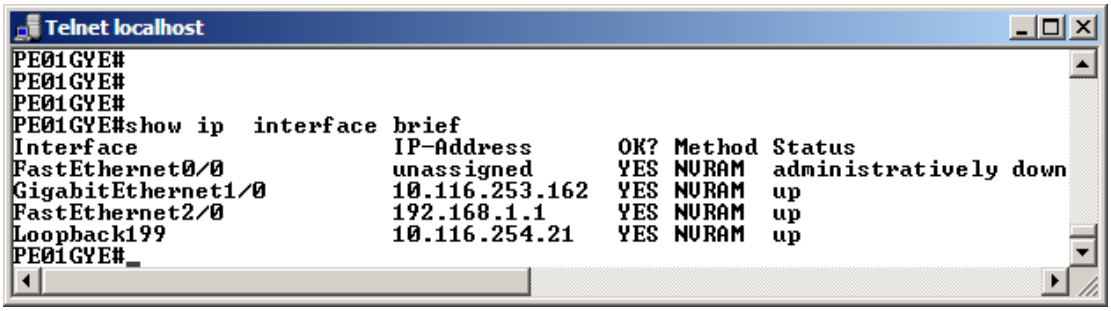


Fig. 6-1.- Interface brief PE01GYE

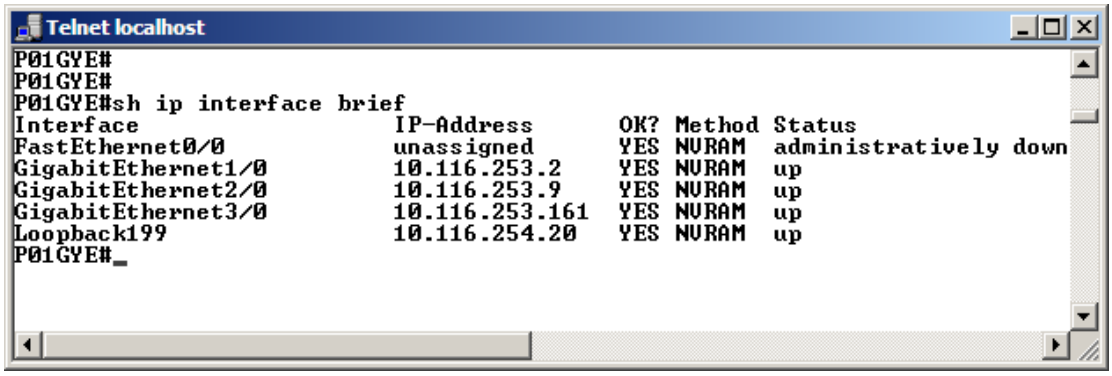


Fig. 6-2.- Interface brief P01GYE

6.2.2 MPLS – LDP

En esta sección se verificará el estado del protocolo LDP en la interfaces habilitadas para el intercambio de etiquetas, que la tabla LIB y LFIB se estén creando de forma correcta, a fondo estas tablas se analizarán en el apartado de verificación de flujo de datos. Los siguientes comandos (gráficos) verifican el correcto funcionamiento del protocolo MPLS sobre nuestra red.

Este comando ***"show mpls interface***" nos permite confirmar que las interfaces de los routers estén habilitadas para la conmutación de etiquetas. Este comando se deberá ejecutar en todos los routers core, a modo de ejemplo presentamos en el equipo P01GYE:

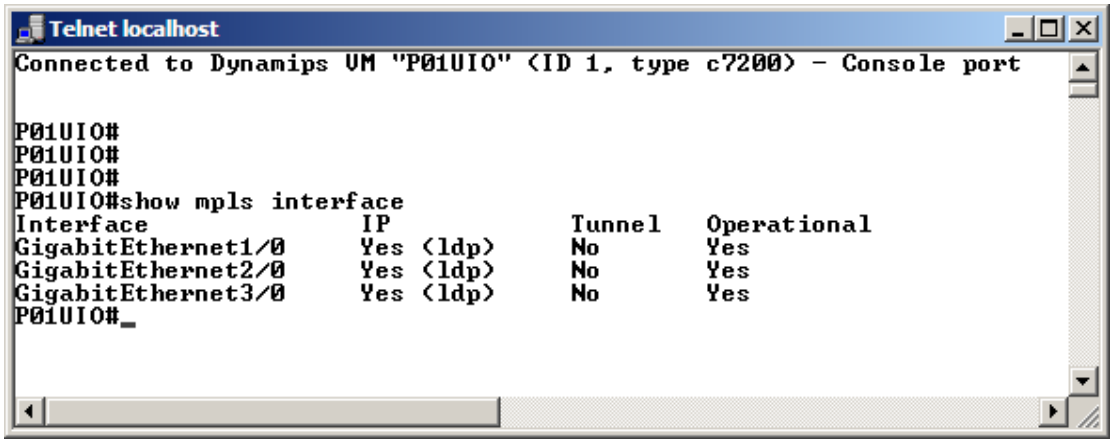


Fig. 6-3.- show mpls interface

Como se aprecia en el gráfico, las interfaces Giga 1-2-3 están habilitadas para conmutar etiquetas. Estas interfaces son las que conectan con los routers PE01GYE, P01UIO y P01CUE.

El siguiente comando ***"show mpls ldp parameters"*** muestra los parámetros sobre los cuales se esta ejecutando MPLS en nuestra red, el más importante es el que indica que la forma de envío de etiquetas a sus vecinos en "Downstream", adicionalmente indica el rango de etiquetas que previamente habíamos configurado.

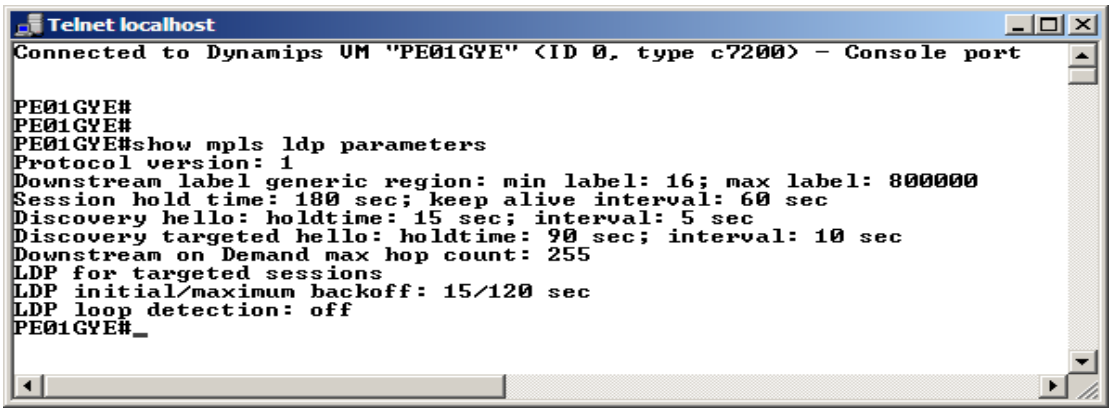


Fig. 6-4.- MPLS Parámetros

El siguiente comando ***"show mpls ldp discovery all"*** muestra como se descubren vecinos LDP, en el gráfico se muestra el comando sobre el P01CUE que esta conectado al PE de Cuenca y a los otros 2 Ps.

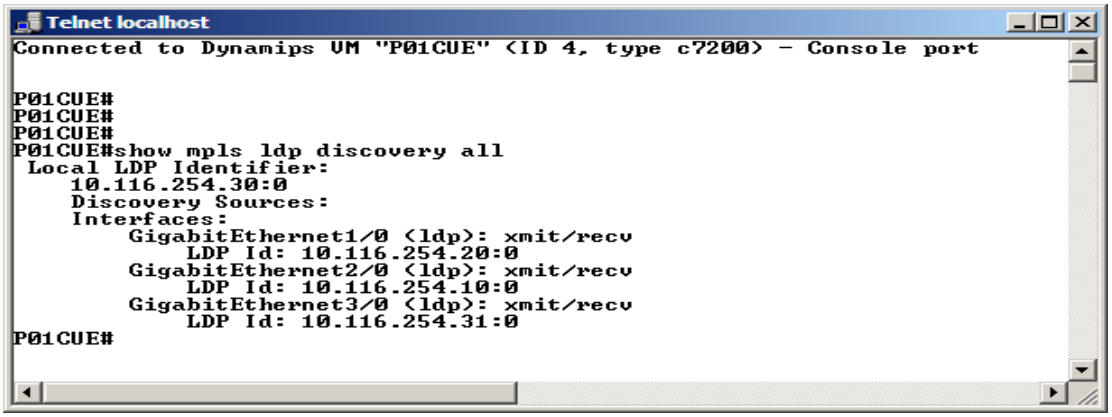


Fig. 6-5.- LDP Discovery

El comando ***"show mpls ldp neighbors"*** indica los vecinos LDP con los cuales **YA** se ha establecido la adyacencia. En el ejemplo se muestra el comando ejecutado sobre el P01UIO.

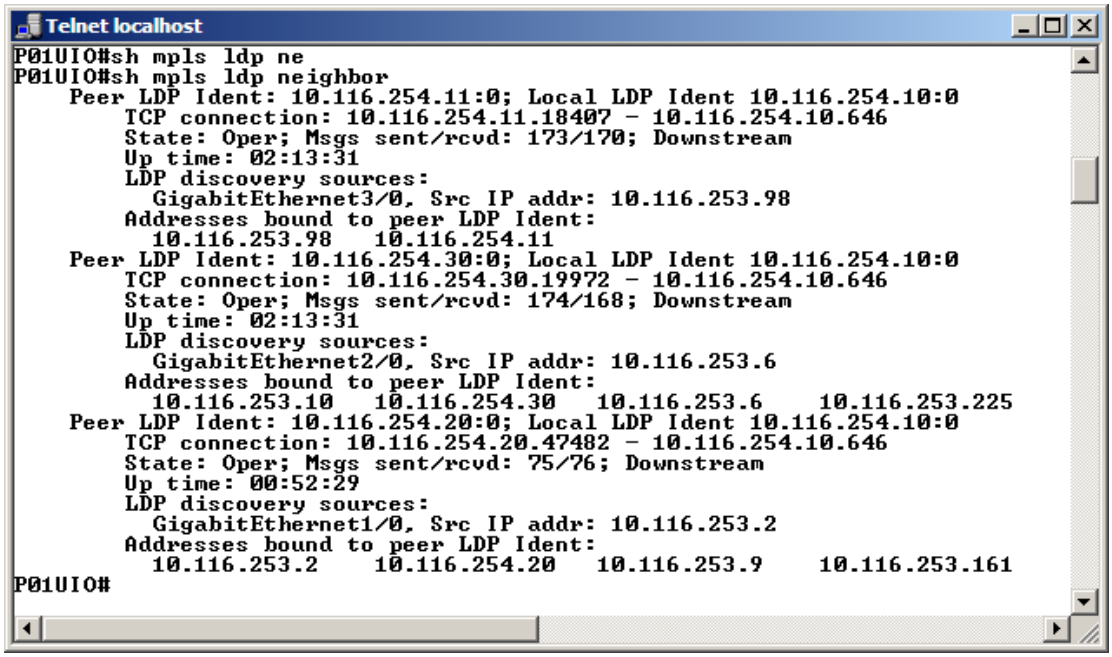


Fig. 6-6.- Vecinos LDP

Nótese que el siguiente gráfico muestra los vecinos del PE01GYE; como era de esperarse solo tiene una vecindad con el P01GYE, puesto que la otra interfaz esta conectada con el cliente, quién no habla LDP.

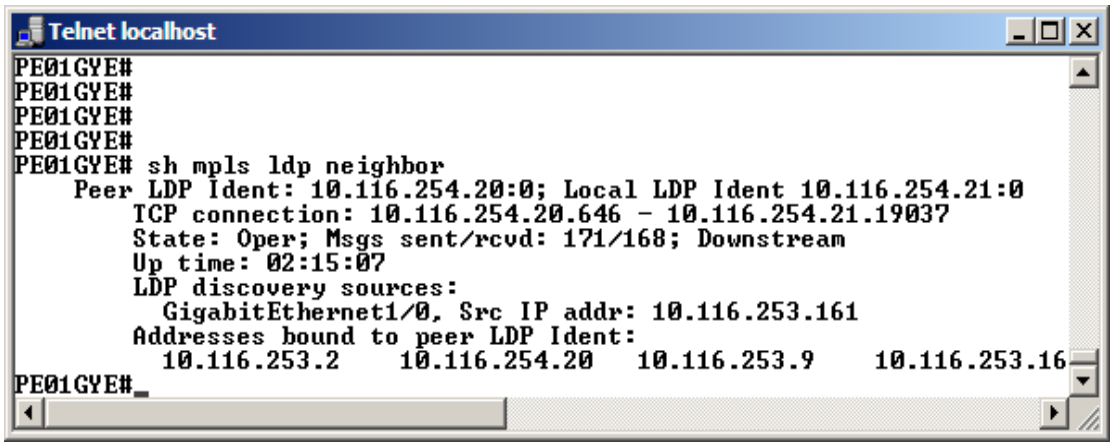


Fig. 6-7.- Vecinos LDP PE01GYE

En esta parte de las pruebas, se muestra el resultado de aplicar el comando ***"show mpls ldp neighbors detail"***; quién no solo muestra las adyacencias sino que entrega mayor información de los vecinos. El comando fue ejecutado una vez más sobre el P01UIO.

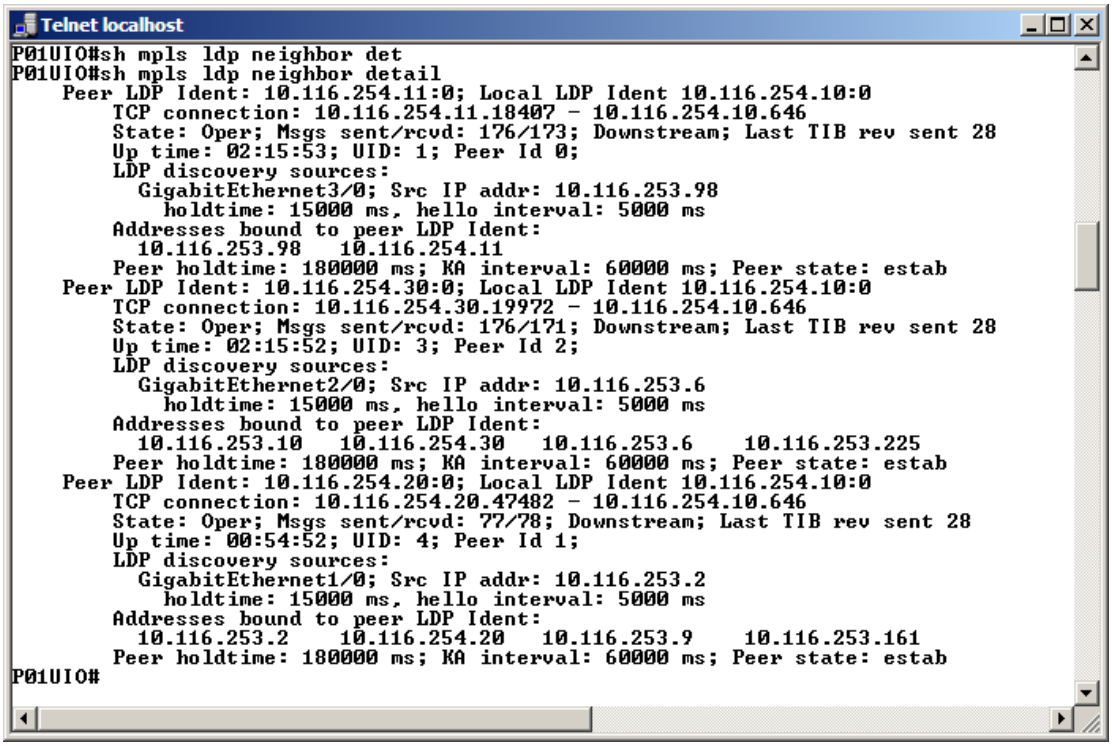


Fig. 6-8.- Vecinos LDP con detalles.

Y en la última parte de estas pruebas de esta sección, presentamos las tablas LIB y LFIB formadas en el equipo PE01GYE mediante el comando ***"show mpls ldp binding"*** y el comando ***"show mpls forwarding-table"*** donde se indican los valores local y remoto de las etiquetas así como el siguiente salto definido para una red destino requerido. Esto se analizará más a detalle cuando se verifique el flujo de datos entre los clientes y la red MPLS.

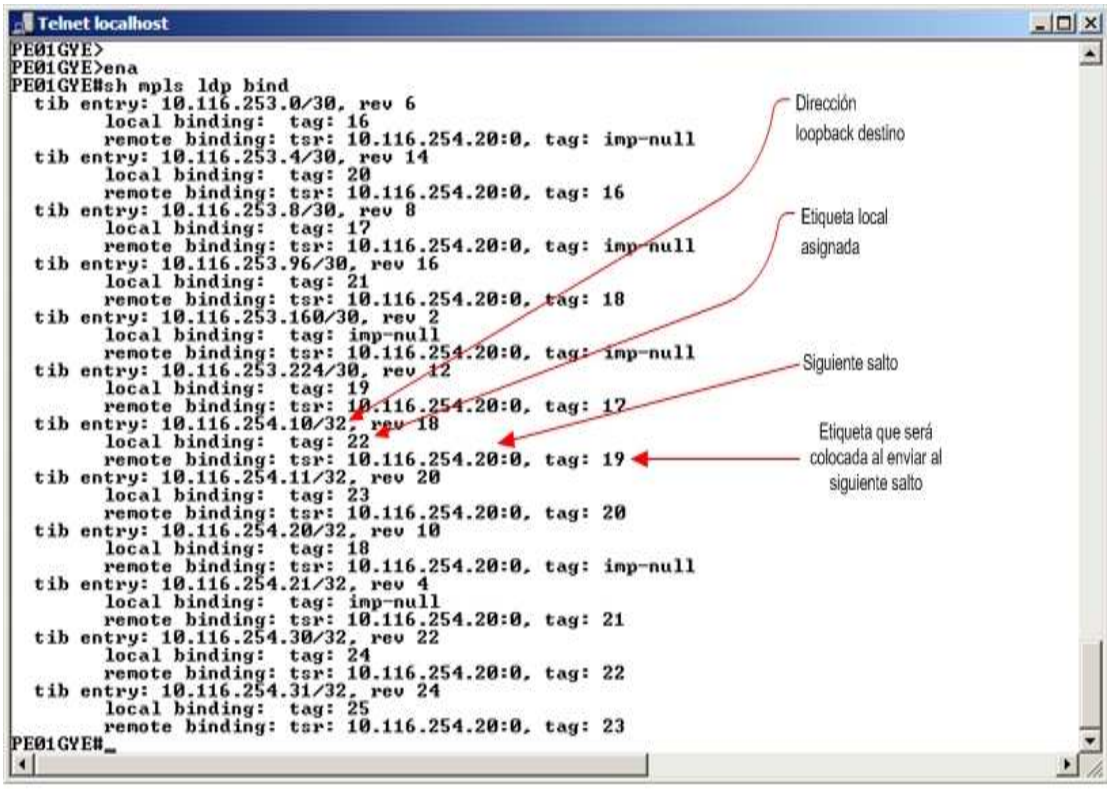


Fig. 6-9.- Tabla LIB del PE01GYE

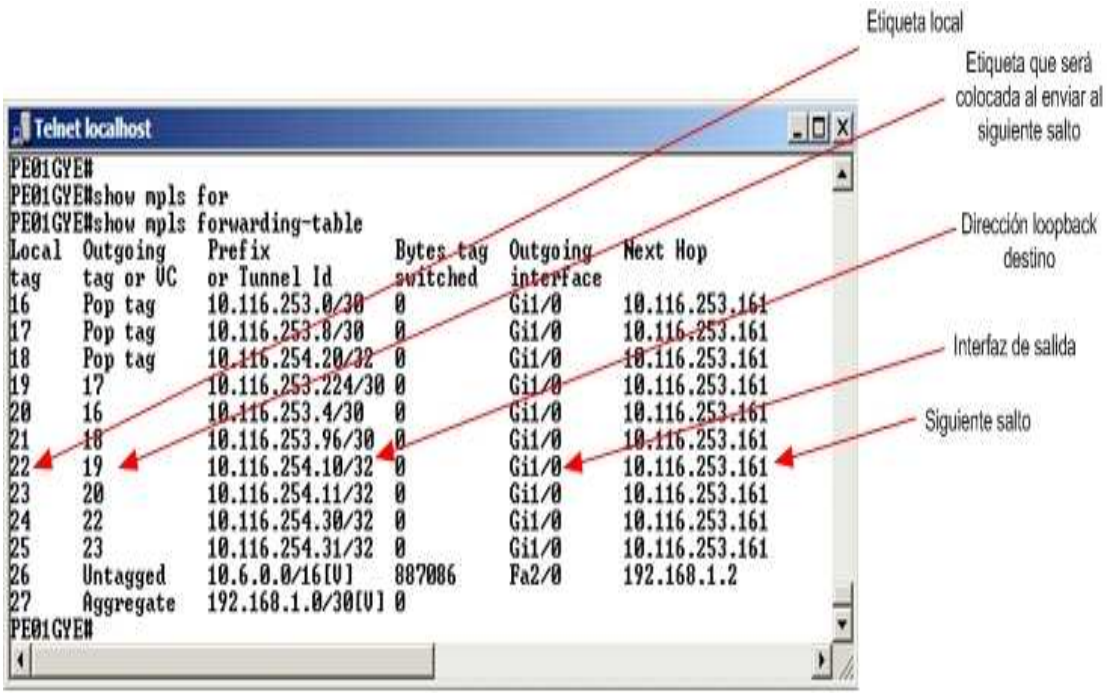


Fig. 6-10.- Tabla LFIB del PE01GYE

6.2.3 OSPF

Como vimos en la fase de diseño, el IGP escogido para que todos nuestros nodos conozcan sus rutas fue OSFP, en los siguientes cuadros verificaremos su correcto funcionamiento. Los comandos deben aplicarse a todos los routers core de la red, pero a modo ilustrativo presentaremos los resultados de los equipos P y PE de Guayaquil.

Los 2 gráficos venideros muestran los protocolos (instancias) que se están ejecutando tanto en el PE y P. En el equipo P vemos los 2 protocolos que hemos configurado el OSPF y BGP; y en el equipo P se observa el protocolo EIGRP configurado (veremos sus rutas dentro de la VRF más adelante) además de los protocolos OSPF y BGP necesarios para el funcionamiento del backbone.

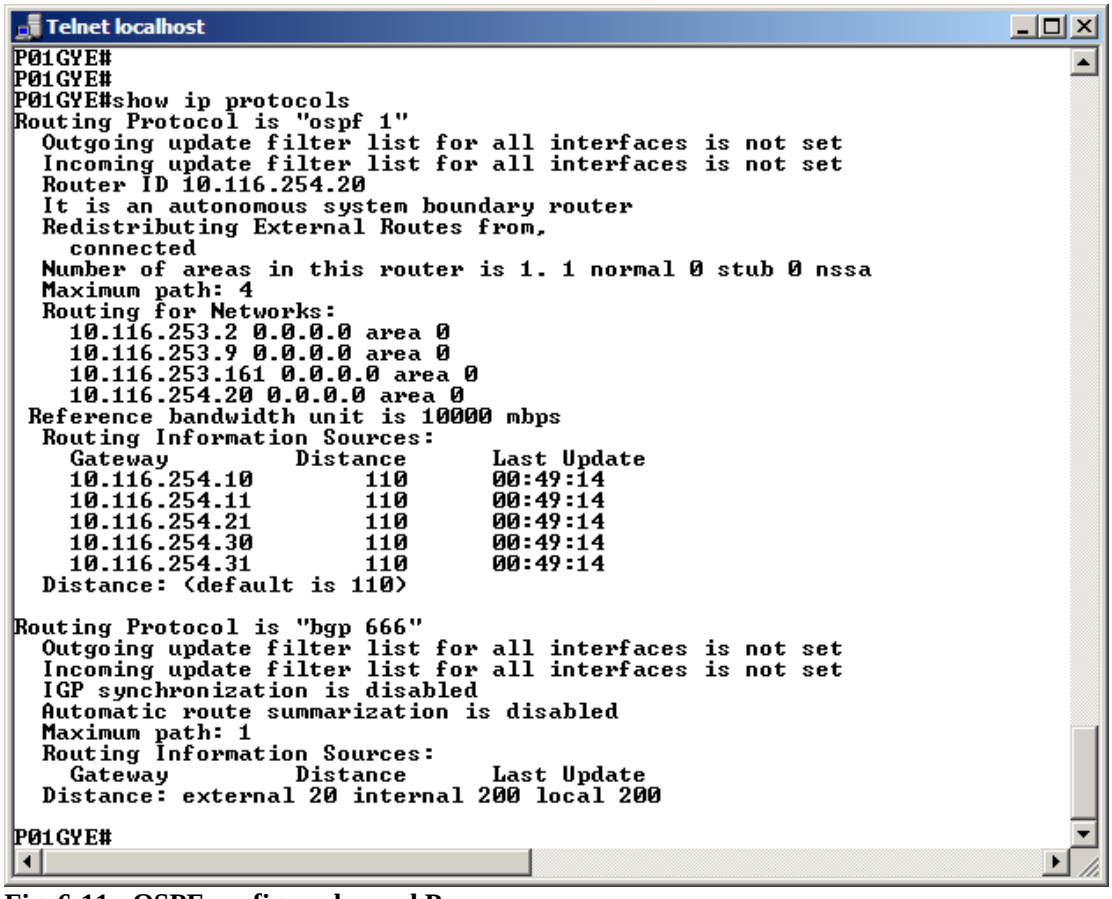


Fig. 6-11.- OSPF configurado en el P

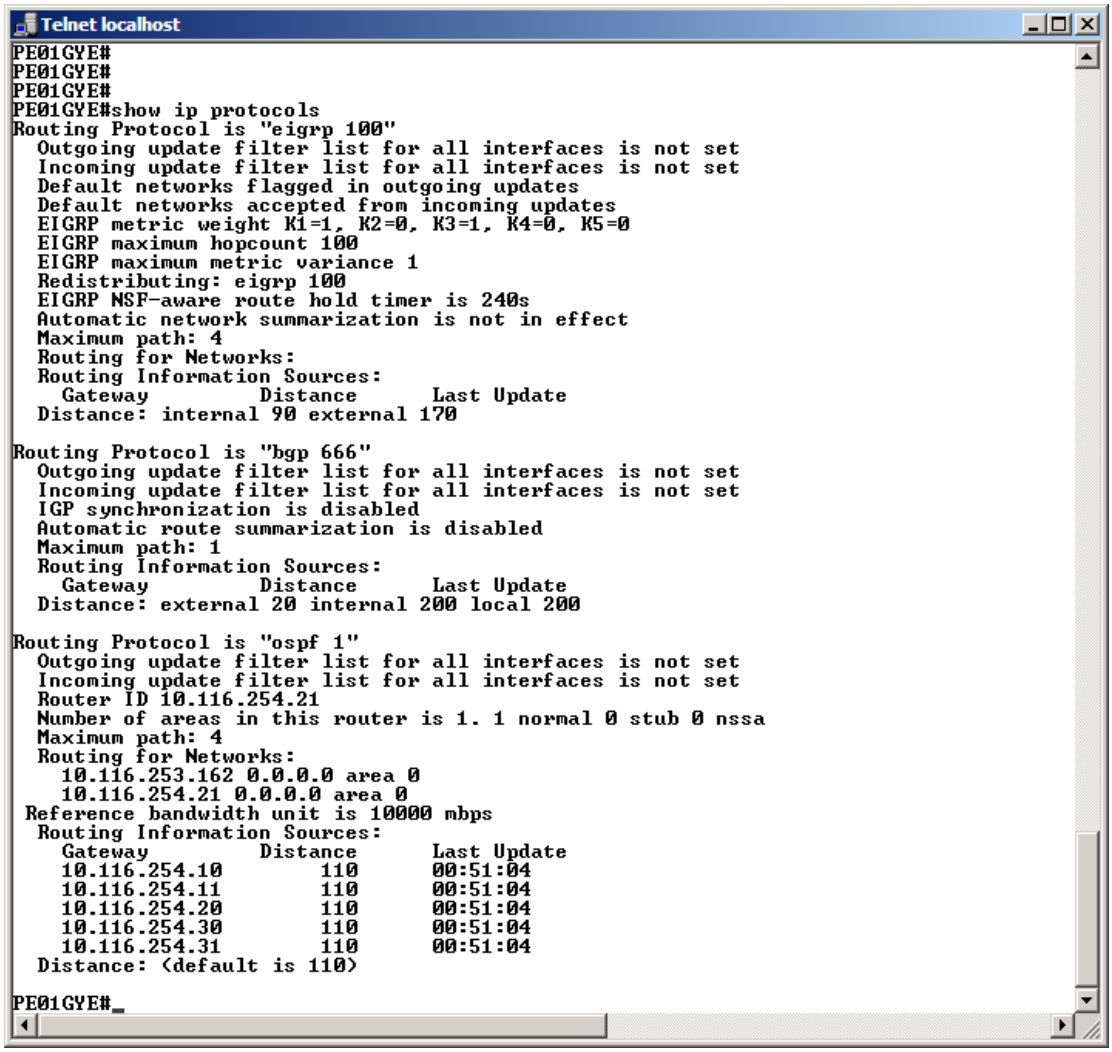


Fig. 6-12.- OSPF configurado en el PE

Estos gráficos son de alta relevancia para la fase de pruebas dado que se confirma que en ambos routers la instancia OSPF se esta ejecutándose de forma correcta haciendo que todos los routers del core puedan conocer las rutas de sus vecinos de red.

Los gráficos siguientes nos muestran todas las interfaces (en cada router) habilitadas para el protocolo OSPF. En el equipo PE01GYE, solo esta habilitada la interfaz G 1/0 que conecta al backbone.

Fig. 6-13.- Interfaces OSPF en el P01GYE

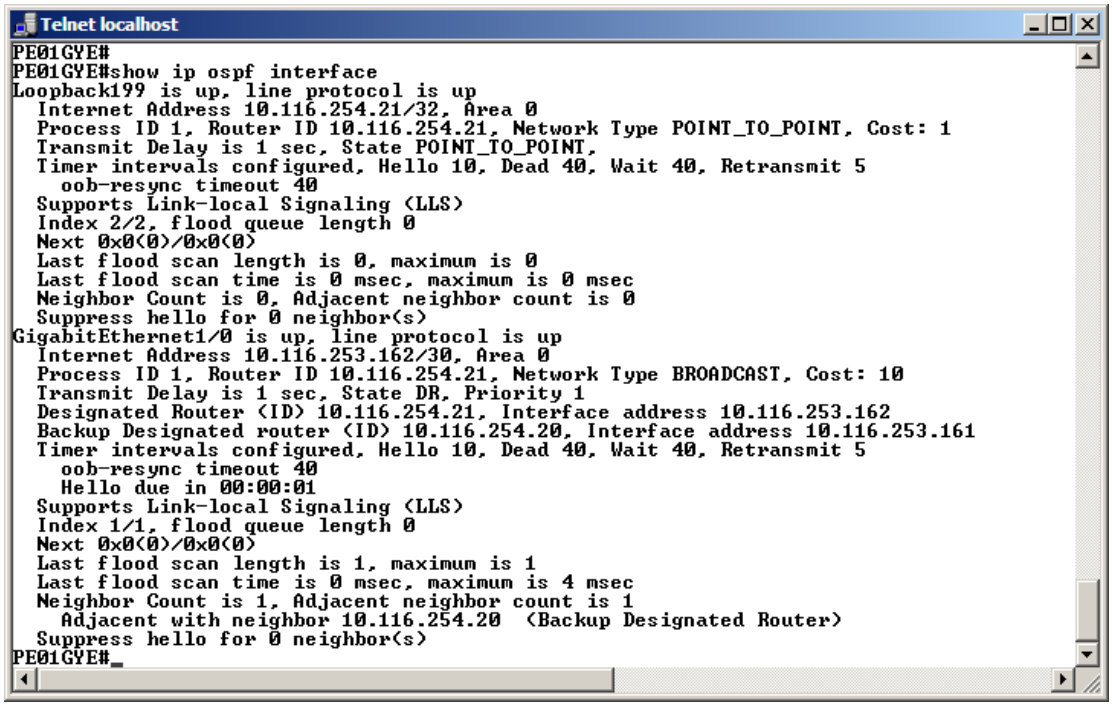


Fig. 6-14 Interfaces OSPF en el PE01GYE

Para finalizar la validación del protocolo OSPF, vamos a validar que los routers estén aprendiendo las rutas por medio del protocolo OSPF, esto lo hacemos ingresando en el modo global el comando ***"show ip route ospf"*** y se deben presentar las rutas aprendidas. A continuación presentamos los resultados obtenidos en el PE01GYE y P01GYE.

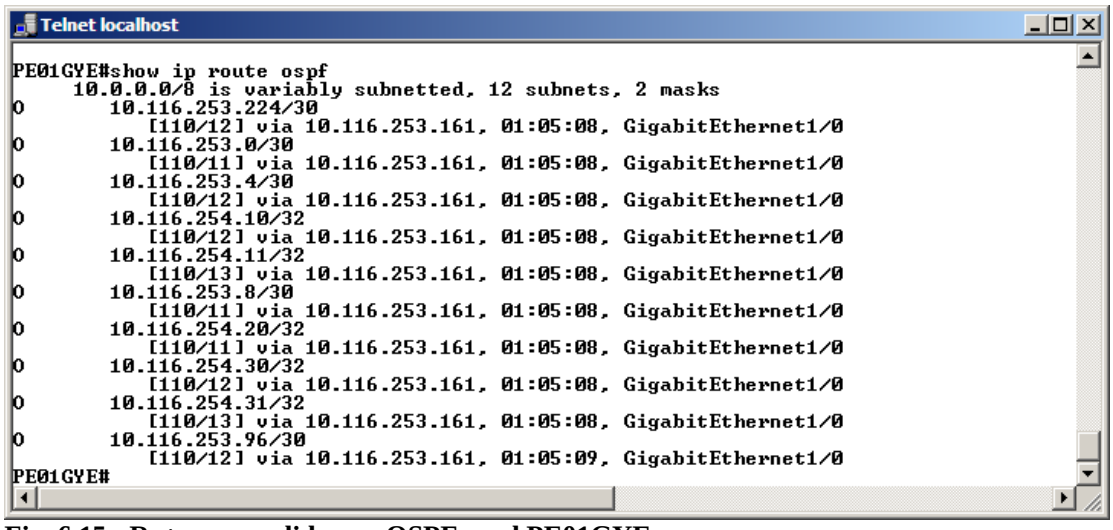


Fig. 6.15.- Rutas aprendida por OSPF en el PE01GYE

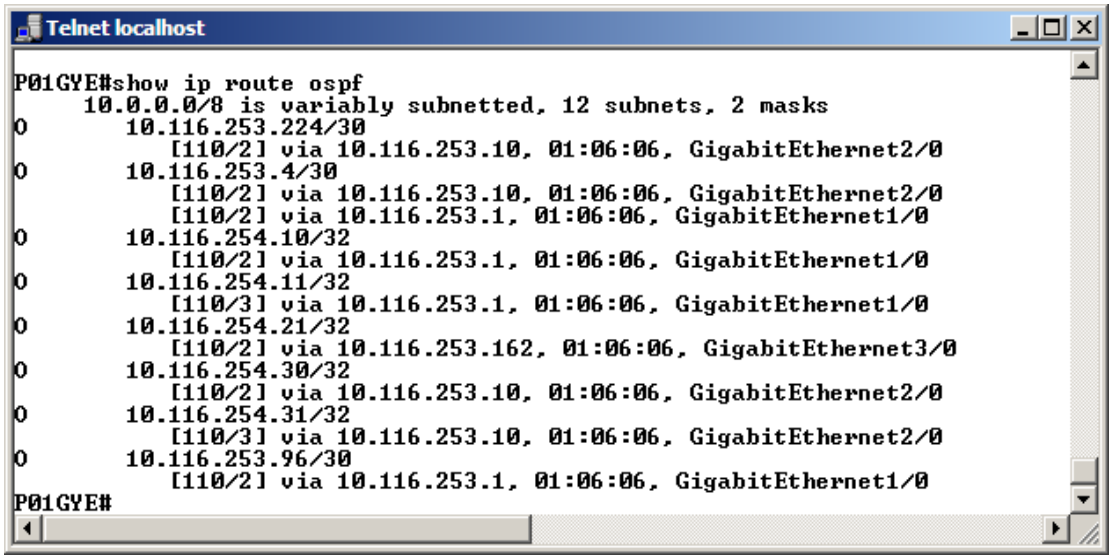


Fig. 6.16.- Rutas aprendida por OSPF en el P01GYE

6.2.4 BGP

Para establecer la comunicación BGP en nuestra red se optó por una configuración en Route Reflectors (reflejos de ruta). Los equipos PE establecen una sesión contra todos los P, quienes serán los encargados de transportar las rutas de los clientes (VPNv4) desde un PE hasta otro.

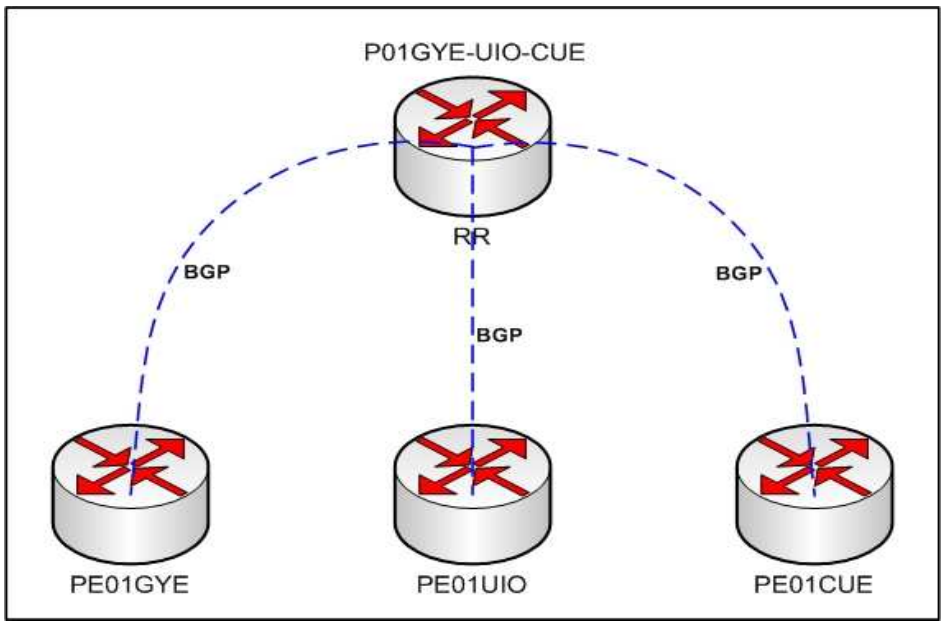


Fig. 6-17.- Configuración Route Reflectors.

El siguiente gráfico muestra mediante el comando ***"show ip bgp neighbors"*** la vecindad BGP existente entre el router P01GYE y el P01CUE (loopback 30):

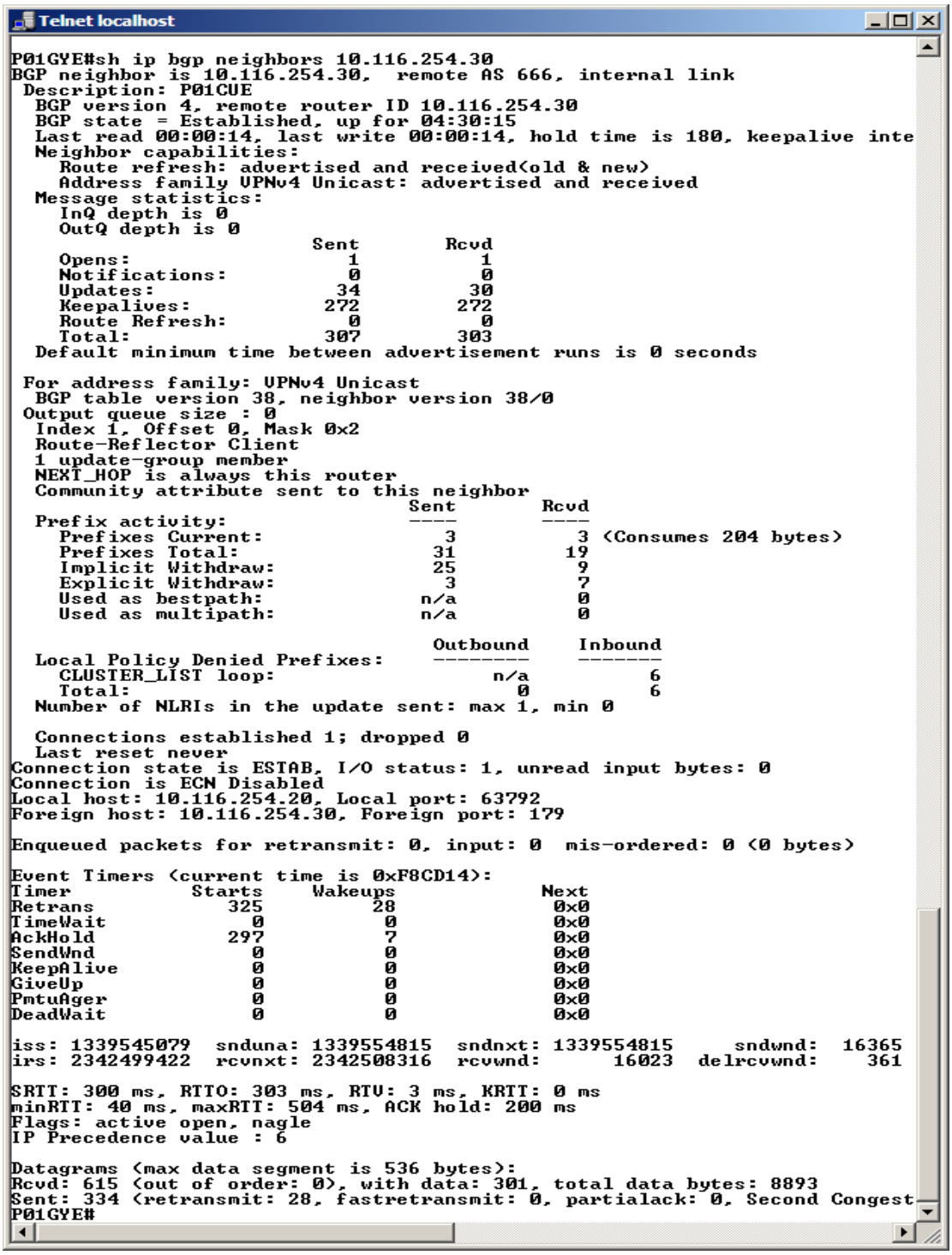


Fig. 6-18.- Vecindad BGP

Los siguientes dos gráficos validan el hecho de que tanto el PEGYE01 y el PE01UIO conozcan las redes del cliente con la etiqueta respectiva para la VPN, esto verifica que el protocolo MP-BGP esta funcionando correctamente.

Fig. 6-19 Rutas aprendidas por MP-BGP en PE01GYE

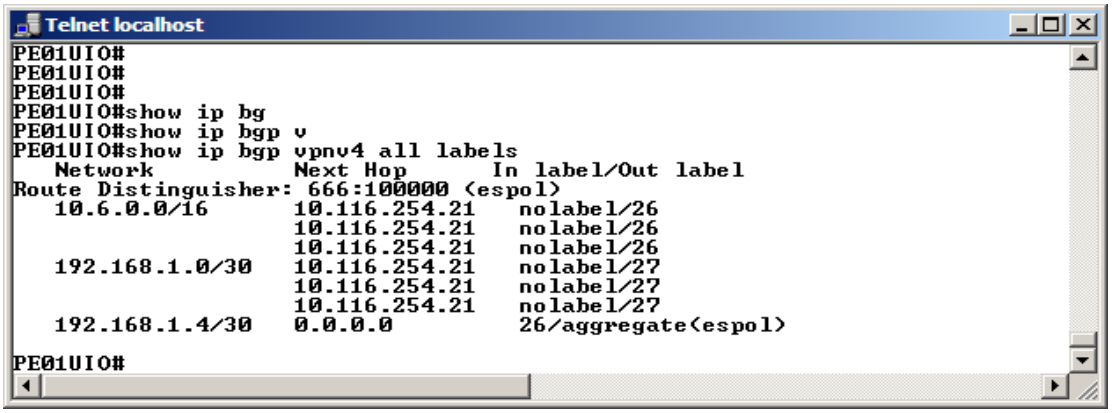


Fig. 6-20 Rutas aprendidas por MP-BGP en PE01UIO

Finalmente, presentamos el gráfico que el route reflector (P01GYE) ha aprendido del PE01GYE con quien ha iniciado una sesión MP-BGP a fin de las rutas del cliente sean propagadas a otros PE.

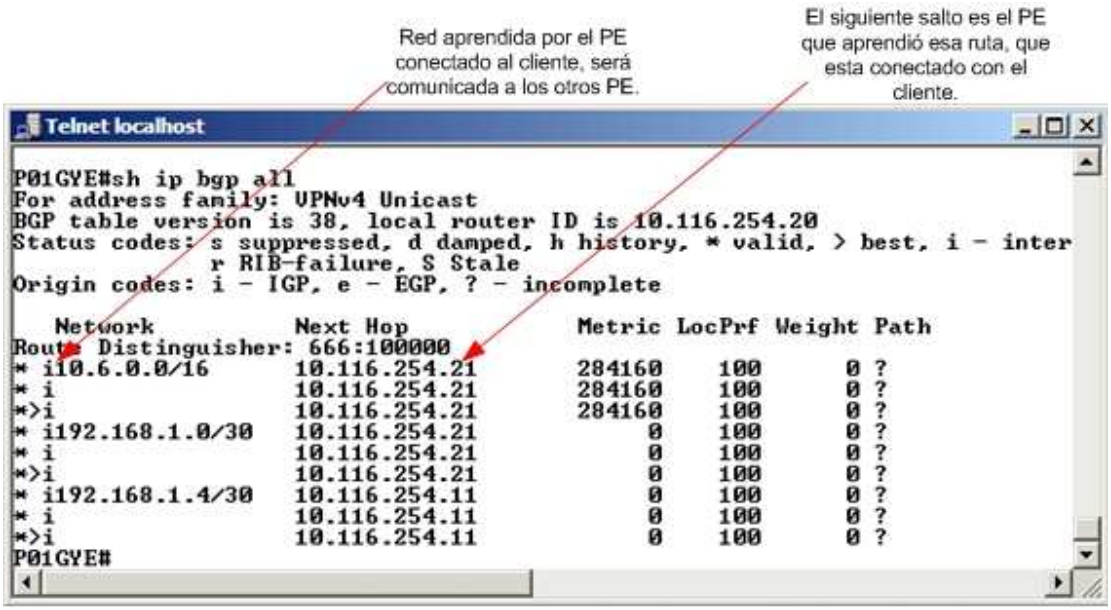


Fig. 6-21 Rutas aprendidas por MP-BGP en P01GYE

6.2.5 QoS

En este apartado se presenta la configuración de QoS: clases, políticas y aplicación en la interfaz respectiva tanto en el cliente (CE) como en el PE.

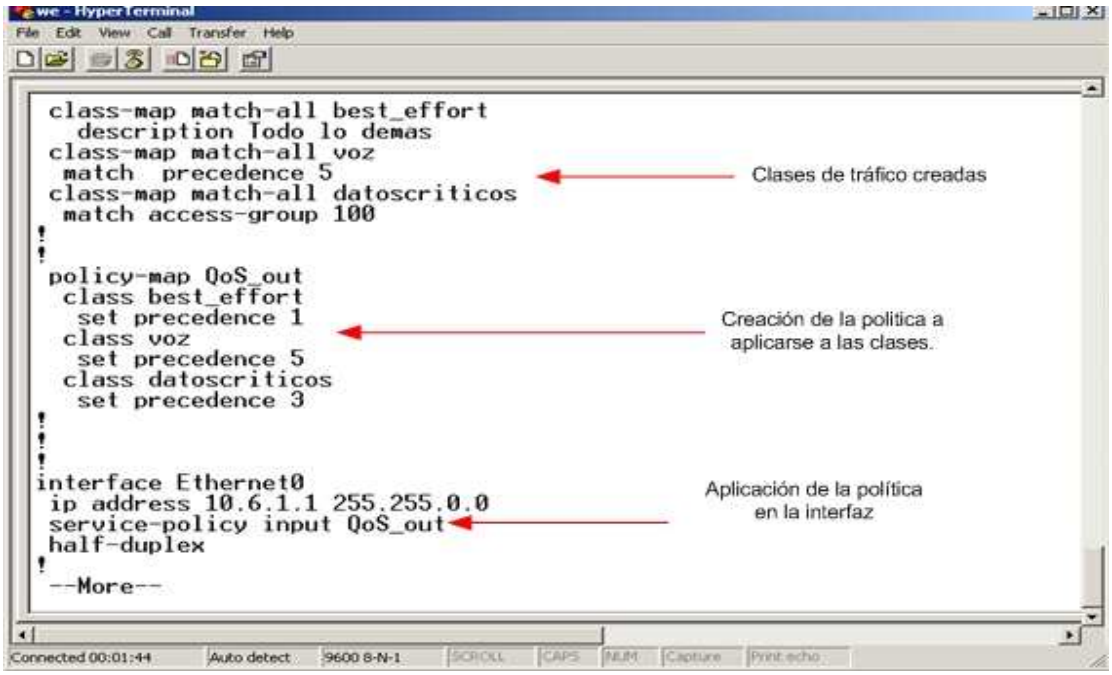


Fig. 6-22.- Creación de clases y políticas en el CE

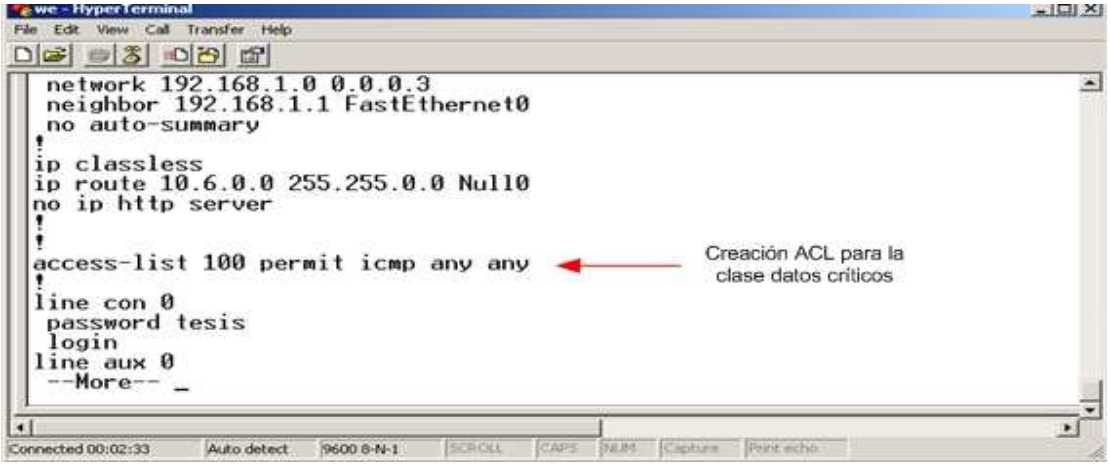


Fig. 6-23.- Access list creada para la clase datos críticos.

Al configurar QoS desde el equipo CE, garantizamos que la calidad de servicio será aplicada en todo el tramo de comunicación, es decir end-to-end.

Ahora, la forma en que estas políticas se aplican es de la siguiente forma:

1.- Cliente inicia transmisión de datos desde una oficina a otra, por citar un ejemplo, la necesidad de comunicación es un canal de comunicación VoIP entre sus oficinas.

2.- Al entrar este tráfico (que recae en la clase voz ya definida) en la interfaz del router que conecta a la red lan del cliente, esta interfaz aplica la política que ha sido definida para el tráfico entrante.

3.- El router del cliente, marca al paquete con el valor de IP precedente de 5, definido en la clase.

4.- El router PE al recibir este paquete marcado con IP precedente 5 le aplica la política definida y se la asigna el bit experimental 5 en la posterior etiqueta MPLS. Este proceso será comprobado en el análisis de tráfico de la red.

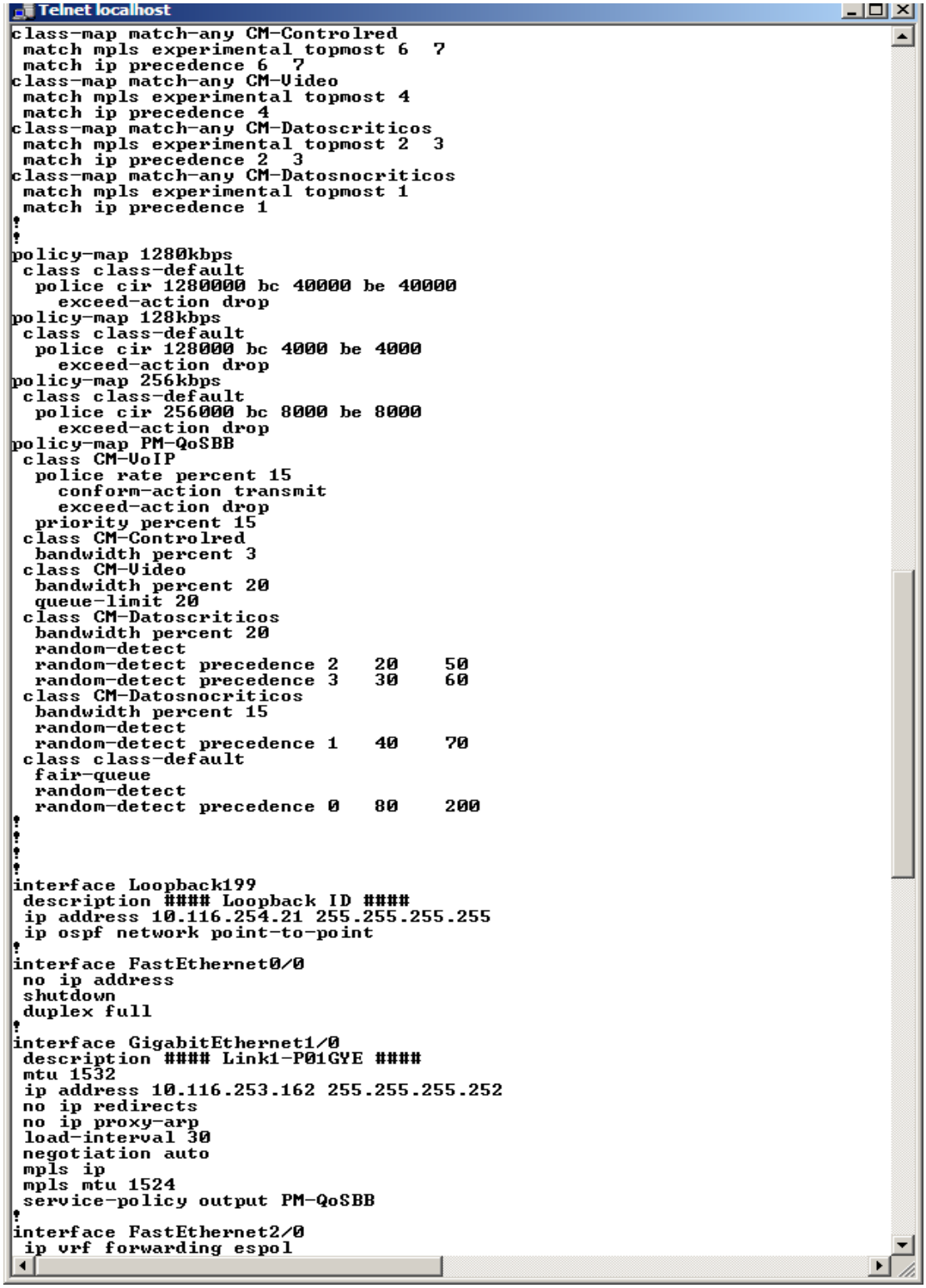


Fig. 6-24.- Aplicación de QoS en el PE01GYE

6.2.6 VPN - VRF

En esta sección se verificará la correcta configuración de la VRF creada para nuestro cliente "ESPOL" a fin de garantizar la comunicación entre sus oficinas en Guayaquil y Quito.

Como se ha descrito antes, las VRF son instancias virtuales que se crean en los routers PE a fin de "individualizar" la conexión a cada cliente re-utilizando el mismo equipo físico. El protocolo de enrutamiento escogido entre el PE y el CE ha sido EIGRP.

El siguiente comando "show ip vrf" nos devuelve las VRFs creadas en ese router. Como se puede apreciar, esta creada la VRF ESPOL con su respectivo RD y la interfaz a la que esta asociada.

Fig. 6-25.- show vrf PE01GYE

Fig. 6-26.- show vrf PE01UIO

El siguiente comando ***"show ip vrf interface"*** nos presenta la información de las interfaces asociadas a nuestra vrf.

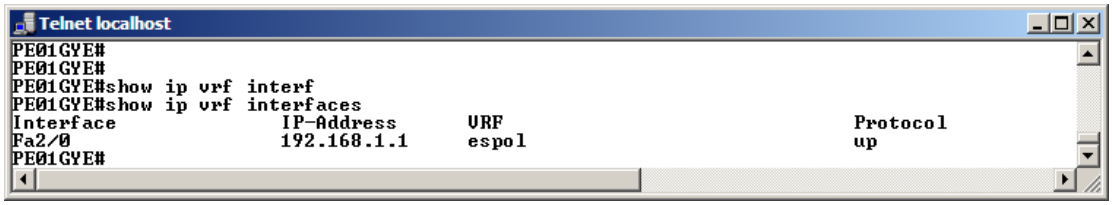


Fig. 6-27.- show vrf interfaces - PE01GYE

Fig. 6-28.- show vrf interfaces - PE01UIO

El comando ***"show ip protocol vrf espol"*** nos permite comprobar que el protocolo seleccionado EIGRP se esta ejecutando de forma correcta en nuestra vrf. Adicional, se comprueba una vez más el funcionamiento del protocolo MP-BGP.

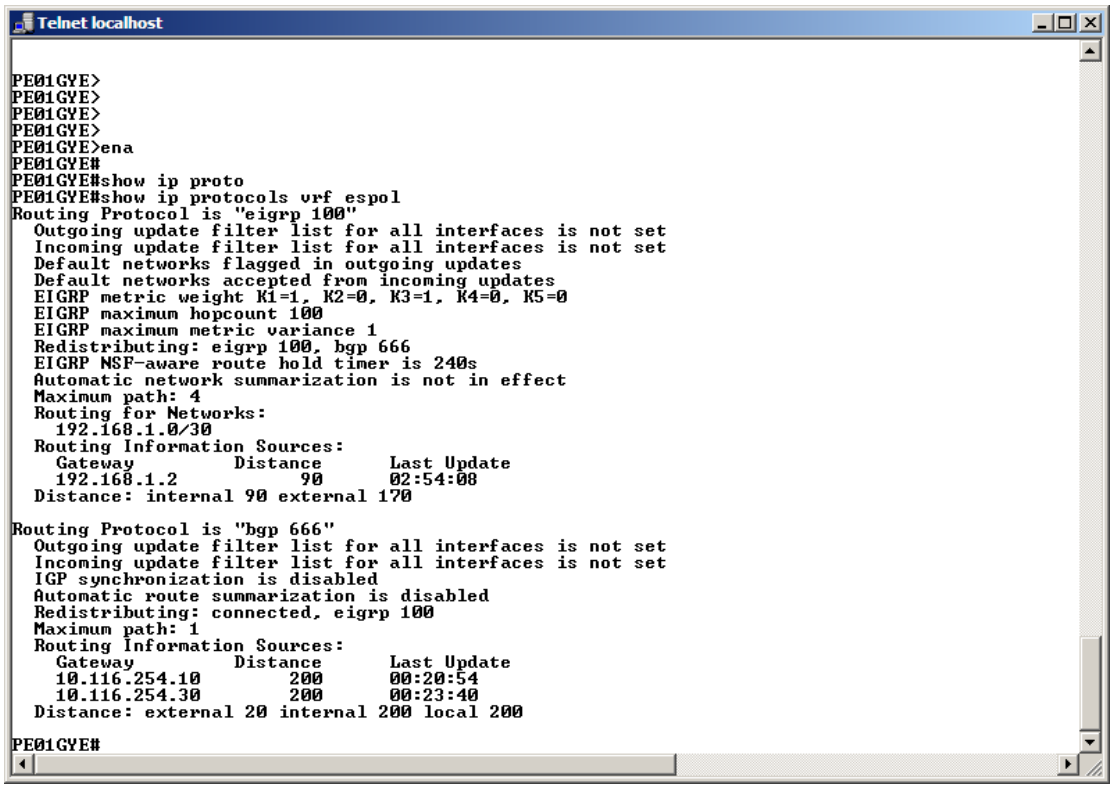


Fig. 6-29.- Protocolo de enrutamiento en la VRF - PE01GYE

Ahora presentamos la tabla de enrutamiento dentro de la VRF, esta se muestra mediante el comando ***"show ip route vrf espol"*** donde se puede apreciar las rutas aprendidas por EIGRP del cliente directamente conectado y las rutas aprendidas BGP de la sucursal remota.

Fig. 6-30.- Tabla de enrutamiento VRF

6.3 Verificación del flujo de información.

Esta es sin dudas, la prueba final y más completa que verifica el funcionamiento de nuestra red MPLS. Hasta ahora hemos visto que los protocolos configurados funcionan correctamente, los equipos están aprendiendo las rutas de los demás y que las interfaces están activadas sin problemas, solo resta confirmar que la red diseñada haga lo que se ha prometido al cliente que hará:

1.- Comunicar sus sucursales mediante una VPN sobre una red MPLS.

2.- Dar el tratamiento respectivo acordado (QoS) a su tráfico durante su transmisión.

A continuación presentamos el esquema final de red, incluyendo los equipos del cliente (CE), desarrollado para la realización de estas pruebas:

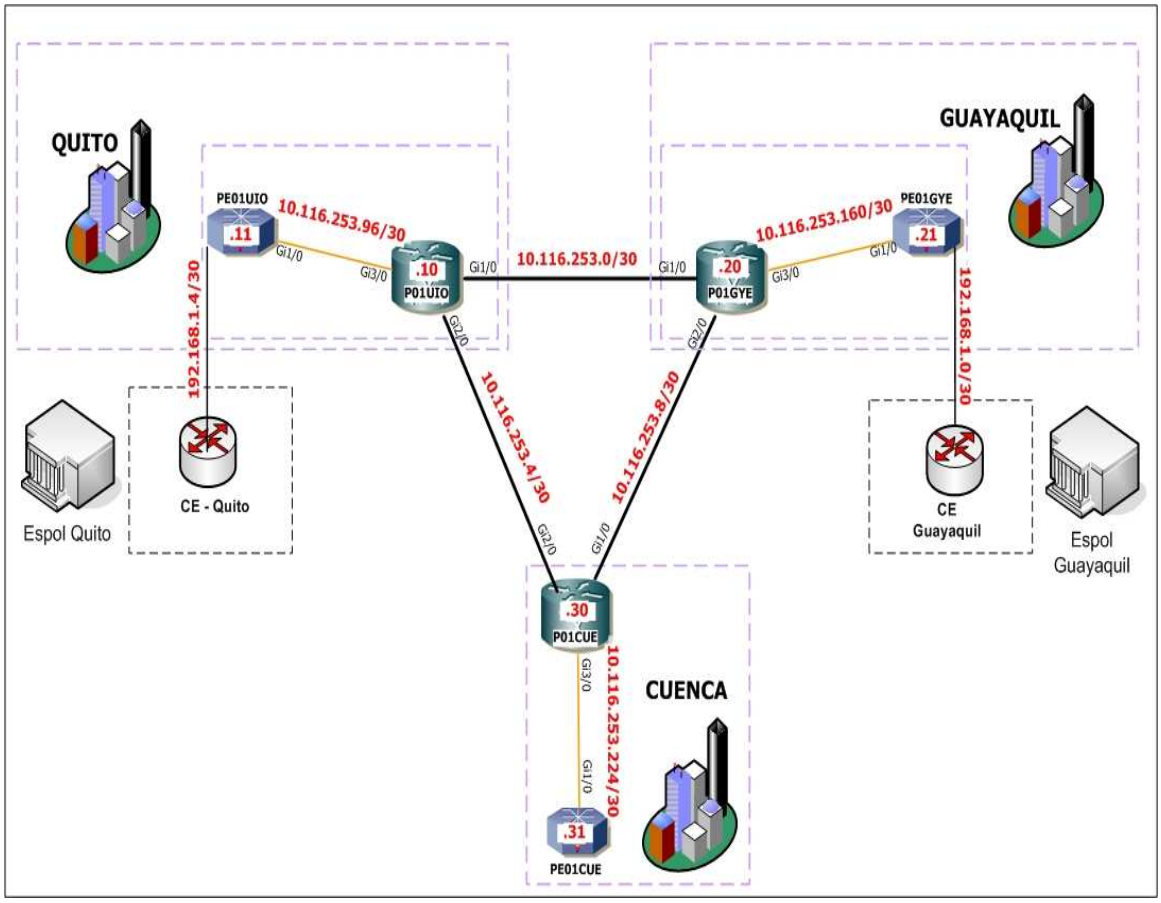


Fig. 6-31.- Esquema de red con cliente.

6.3.1 Pruebas de conectividad: IMCP, TRACERT y TELNET

Lo primero que vamos a confirmar es la conectividad, lo haremos utilizando las siguientes herramientas:

- IMCP: Pruebas de ping
- Tracert
- Telnet

A continuación presentamos los resultados de estas pruebas con resultados exitosos:

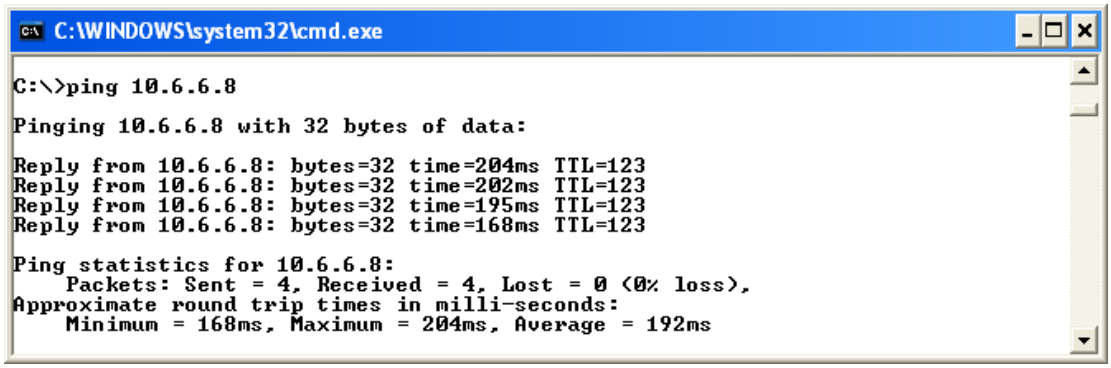


Fig. 6-32.- Pruebas de ping entre las localidades del cliente.

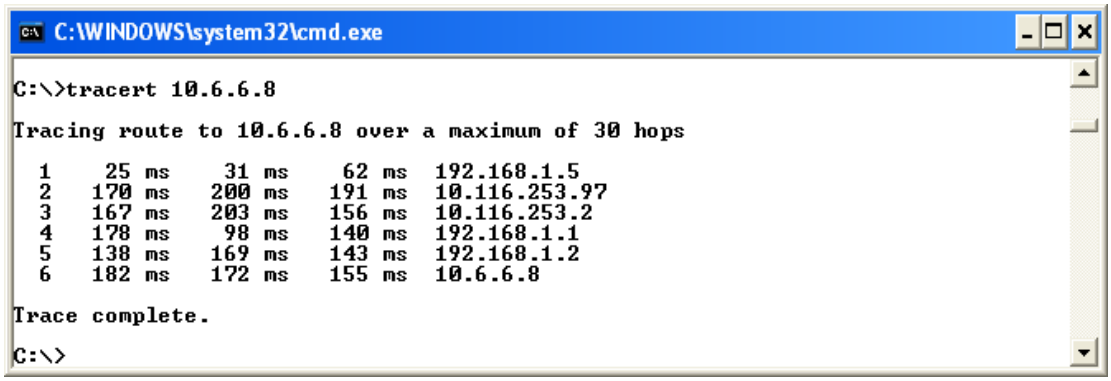


Fig. 6-33.- Pruebas de tracert desde Quito a Guayaquil.

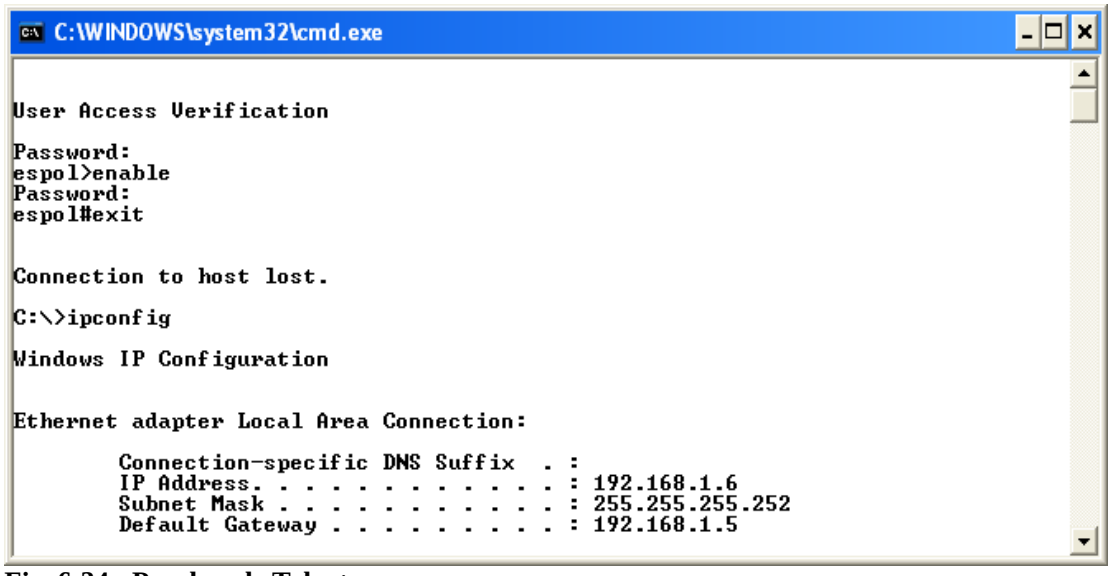


Fig. 6-34.- Pruebas de Telnet

6.3.2 Etiquetas (túnel LDP) y QoS

Para esta prueba, se configuró lo siguiente:

1.- Se habilitó la aplicación netmeeting de Microsoft en los computadores del cliente. Uno conectado en Guayaquil y el otro en Quito. Este tráfico tiene prioridad VOZ (bit exp 5).

2.- Se aplicó en el cliente la calidad de servicio Datos Críticos, donde para efectos de pruebas, se permitió el tráfico ICMP y se lo priorizó con bit experimental 3.

3.- Se realizó una llamada entre Guayaquil y Quito y se inundó la red con un ping de 1400bytes extendido.

Al realizar las pruebas, se capturó el tráfico que recorre la red e iremos estudiando sus etiquetas mediante el programa analizador de tráfico wireshark comparando los resultados con la tabla LFIB de cada equipo.

Análisis de resultados:

1.- Se muestra la tabla FIB del PE01GYE donde se muestra la etiqueta de la VPN, esta será la segunda etiqueta que transportará nuestra red, pues como vimos anteriormente para transportar vpn se requieren de 2 etiquetas:

- La etiqueta que se aprende por LDP y marca el LDP a seguir.
- La etiqueta que se aprende por MP-BGP y solo se intercambian entre PEs para poder enlutar dentro de las VRF de los clientes.

Esta segunda etiqueta se muestra en esta tabla, donde la **etiqueta 26** es la que sirve para enrutar en el PE de Quito y la 27 en el PE de Guayaquil.

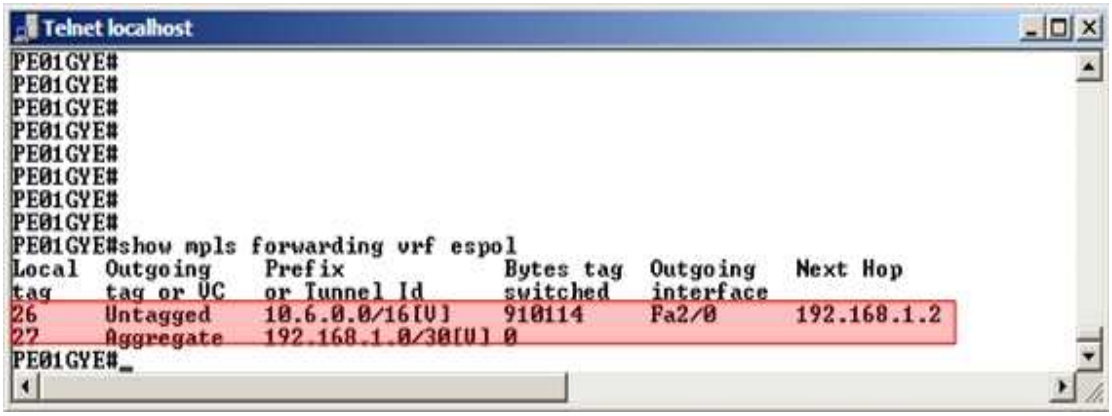


Fig. 6-35.- Etiqueta VPN

2.- Se muestra la tabla LFIB del router PE01GYE, equipo que recibe los paquetes IP sin etiquetar de voz e IMCP del el equipo del cliente en Guayaquil que van dirigidos mediante una VPN a la sucursal en Quito conectado al PE01UIO con **loopback 11**. En esta tabla se ha sombreado la línea correspondiente al paquete que va enrutado desde Guayaquil hasta Quito.

Se observa que para ese paquete la etiqueta con la que enviará al paquete hacia el siguiente salto es la **etiqueta 20** y el siguiente salto será el router P01GYE con dirección **10.116.253.161** por la interfaz Giga 1/0.

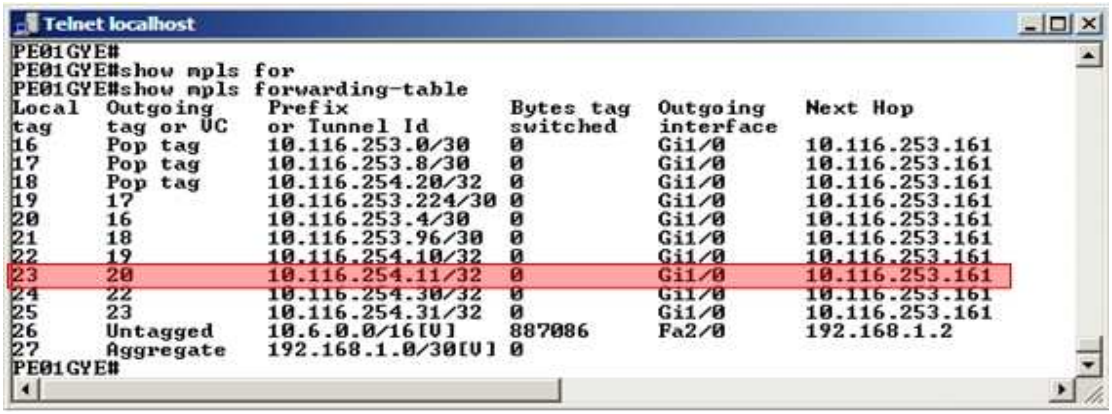


Fig. 6-36 Tabla LFIB en PE01GYE

Esto es comprobado mediante la captura del tráfico entre el PE01GYE y el P01GYE que se presenta a continuación:

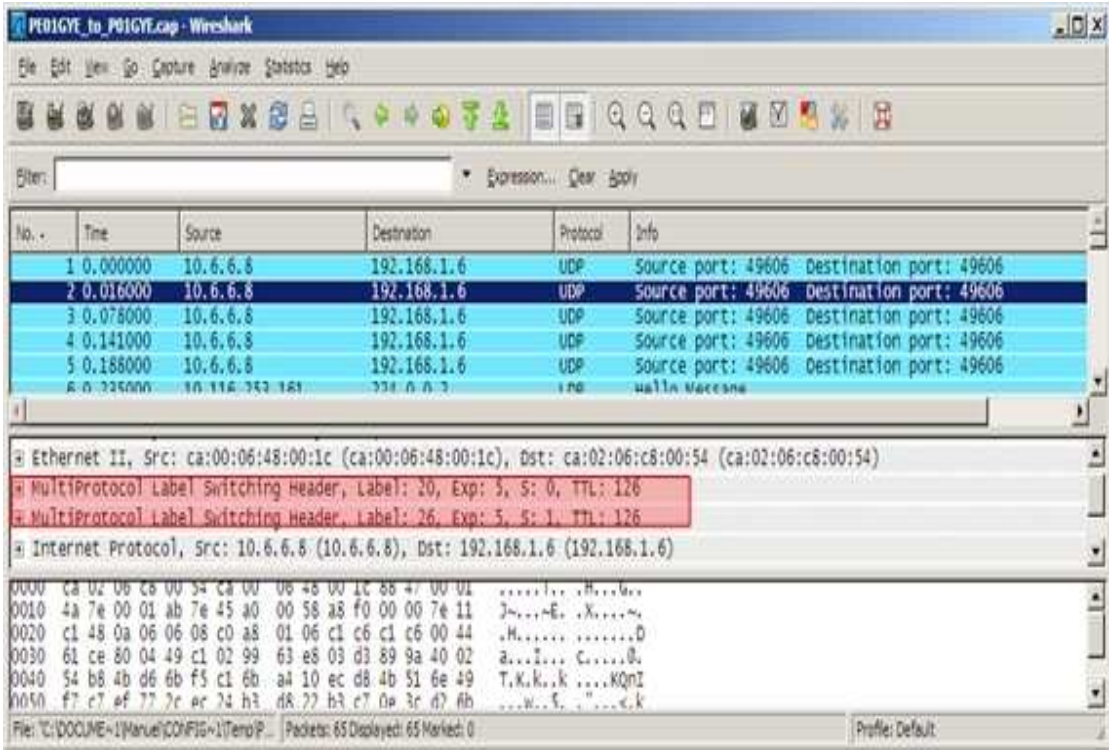


Fig. 6-37.- Captura de tráfico PE01GYE – P01GYE

De este gráfico verificamos lo siguiente:

La etiqueta para elaborar el túnel LDP es la número 20 como se había previsto y que la segunda etiqueta, de la VPN, es la número 26 como se había demostrado anteriormente.

Adicionalmente, podemos validar que el bit de pila (stack) esta seteado de forma correcta: 0 para la etiqueta top y 1 para la segunda etiqueta. Finalmente, comprobamos que este paquete de VOZ esta priorizado con el bit experimental 5 como se esperaba que aconteciera.

3.- Se presenta la tabla LFIB del equipo P01GYE quién recibe el trafico etiquetado que proviene del PE01GYE dirigido hacia el PE01UIO, podemos observar que **recibe el paquete con la**

etiqueta 20 y la intercambia con la etiqueta 19 y lo enviará por medio de la interfaz G.1/0 al siguiente salto que será el P01UIO con la ip 10.116.253.1

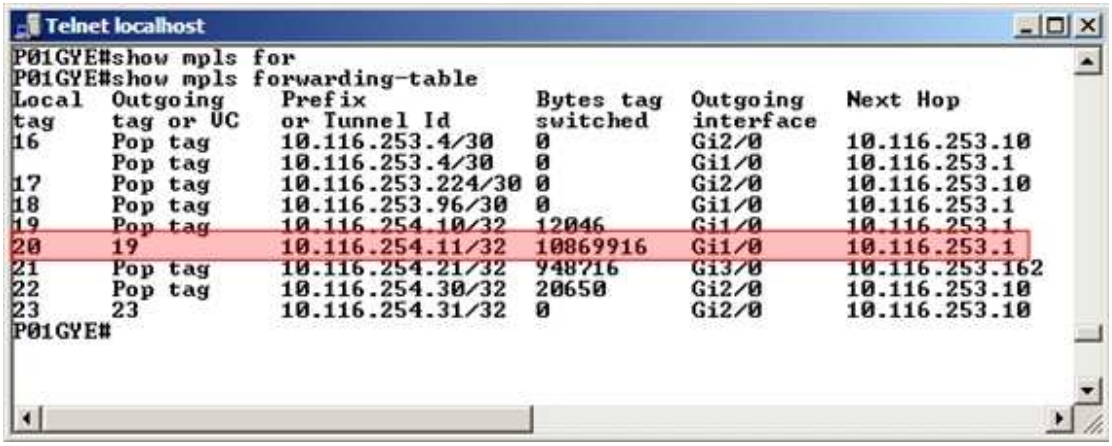


Fig. 6-38 Tabla LFIB en P01GYE

En el siguiente gráfico presentamos el tráfico capturado entre el PE01GYE y el P01GYE, de esta captura podemos comprobar lo que se había comentado anteriormente:

- ✓ El paquete fue enviado con la nueva etiqueta de túnel LDP 19
- ✓ Mantiene la etiqueta 26 de la VPN
- ✓ Como es tráfico de voz, tiene bit exp 5
- ✓ Como tiene una pila de etiquetas, el bit S esta seteado de forma correcta: 0 para la etiqueta LDP y 1 para la etiqueta de la VPN.

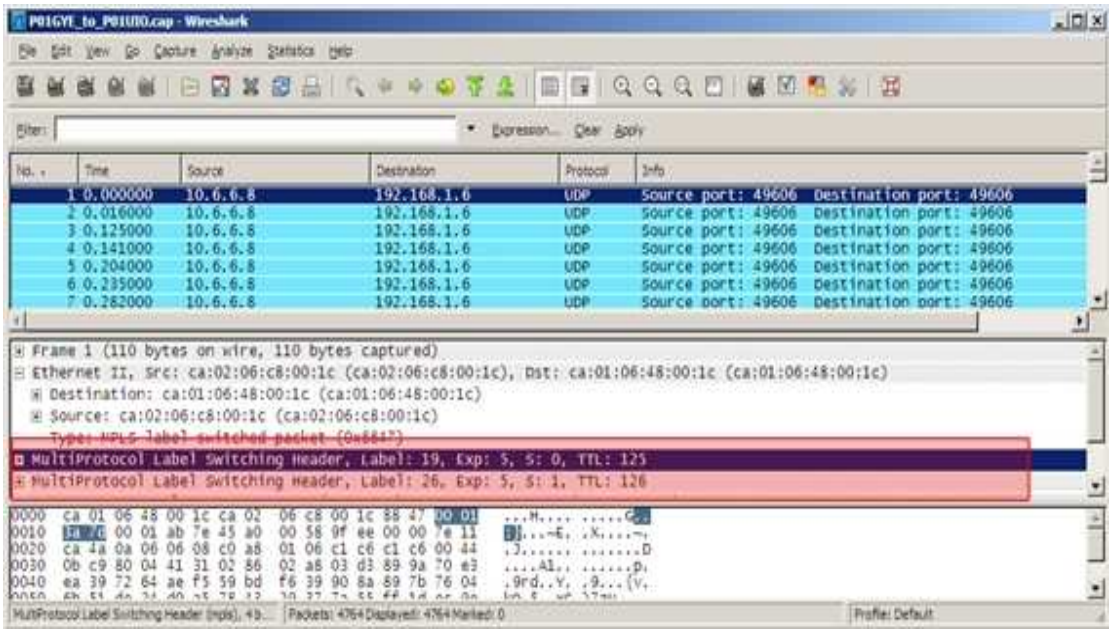


Fig. 6-39.- Captura de tráfico P01GYE – P01UIO

4.- En el gráfico a continuación presentamos la tabla LFIB del equipo P01UIO, este equipo **recibe el paquete con la etiqueta 19** proveniente del P01GYE y según su tabla LFIB deberá intercambiarlo por la siguiente etiqueta que lo lleve a su siguiente salto. Sin embargo, notamos que la acción que realiza este equipo no es colocarle una nueva etiqueta (y reemplazar la anterior) sino que realiza un ***"POP TAG***, es decir **RETIRA LA ETIQUETA LDP** dejando únicamente a la etiqueta 26 que corresponde a la VPN.

Esta acción es congruente con lo que se había descrito en el capítulo 2 en la técnica del PHP (penultimate hop popping) que básicamente lo que hace es retirar la etiqueta del túnel LDP conociendo que el siguiente vecino LDP es ya el último salto del túnel. Con esta acción, lo único que se logra es evitar que el PE01UIO realice una búsqueda adicional, dado que ya no tendrá etiqueta del túnel LDP, no deberá buscar en la tabla LFIB sino solamente en la tabla FIB dentro de la VRF para lograr el enrutamiento hacia el CE del cliente en Quito.

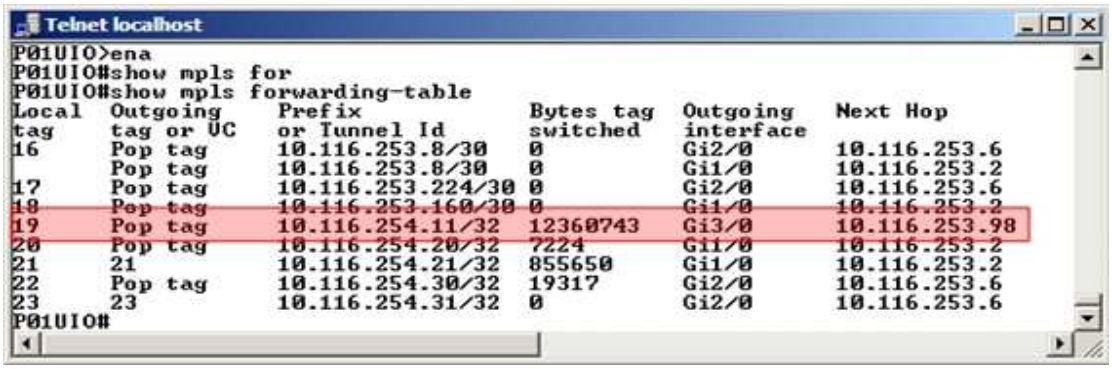


Fig. 6-40 Tabla LFIB en P01UIO

Lo que hemos descrito en el gráfico anterior, lo podemos verificar gracias a la captura de tráfico realizada entre en el P01UIO y el PE01UIO, donde se puede apreciar lo siguiente:

- Una sola etiqueta, la 26 perteneciente a la VPN.
- El bit S (stack) esta correctamente seteado en 1.
- Mantiene la prioridad de tráfico de voz (bit exp 5)

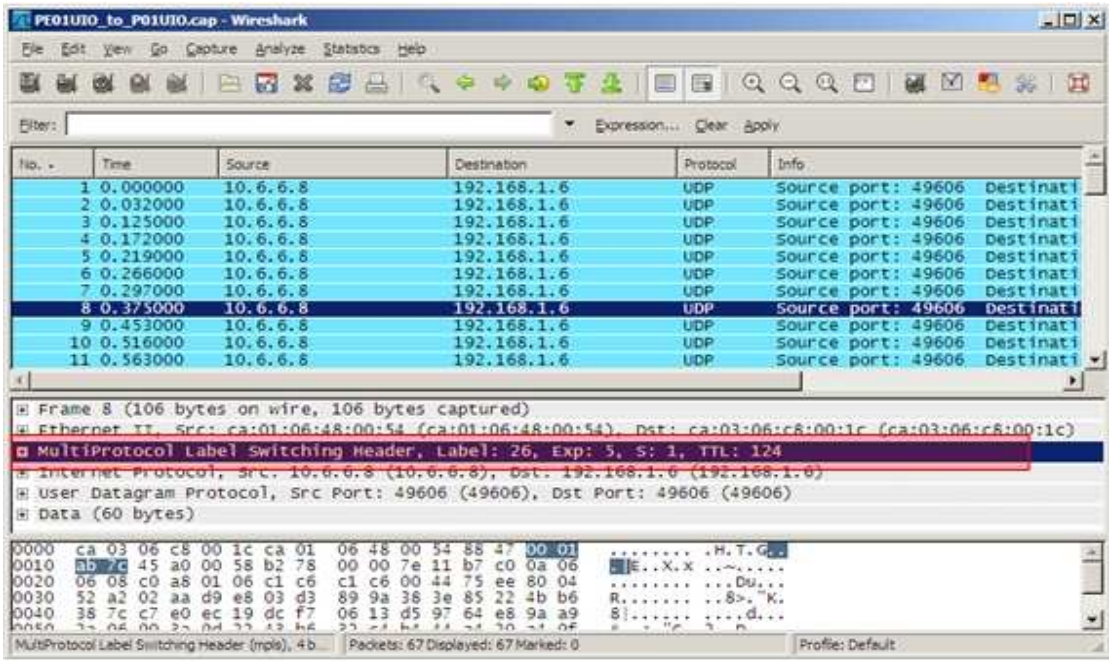


Fig. 6-41.- Captura de tráfico P01UIO – PE01UIO

5.- En la parte final de las pruebas, presentamos los gráficos de del equipo PE01UIO, las tablas LFIB y FIB para verificar el correcto manejo de las etiquetas.

Observamos en la tabla LFIB que el paquete recibido desde el P01UIO aparece con la etiqueta 26, lo cual concuerda con lo expuesto en la captura de tráfico anterior donde vimos que solo tenían una etiqueta, la 26, en lugar de las 2 que traían desde el PE01GYE y esto debido al PHP aplicado.

De esta LFIB podemos ver que la etiqueta 26 esta asociada con la ruta que conecta al PE01UIO con el cliente (192.168.1.4/30) y que NO tiene siguiente salto, lo cual indica que el siguiente salto deberá ser buscado en la tabla FIB dentro de la VRF. Con esto finaliza la prueba y se valida que la conectividad, el túnel LDP y el QoS esta correctamente aplicado de extremo a extremo en nuestra red.

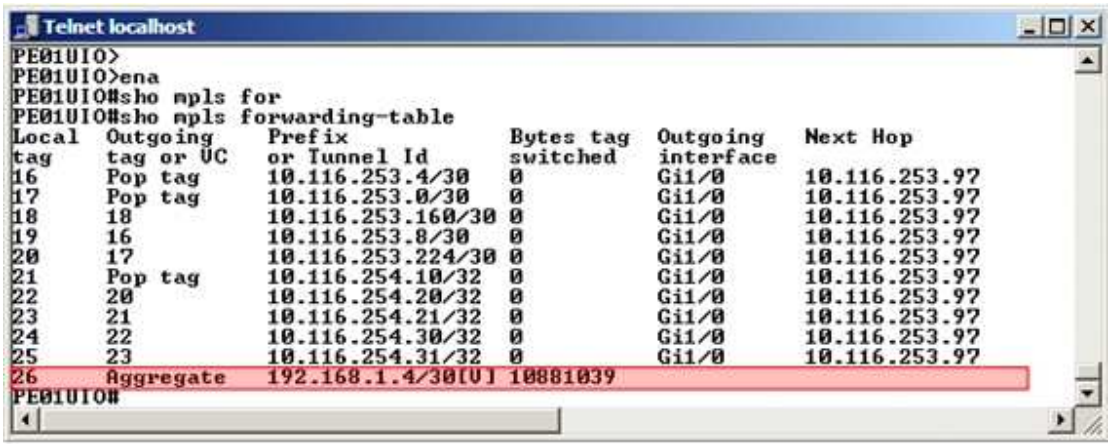


Fig. 6-42 Tabla LFIB en PE01UIO

CAPITULO VII

Diseño de la red

ANALISIS DE COSTOS

7.1 Equipos Activos

En esta sección procederemos a describir uno a uno los ítems necesarios para la implementación de la red propuesta. En esta primera parte, exponemos los costos de los equipos de red o equipos activos descritos anteriormente.

7.1.1 Equipos Cisco 7206VXR

Para calcular los costos de la adquisición de los ***6 equipos CORE de nuestra red***, hemos cotizado los siguientes componentes directamente de la lista de precios global de Cisco para Latinoamérica o GLP Latam.

Luego, considerando empresas locales que tienen la representación de Cisco en el Ecuador y son de categoría GOLDPARTNER se cálculo al máximo margen de descuento que este tipo de proveedores pueden ofrecer en comparación de la GLP. Los componentes que se cotizaron fueron:

- ✓ Chasis Cisco 7206VXR con NPE-G2 (módulo de procesamiento)
- ✓ Doble fuente redundante de alimentación
- ✓ Tarjeta de 3 puerto ópticos (para la conexión con los ADMs)
- ✓ Soporte Smartnet 24x7x4 (soporte posventa de Cisco con tiempo de respuesta de 4 horas para cambio de partes dañadas por 3 años)

Valor por Unidad tomado de la GLP de Cisco

Product	Description	Quantity	List Price	Price
7206VXR/NPE-G2	7206VXR with NPE-G2 includes 3GigE/FE/E Ports and IP SW	1	24000	24,000.00
PWR-7200	Cisco 7200 AC Power Supply Option	1	0	0
PWR-7200/2	Cisco 7200 Redundant AC Power Supply Option (280W)	1	3000	3,000.00
CAB-AC	Power Cord,110V	2	0	0
S72PZK91-12231SB	Cisco 7200 NPE G2/7201 IOS Series SERVICE PROVIDER/SSH 3DES	1	750	750
SFP-GE-S	1000BASE-SX SFP (DOM)	3	550	1,650.00
NPE-G2	7200 series NPE-G2 engine with 3 GE/FE/E ports	1	19000	0
MEM-NPE-G2-1GB	7200 Series NPE-G2 1GB Memory	1	0	0
MEM-NPE-G2-FLD256	Cisco 7200 Compact Flash Disk for NPE-G2, 256 MB	1	0	0
CON-SNTP-7206VXRN	SMARTNET 24X7X4 7206VXR with NPE-G2	1	7278	21,834.00

Total Price: USD 51,234.00

Valor por Unidad considerando el máximo descuento ofrecido por un GOLDPARTNER de Cisco

Product	Description	Quantity	Discount	Price
7206VXR/NPE-G2	7206VXR with NPE-G2 includes 3GigE/FE/E Ports and IP SW	1	41%	14,160.00
PWR-7200	Cisco 7200 AC Power Supply Option	1	0	0
PWR-7200/2	Cisco 7200 Redundant AC Power Supply Option (280W)	1	41%	1,770.00
CAB-AC	Power Cord,110V	2	0	0
S72PZK91-12231SB	Cisco 7200 NPE G2/7201 IOS Series SERVICE PROVIDER/SSH 3DES	1	41%	442.5
SFP-GE-S	1000BASE-SX SFP (DOM)	3	41%	973.50
NPE-G2	7200 series NPE-G2 engine with 3 GE/FE/E ports	1	41%	0
MEM-NPE-G2-1GB	7200 Series NPE-G2 1GB Memory	1	0	0
MEM-NPE-G2-FLD256	Cisco 7200 Compact Flash Disk for NPE-G2, 256 MB	1	0	0
CON-SNTP-7206VXRN	SMARTNET 24X7X4 7206VXR with NPE-G2	1	41%	12,882.06

Total Price: USD 30,228.06

Valor total de los 6 equipos Cisco 7206VXR

Product	Description	Quantity	Discount	Price
7206VXR/NPE-G2	7206VXR with NPE-G2 includes 3GigE/FE/E Ports and IP SW	6	41%	84,960.00
PWR-7200	Cisco 7200 AC Power Supply Option	6	0	0
PWR-7200/2	Cisco 7200 Redundant AC Power Supply Option (280W)	6	41%	10,620.00
CAB-AC	Power Cord,110V	12	0	0
S72PZK91-12231SB	Cisco 7200 NPE G2/7201 IOS Series SERVICE PROVIDER/SSH 3DES	6	41%	2655
SFP-GE-S	1000BASE-SX SFP (DOM)	18	41%	17,523.00
NPE-G2	7200 series NPE-G2 engine with 3 GE/FE/E ports	6	41%	0
MEM-NPE-G2-1GB	7200 Series NPE-G2 1GB Memory	6	0	0
MEM-NPE-G2-FLD256	Cisco 7200 Compact Flash Disk for NPE-G2, 256 MB	6	0	0
CON-SNTP-7206VXRN	SMARTNET 24X7X4 7206VXR with NPE-G2	6	41%	77,292.36

Total Price: USD 181,368.36

7.1.2 Equipos Huawei OPTIX OSN 3500

La totalidad de puntos de repetición donde se ha considerado colocar equipos ADM en nuestro diseño llega a la cantidad de 18 estaciones. Cabe recordar, que estos equipos además de amplificar la señal óptica que circula por la fibra conectada, sirve para que en futuras planeaciones se pueda "romper" el anillo óptico y colocar equipos de agregación de cliente pudiendo ser equipos de Core como PEs o simples switches que permitan crear puntos de acceso a nuestra red en cada una de las ciudades por las que nuestra red de fibra transita sin necesidad de mayores cambios en el tendido físico de la red.

Se ha considerado los precios del fabricante Huawei, quién dispone de representación localm sin contemplar descuento alguno sobre su lista de precios. Los componentes más relevantes que se cotizaron fueron:

- ✓ Sistema de control de capacidad de 1STM-1. (Capacidad inicial de la red)
- ✓ Doble fuente redundante de alimentación
- ✓ Tarjeta de Procesamiento de servicio con capacidad de 63xE1.

Valor Total de los 18 equipos ADM

Product	Description	Quantity	Price per Unit	Total Price
Optix OSN 3500		18		
SS-EOW-3500	Engineering Order Wire Board	18	147.05	2646.9
SS-AUX-3500-R1	System Auxiliary Interface Board	36	235.41	8,474.76
SS-PIU-3500	Power Interface Board	36	22.9	824.4
SS-CXL1 (l-1 LC)-Q2	STM-1 System Control, Cross-connect optical board	36	1611.88	58027.68
SS-PQ1(75)	Service Processing Board (75 ohm)	36	745.23	26828.28

Total Price: USD 98,217.18

7.2 Equipos Pasivos

En esta segunda parte, procedemos a detallar los costos de los equipos pasivos de la red. Que son aquellos equipos que pertenecen a una red y que no necesitan energía eléctrica para realizar su funcionamiento.

7.2.1 Fibra óptica y conectores

Para obtener el costo de la fibra óptica con la que realizamos el estudio, se procedió a contactar a unos de los fabricantes vía correo electrónico, los cuales nos informaron del valor por metro cuando se adquieren mas de 10.000 mts. Este Fabricante de nombre PRYSMIAN no solo fabrica las fibras si no que a su vez distribuye conectores tipos LC que son los que vamos a utilizar.

Valor del cable de Fibra y Conectores

Product	Description	Quantity	Discount	Price
Fibra Optica	Fibra Optica Headrow (Prysmian) 48 hilos	1289 KM	10	12890
Conector	Patch cord FC/PC, LC/PC, single mode, 2mm	36 u	14.31	515.16
EMPALMES	Cajas de empalmes de 48 Fibras para arquetas	331 u	150	49650
	Total : 63055.16			

7.2.2 Rack y accesorios

Los precios de los Rack y accesorios necesarios para el levantamiento de este sistema fueron consultados con distribuidores nacionales, este precio que detallamos a continuación correspondes a equipos de marca QUEST.

Valor de Equipos Pasivos

Product	Description	Quantity	Discount	Price
RACK DE PISO	RACK 2.16 Mts Alto X 0.254 Mts. X 0.152 Mts. Profundidad (Queso)	18 U	250	4500
GABINETE	Gabinete Puerta de vidrio 2 Mts Alto X 0.6 Mts Ancho X 0.4 Mts. (Queso)	18 u	320	5760
PANEL DISTRIBUCION	Cajas para Distribución de fibras	36 u	400	14400
POTECCION	Placa protectora de cajas de conexiones	36 u	25	900
ELECTROCANALES	Bandejas metálicas para tendido de cables x 2 mts	54 u	50	2700
	Total : 28260			

7.3 Infraestructura Civil

La parte civil de nuestro proyecto involucra la construcción de cuartos de 18 MT2 para alojamiento de los Equipos de Telecomunicaciones que se levantaran en cada una de las ciudades de las 18 ciudades que hemos llamado Nodos de Regeneración.

Además involucra la realización de las zanjas con maquinaria pesada implementadas con cierras que perforan el concreto o cemento de las carreteras. Se Plantea utilizar 6 frentes 2 maquinarias que parten por diferente ruta de cada nodo principal llámese así a Guayaquil – Quito – Cuenca

OBRA CIVIL

Product	Description	Quantity	Discount	Price
CUARTOS DE EQUIPOS	Construcción de cuarto 18 mt2	18 u	4000	72000
ARQUETAS	Arquetas plásticas + tuberías y tapa de fundición	331u	40	13240
MAQUINARIAS	Alquiler maquina zanjadora 6 frentes x días	30	900	27000

Total : 112240

7.4 Equipos de Alimentación y Protección

EQUIPOS DE ALIMENTACION Y PROTECCION				
Product	**Description**	**Quantity**	**Discount**	**Price**
Generadores	Generador 12 kva	18	2500	45000
Malla tierra	Malla de puesta a tierra	18	300	5400
Ups	Banco de baterías	18	350	6300
Rectificador	Rectificador 60 a.	18	180	3240
	Total : 59940			

7.5 Equipos de Climatización

EQUIPOS DE CLIMATIZACION				
Product	**Description**	**Quantity**	**Discount**	**Price**
AIRE ACOND	AIRE ACONDICIONADO 1800 BTU	18	700	12600
				12600
	Total : 12600			

7.6 Cuadro Total de Costos

Red Lógica	Precio Unitario	Cantidad	Total
Equipos de Networking	30,228.06	6 u	181,368.36
Equipos MUX	5,456.51	18 u	98,217.18
Red Física	**Precio Unitario**	**Cantidad**	**Total**
Tendido de Fibra	48.92	1289Km	63,055.16
Rack y Accesorios	1,570.00	18 u	28,260.00
Obra Civil	6,235.56	18 u	112,240.00
Alimentación y Protección	3,330.00	18 u	59,940.00
Climatización	700.00	18 u	12,600.00
		TOTAL	USD$ 555,680.70

Conclusiones y Recomendaciones

Conclusiones

- ✓ La ruta seleccionada para el tendido de fibra tiene como puntos o nodos principales Guayaquil- Quito – Cuenca y la trayectoria que une estos nodos cruzan por las ciudades más importantes a lo largo de la ruta donde se instalaran equipos ADM para regeneración de señal e incursión de futuros clientes a la red, El total de recorrido del anillo de fibra es de 1289 Km. e involucra el levantamiento de 18 estaciones de regeneración.

- ✓ Para la instalación de la fibra nos basamos en la recomendación UIT-T L.49. En esta Recomendación se describe la técnica con microzanjas, que permite instalar cables subterráneos en pequeñas ranuras a una profundidad reducida y ubicadas a los costados de las carreteras. Las ventajas de esta técnica con relación a las tecnologías convencionales de tendido de cables estriban esencialmente en su mayor velocidad de ejecución, bajo costo, repercusión ambiental significativamente baja y una interrupción limitada del tráfico en los caminos.

- ✓ Para este proyecto se ha escogido un cable de fibra denominado Headrow, este es un producto diseñado para soportar las condiciones más severas reduciendo notablemente los costes de los tendidos de fibra óptica, esta fibra es del tipo monomodo de 48 hilos especial para este tipo de tendido y es un diseño que involucra algunas capas protectores contra vibraciones, protecciones antiroedores, doble protección contra humedad ya que no esta protegida por ningún tipo de tubería de pvc o metal.

- ✓ Cada uno de los cuartos de equipos están diseñados y acondicionados de acuerdo a la norma ANSI/TIA/EIA-569-A que específica rutas y espacios de telecomunicaciones en edificios comerciales. Cada cuarto de equipos tiene una dimensión de 18 mt² y contarán con sus respectivos acondicionadores de aire, sistema puesta a tierra, sistemas de protecciones, UPS y generadores de energía en caso de falla de la empresa eléctrica.

- ✓ El equipo que se escogió para regeneración de señal fue el Optix OSN 3500. Este equipo proviene de la serie Optix proporcionados por el fabricante HUAWEI y funcionan como multiplexores, sistemas Add Drop y como Cross connect. Posee una plataforma de transmisión multiservicios, compatible con las tradicionales redes SDH e integra además, muchas y variadas tecnologías, tales como PDH, Ethernet, DWDM, ATM y MPLS , entre otras tecnologías.

- ✓ Para el estudio de los cálculos del diseño se consideraron 1,289 Km de fibra Optica Headrow, 36 patch cord de fibra monomodo, 331 empalmes que se alojaran en sus respectivas cajas protectoras y cada una de esta se localizará en arquetas o cajas para revisión y protección. Estos cáculos mostraron valores de potencia recibida aceptables por los equipos ADM por lo que se concluye que la localización de los cuartos de equipos es aceptada.

- ✓ La utilización de los equipos Huawei Optix 3500 en cada uno de los nodos, permitirá en un futuro, romper el anillo de fibra óptica y poder habilitar desde un PE a un P o simplemente un Switch de acceso para suplir la necesidad de comunicación en la ciudad donde este ubicado el nodo.

- ✓ El equipo de networking escogido fue el Cisco 7206VXR de la compañía CISCO. Con diseño modular, soporte de tarjetas de procesamiento NPE – G1 y G2 son equipos ideales para empresas proveedoreas de servicios de tamaño mediano que deciden implementar MPLS en su red de backbone.

- ✓ El protocolo de estado enlace OSPF fue el escogido como el protocolo IGP (protocolo interior) de nuestra red, dado que permite que todos los equipos del dominio MPLS conozcan al detalle toda la topología de la red. Esto es importante si se desea implementar Ingeniería de Tráfico como servicio para los clientes finales. Cabe mencionar que el protocolo IS-IS cumple también con las ventajas de OSPF, pero comercialmente y académicamente, el protocolo OSPF es más difundido e implementado.

- ✓ El protocolo BGP fue el escogido como protocolo EGP (protocolo exterior) de nuestra red, dada su riqueza de atributos y estabilidad, es el único que es capaz de soportar tablas de enrutamiento con más de 300K entradas, tal como ocurre cuando se aprende rutas desde el Internet.

- ✓ Cada cliente puede tener el direccionamiento privado que desee, sin preocuparse por duplicación de redes con otros clientes, sin necesidad de aplicar NAT a sus redes. Esto se debe gracias a la riqueza de atributos de BGP, que asignandole una caracteristica única a las redes del cliente (Route Distinguisher - RD), las convierten en redes privadas y únicas en el dominio MPLS a las redes de cada cliente.

- ✓ Entre el cliente y nuestro PE (punto de acceso a nuestro dominio MPLS) se puede configurar cualquier tipo de enrutamiento: dinámico con OSPF, EIGRP, RIP, BGP y estático mediante rutas aprendidas de forma manual.

- ✓ Son dos los servicios fundamentales que hacen a las redes MPLS comercialmente atractivas: Ofrecer conexiones privadas y dedicadas mediante medios compartidos gracias a la implementación de las VPNs. Y el ofrecer sobre estos canales Calidad de Servicio. El poder priorizar el tratamiento que se le dará a cada paquete según su naturaleza e importancia para el cliente es efectivamente un producto muy atractivo comercialmente.

Recomendaciones

- Es importante basar todo tipo de diseño y cálculo bajo las recomendaciones que emiten los organismos Internacionales tales como UIT – T y las ANSI/TIA/EIA.

- En el momento de escoger la ruta para el tendido de la fibra se deben evitar lugares con climas extremos o muy propensos a inundaciones donde se localizaran las arquetas o sajas de revisión.

- Queda como trabajo futuro el desarrollo de un estudio del impacto ambiental – visual que existe alrededor de esta tecnica relativamente novel como lo es el microzanjado.

BIBLIOGRAFIA

[1] BUECHE, FREDERICK, "Instalaciones de Fibras Ópticas"

[2] SIEMENS, "Conductores de Fibra Óptica

[3] ITU-T, Recomendacion L-49 para Microzanjado.
http://www.itu.int/itudoc/itu-t/aap/sg6aap/history/l49/index.html

[4] Cisco System Learning., "Implementing Cisco MPLS" Student Guide
Version 2.2

[5] Cisco System Learning., "Implementing Cisco Quality of Services " Student Guide
Version 1.2

[6] Cisco System Learning., "Building Scalable Cisco Internetwork " Student Guide
Version 3.0

[7] Cisco System Learning., "Configuring BGP on Cisco Routers" Student Guide
Version 3.2

[8] Zamora Hugo., "Implementación de redes MPLS-VPN – Casos de Estudio"
Año 2002, Conferencia en México.
http://www.cudi.edu.mx/primavera2002/presentaciones/MPLSVPN.pdf

[9] Cisco System Inc., "Cisco 7200 VXR Installation and Configuration Guide"
http://www.cisco.com/en/US/docs/routers/7200/install_and_upgrade/7200vxr_install_config/72vxicg.html

[10] IETF - Multiprotocol Label Switching (MPLS)
http://www.ietf.org/html.charters/mpls-charter.html.

[11] APC, Withepaper #11., " Explanation of Cooling and Air Conditioning Terminology for IT Professionals"
www.apcmedia.com/salestools/TEVS-5TXPED_R1_EN.pdf

GLOSARIO

AS: Autonomous System – Sistema Autónomo.

ATM: Asynchronous Transfer Mode – Modo de Transferencia Asincróna.

BDR: Backup Designed Router – Router Designado de Respaldo.

BGP: Border Gateway Protocol – Protocolo de Puerta Frontera.

CE: Costumer Equipment – Equipo del cliente.

CEF: Cisco Express Forwarding – Reenvío Rápido de Cisco

DR: Designed Router – Router Designado.

E-BGP:_ External BGP – BGP Externo.

E-LSR: Edge Label Swich Router – Ruteador de Borde Conmutador de Etiquetas.

EIGRP: Enhanced Internal Gateway Routing Protocol –Protocolo de enrutamiento interior mejorado.

FEC: Forwarding Equivalence Class – Equivalencia de Reenvío.

FIB: Forwarding Information Base – Tabla de Información de Reenvío.

FIFO: First Imput First Output – Primero en llegar, primero en salir.

I-BGP: Internal BGP – BGP Interno.

IETF: Internet Engineering Task Force.

IGRP: Internal Gateway Routing Protocol –Protocolo de enrutamiento interior.

IP: Internet Protocol – Protocolo de Internet.

IS-IS: Intermediate System to Intermediate System – Protocolo Intersistemas.

LDP: Label Distribution Protocol - Protocolo de Distribución de Etiquetas.

LIB: Label Information Base - Tabla de Información de Etiquetas.

LFIB: Label Forwarding Information Base - Tabla de Información de Reenvío de Etiquetas.

LSA: Link State Advertisement – Publicación del estado del enlace.

LSP: Label Switched Path – Camino conmutado de etiquetas.

LSR: Label Swich Router – Ruteador Conmutador de Etiquetas.

MP-BGP: Multiprotocol BGP – Extensión MPLS para BGP.

MPLS: Multiprotocol Label Switching – Multiprotocolo de conmutación de etiquetas.

NPE: Network Processing Engine – Motor de procesamiento de red.

OSI: Organization Standard International – Organización Internacional de Estandarización.

OSPF: Open Shortest Path First – Primero la ruta más corta.

PE: Provider Edge Router – Ruteador de Borde del Proveedor.

P: Provider Router – Ruteador del Proveedor

QoS: Quality Of Service – Calidad de Servicio.

RIB: Routing Information Base – Tabla de Información de Enrutamiento.

RIP: Routing Information Protocol – Protocolo de enrutamiento de información.

RSVP: Resource Reservation Protocolo – Protocolo de Reserva de Recursos.

TDP: Tag Distribution Protocolo – Protocolo de Distribución de Marcado.

TE: Traffic Engineering - Ingenieria de Trafico.

TCP: Transport Control Protocol – Protocolo de Control de Transporte.

UDP: User Datagram Protocol – Protocolo de Datagrama de Usuario.

VPN: Virtual Private Network – Red privada virtual.

VRF: Virtual Rounting and Forwarding.

ANEXOS

ANEXO A

Cisco 7200 Series Routers

Cisco 7200 series

Introducción

Este documento es proporciona la descripción de la arquitectura del soporte físico y de los programas de los ranuradores de la serie de Cisco 720x.

Componentes usados

Este documento no se restringe a las versiones del programa específicas, y se basa en Cisco de 7200 series.

La información en este documento fue creada de los dispositivos en un ambiente específico del laboratorio. Todos los dispositivos usados en este documento comenzaron con una configuración despejada (del defecto). Si su red está viva, cerciórense de que ustedes entiendan el impacto potencial de cualquier comando.

Convenciones

Para más información sobre convenciones del documento, vean a las convenciones de las extremidades técnicas de Cisco.

Arquitectura de hardware

Descripción del chasis

El chasis del ranurador de 7200 series consiste en el 2-slot Cisco 7202, el 4-slot Cisco 7204 y Cisco 7204VXR, y el 6-slot Cisco 7206 y Cisco 7206VXR:

- 7202: Un chasis de la dos-ranura que apoya solamente este la red que procesa los motores (NPEs):
  - NPE-100
  - NPE-150
  - NPE-200
- 7204: Un chasis 4-slot con el midplane de la herencia.
- 7206: Un chasis 6-slot con el midplane de la herencia.
- 7204VXR: Un chasis 4-slot con el midplane VXR.
- 7206VXR: Un chasis 6-slot con el midplane VXR.

Las 7200 series de la arquitectura de hardware varían de modelo para modelar, y dependen de la combinación de chasis y de NPE, pero puede ser separada generalmente en dos diseños importantes. Este documento se centra en estos dos diseños principales:

- Ranuradores con el midplane original, y un NPE temprano (NPE-100, NPE-150, NPE-200).
- Ranuradores con el midplane VXR, y un NPE posterior (NPE-175, NPE-225, NPE-300, NPE-400, NPE-G1, y así sucesivamente)

El chasis VXR provee de un 1 midplane Gbps cuando está utilizado el NPE-300, el NPE-400, o el NPE-G1. Además, el midplane VXR incluye un intercambio multiservicios (MIX). El cambiar de las ayudas de la MEZCLA de las franjas horarias DS0 a través de MEZCLA interconecta a través del midplane a cada ranura del adaptador del puerto. El midplane y la MEZCLA también apoyan la distribución de la sincronización entre los interfaces separados para apoyar voz y otros usos del constante-pedacito-rate. El midplane VXR proporciona dos 8,192 corrientes lleno-a dos caras de la multiplexación de división de tiempo (TDM) de Mbps entre cada ranura del adaptador del puerto y la MEZCLA, que tiene la capacidad de cambiar DS0s en las 12 8,192 corrientes de Mbps. Cada corriente puede apoyar hasta 128 canales DS0.

Cisco 7200 ranuradores VXR también apoya el motor NSE-1 del servicio en red, que consiste en dos tableros modulares: el tablero del motor del procesador y el tablero de regulador de la red. El tablero de procesador se basa en la arquitectura NPE-300. El tablero de regulador de la red recibe el procesador paralelo de la expedición expresa (PXF), que trabaja con el procesador de la encaminamiento para proporcionar conmutación de conjunto de bits acelerada, y el proceso acelerado de la característica de la capa 3 IP.

Red que procesa los motores - motor de los servicios en red

El NPE contiene el de memoria principal, la CPU, la memoria de la interconexión del componente (PCI) periférico (memoria de acceso aleatorio estática - SRAM), excepto en el NPE-100 que utiliza RAM dinámico (la COPITA)), y el trazado de circuito del control para los autobuses PCI. La red que procesa los motores consiste en los componentes siguientes:

- Un microprocesador computacional reducido del sistema (RISC) de instrucción. El cuadro 1 enumera los microprocesadores y sus frecuencias de reloj internas para vario NPEs.

Cuadro 1 - Microprocesadores RISC para vario NPEs Red que procesa el motor	Microprocesador	Frecuencia de reloj interna
NPE-100 y NPE-150	R4700	150 megaciclos
NPE-175	RM5270	200 megaciclos
NPE-200	R5000	200MHz
NPE-225	RM5271	262 megaciclos
NPE-300	RM7000	262

		megaciclos
NPE- 400	RM7000	350 megaciclos
NPE-G1	BCM1250	700 megaciclos
NSE-1	RM7000	262 megaciclos

- Regulador de sistema
  - Los NPE-100, los NPE-150, y los NPE-200 tienen un regulador de sistema que utilice el acceso directo de memoria (DMA) para transferir datos entre la COPITA y el paquete SRAM en la red que procesa el motor.
  - Los NPE-175 y los NPE-225 tienen un regulador de sistema que proporcione el acceso del procesador al midplane dos y a los solos autobuses PCI del regulador de la entrada-salida (entrada-salida). El regulador de sistema también permite que los adaptadores del puerto en cualquiera de los dos autobuses PCI del midplane tengan acceso a SDRAM
  - El NPE-300 tiene dos reguladores de sistema que proporcionen el acceso del procesador al midplane dos y a los solos autobuses PCI del regulador entrada-salida. El regulador de sistema también permite que los adaptadores del puerto en cualquiera de los dos autobuses PCI del midplane tengan acceso a SDRAM.
  - El NPE-400 tiene un regulador de sistema que proporcione el acceso de sistema.
  - El NPE-G1 BCM1250 también mantiene y ejecuta las funciones de administración de sistemas para Cisco 7200 ranuradores VXR, y lleva a cabo las funciones de la memoria de sistema y del control del medio ambiente.
  - El NSE-1 tiene un regulador de sistema que proporcione el acceso del procesador al midplane y a los solos autobuses PCI del regulador entrada-salida. El regulador de sistema también permite que los adaptadores del puerto en cualquiera de los dos autobuses PCI del midplane tengan acceso a SDRAM.

- Módulos de la memoria que pueden ser aumentados
  - La COPITA del uso NPE-100, NPE-150, y NPE-200 para almacenar las tablas de encaminamiento, los usos de la contabilidad de red, los paquetes de información con objeto de la conmutación de proceso, y el buffering del paquete para el desbordamiento de SRAM (excepto en el NPE-100, que no contiene ningún paquete SRAM). La configuración estándar es MB 32, con hasta 128 mejoras directas disponibles del módulo de memoria en línea MB solas (SIMM).
  - Los NPE-175 y los NPE-225 utilizan SDRAM para proporcionar código, datos, y almacenaje del paquete.
  - El NPE-300 utiliza SDRAM para almacenar todos los paquetes recibidos o enviados de interfaces de red. SDRAM también almacena usos de las tablas de encaminamiento y de la contabilidad de red. Dos órdenes de la memoria de SDRAM de la independiente en el sistema permiten el acceso concurrente por

los adaptadores del puerto y el procesador. El NPE-300 tiene una advertencia fija de la configuración con el primer dimm 32MB. Vean el cuadro 3-2 en la descripción NPE-300 y NPE-400 para más información.
    - El NPE-400 utiliza SDRAM para almacenar todos los paquetes recibidos o enviados de interfaces de red. El arsenal de la memoria de SDRAM en el sistema permite el acceso concurrente por los adaptadores del puerto y el procesador.
    - El NSE-1 utiliza SDRAM para proporcionar código, datos, y almacenaje del paquete.
    - El NPE-G1 utiliza SDRAM para almacenar todos los paquetes recibidos o enviados de interfaces de red. SDRAM también almacena usos de las tablas de encaminamiento y de la contabilidad de red. Dos órdenes de la memoria de SDRAM de la independiente en el sistema permiten el acceso concurrente por los adaptadores del puerto y el procesador.

- Paquete SRAM para almacenar los paquetes de información con objeto de la conmutación rápida
    - El NPE-150 tiene 1 MB de SRAM y el NPE-200 tiene MB 4 de SRAM. Ninguna otra red que procesa el motor o el motor de los servicios en red tiene SRAM.

- Memoria ocult0
    - Los NPE-100, los NPE-150, y los NPE-200 han unificado el escondrijo que las funciones como el escondrijo secundario para el microprocesador (el escondrijo primario está dentro del microprocesador).
    - Los NPE-175 y los NPE-225 tienen dos niveles de escondrijo: un escondrijo primario que es interno al procesador y a un secundario, escondrijo externo 2-MB que proporciona el almacenaje de alta velocidad adicional para los datos y las instrucciones.
    - El NPE-300 tiene tres niveles de escondrijo: un escondrijo primario y secundario que es interno al microprocesador, y un terciario, escondrijo externo 2-MB que proporciona el almacenaje de alta velocidad adicional para los datos y las instrucciones.
    - El NPE-400 tiene tres niveles de escondrijo: un escondrijo externo primario y un escondrijo secundario que es interno al microprocesador, y terciario 4-MB que proporciona el almacenaje de alta velocidad adicional para los datos y las instrucciones.
    - El NSE-1 tiene tres niveles de escondrijo: un escondrijo unificado primario y secundario que es interno al microprocesador, y un terciario, escondrijo del external 2-MB.
    - El NPE-G1 tiene dos niveles de escondrijo: un escondrijo primario y secundario que es interno al microprocesador. El escondrijo unificado secundario se utiliza para los datos y la instrucción.
- Dos sensores ambientales para supervisar el aire de enfriamiento como sale del chasis.
- Pateen la ROM para almacenar suficiente código para patear el software de Cisco IOS®; los NPE-175, los NPE-200, los NPE-225, los NPE-300, los NPE-400, los NPE-G1, y los NSE-1 tienen ROM del cargador.

El motor del servicio en red (NSE-1) entrega rendimiento de procesamiento de la tarifa OC3 del alambre mientras que funciona con servicios PÁLIDOS del borde del alto-tacto concurrente. El diseño subyacente leverages la tecnología NPE-300 realzada por un motor intensivo de proceso del microcódigo llamado motor de la expedición expresa Parallel (PXF). Esta arquitectura de proceso dual única ofrece un enorme aumento del funcionamiento para los servicios en red proceso-hambrientos, inteligentes. El procesador de la ruta/del interruptor saca datos los servicios del alto-tacto complejo de la capa 4 a de la capa 7 al procesador PXF, y sostiene funcionamiento de la tarifa del alambre.

Para la información adicional, vean:

- NPE e instalación y configuración NSE
- Boletines del producto y avisos FOE

Tablero entrada-salida

El regulador entrada-salida comparte las funciones de memoria de sistema y las funciones del control del medio ambiente para el ranurador de Cisco 7200 con la red que procesa el motor. Contiene estos componentes:

- Uno o dos Ethernet autosensing/puertos de Ethernet rápidos o Ethernet de 1 gigabit y 1 puerto de Ethernet, basados en el tipo del regulador entrada-salida.
- Canales duales para la consola local y los puertos auxiliares.
- Memoria Flash para almacenar la imagen del ayudante del cargador así como otros datos (tales como ficheros del crashinfo).
- Dos ranuras de la tarjeta PC para las tarjetas de los discos de destello o de memoria Flash, que contienen la imagen del software IOS de Cisco del defecto.
- ROM del cargador para almacenar suficiente código para patear el software IOS de Cisco (el C7200-I/O-2FE/E no tiene un componente ROM del cargador).
- Dos sensores ambientales para supervisar el aire de enfriamiento como entra en y sale Cisco de 7200 chasis.
- Memoria de acceso aleatorio permanente (NVRAM) para almacenar los registros de la configuración de sistema y del control del medio ambiente.

Descripciones del regulador entrada-salida

Cuadro 2 - Reguladores entrada-salida y sus descripciones Número del producto	Descripción
C7200-I/O-GE+E	Una Ethernet del gigabit y un puerto de Ethernet; equipado de un receptáculo GBIC para 1000 megabits por la operación del segundo (Mbps) y de un receptáculo RJ-45 para la operación 10-Mbps
C7200-I/O-2FE/E	Dos Ethernet autosensing/puertos de Ethernet rápidos; equipado de dos receptáculos RJ-45 para la operación 10/100-Mbps.
C7200-I/O-FE1	Un puerto de Ethernet rápido; equipado de un receptáculo MII y de un receptáculo RJ-45 para el uso en 100 operación lleno-a dos caras o semidúplex de Mbps. Solamente un receptáculo se puede configurar para el uso a la vez.
C7200-I/O	No tiene ningún puerto de Ethernet rápido.
C7200-I/O-FE-MII2	Un puerto de Ethernet rápido; equipado de un solo receptáculo MII.

1 el número C7200-I/O-FE del producto no especifica MII porque un MII y un receptáculo RJ-45 es incluidos.

2 el regulador entrada-salida con el número C7200-I/O-FE-MII del producto tiene un receptáculo rápido de Ethernet solo MII solamente. Aunque todavía sea apoyado por Cisco Systems, este regulador entrada-salida con un solo receptáculo MII no haya estado disponible para la orden desde mayo 1998.

Ustedes pueden también identificar su modelo del regulador entrada-salida de un terminal. Para hacer así pues, utilicen el comando de la ranura 0 del diag de la demostración.

El NPE-G1 es la primera red que procesa el motor para Cisco 7200 ranuradores VXR para proporcionar la funcionalidad de una red que procesa el motor y el regulador entrada-salida. Mientras que su diseño proporciona funcionalidad del regulador entrada-salida, puede también trabajar con cualquier regulador entrada-salida apoyado en Cisco 7200 VXR. Cuando ustedes instalan un regulador entrada-salida en un chasis con el NPE-G1, la consola y los puertos auxiliares en el regulador entrada-salida se activan. Además, la consola y los puertos auxiliares a bordo el NPE-G1 se inhabilitan automáticamente. Sin embargo, ustedes pueden todavía utilizar las ranuras del disco de destello y los puertos de Ethernet en el regulador NPE-G1 y entrada-salida cuando ambas tarjetas están instaladas.

Nota: Los reguladores entrada-salida no son caliente-intercambiables. Antes de ustedes inserten el regulador entrada-salida, interruptor de la energía.

Para la información adicional, vean:

- Instrucciones del reemplazo del controlador de entradas-salidas
- Controlador de entradas-salidas para el Midplane de la herencia
- Controlador de entradas-salidas para el Midplane VXR

Adaptadores del puerto (PAs)

Éstos son los reguladores modulares del interfaz que contienen el trazado de circuito para transmitir y para recibir los paquetes en los medios físicos. Éstos son los mismos adaptadores del puerto usados en el procesador versátil del interfaz (VIP) con Cisco ranurador de 7500 series. La ayuda de ambas plataformas la mayoría de los adaptadores del puerto, pero allí es algunas excepciones. Un cierto PAs que requiere el interruptor de la multiplexación de división (TDM) de tiempo se apoya solamente en el midplane VXR.

Los adaptadores del puerto instalaron en la inserción y el retiro en línea (OIR) de la ayuda de los ranuradores de Cisco 7200. Son caliente-intercambiables.

Cisco los ranuradores de 7200 series tiene una capacidad del dato-llevar, designada la anchura de banda, que afecta a la distribución del adaptador del puerto en el chasis, así como el número y los tipos de adaptadores del puerto que ustedes pueden instalar. Los adaptadores del puerto se deben distribuir uniformemente por anchura de banda entre el autobús mb1 PCI (el PA ranura 0, 1, 3, y 5) y el autobús mb2 PCI (el PA ranura 2, 4, 6).

Cisco 7200 o Cisco 7200 ranuradores VXR con una red que procesa el motor (NPE) NPE-100, NPE-150, NPE-175, NPE-200, o NPE-225, utiliza una designación alta, media, o de la bajo-anchura de banda para determinar la distribución y la configuración del adaptador del puerto.

Cisco 7200 ranuradores VXR con un NPE-300, un NPE-400, o puntos de una anchura de banda del uso NSE-1 para determinar la distribución del adaptador del puerto y la configuración en vez de designaciones altas, medias, o de la bajo-anchura de banda. Los puntos de la anchura de banda son un valor asignado relacionado con la anchura de banda; sin embargo, se ajusta el valor basó en cómo el hardware utiliza eficientemente el autobús PCI.

Nota: Ustedes pueden utilizar Cisco ranurador de 7200 series con una configuración del adaptador del puerto que exceda las pautas. Sin embargo, para prevenir irregularidades mientras que el ranurador es funcionando, recomendamos fuertemente que ustedes restrinjan los tipos del adaptador del puerto instalados en el ranurador, según las pautas enumeradas en los vínculos abajo. Además, su configuración del adaptador del puerto debe estar dentro de estas pautas ante Cisco que el centro de la asistencia técnica localizará averías las anomalías que ocurren en su Cisco ranurador de 7200 series. Los adaptadores del puerto son caliente-intercambiables.

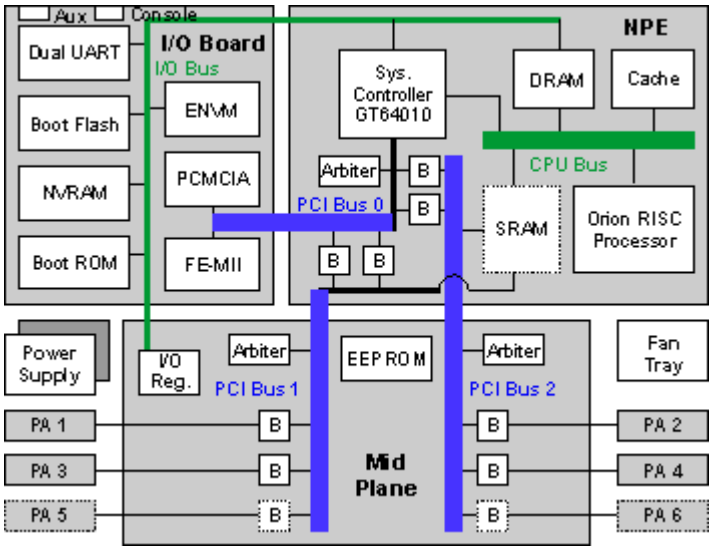
La información adicional se puede encontrar aquí:

- ¿Qué causa mensajes de error %PLATFORM-3-PACONFIG y %C7200-3-PACONFIG?
- Cisco pautas de la configuración de hardware del adaptador del puerto de 7200 series

Nota: El lanzamiento del nuevo ranurador de Cisco 7200 VXR requiere ciertas actualizaciones del adaptador del puerto para la compatibilidad delantera. Este requisito es debido al midplane nuevo y más de alta velocidad de la interconexión del componente (PCI) periférico en el ranurador de Cisco 7200 VXR. Solamente los adaptadores del puerto utilizaron en Cisco que 7200 ranuradores

VXR requieren esta actualización. Puesto que todos los adaptadores del puerto no pueden ser aumentados, algunos adaptadores del puerto no se apoyan en Cisco 7200 ranuradores VXR. Para los detalles, vean el aviso de campo: Viren la compatibilidad del adaptador hacia el lado de babor para Cisco 7200 ranuradores VXR.

Bloque diagrama



Detalles de la memoria

El ranurador de 7200 series utiliza memoria de la COPITA, de SDRAM, y de SRAM en el NPE en las varias combinaciones basadas en el modelo. La memoria disponible se divide en tres piscinas de memoria: la piscina del procesador, la piscina entrada-salida, y la piscina PCI (I/O-2 en NPE-300).

Aquí están algunos ejemplos de la salida del comando de la memoria de la demostración que utilizan un procesador de Cisco 7206 (NPE150) (revisión B) con los octetos 43008K/6144K de memoria:

- Memoria del procesador: Esta piscina se utiliza para almacenar el IOS de Cisco codifica en software, las tablas de encaminamiento, y los almacenadores intermediarios del sistema. Se asigna de la COPITA en el NPE-100, NPE-150, y el NPE-200; la región de SDRAM en el NPE-175 y el NPE-225; y banco 1 de SDRAM en el NPE-300.
- Memoria entrada-salida: Esta piscina se utiliza para las piscinas de la partícula. Las piscinas privadas del interfaz y la piscina pública de la partícula se asignan de esta memoria. El tamaño de esta memoria depende del tipo de NPE. Los NPE-150 y los NPE-200 ambos tienen una cantidad fija de SRAM que se utilice para una forma de memoria de la entrada-salida (entrada-salida): 1 MB para el NPE-150 y 4 MBs para el NPE-200. El NPE-300 utiliza su banco 0 de SDRAM que sea fijo en MB 32.
- Memoria PCI: Esta pequeña piscina se utiliza principalmente para el interfaz recibe y transmite los anillos. Se utiliza a veces para asignar las piscinas privadas de la partícula

del interfaz para los interfaces de alta velocidad. En los sistemas NPE-175, NPE-225, y NPE-300, esta piscina se crea en SDRAM. En el NPE-150 y el NPE-200, se crea enteramente en SRAM.

Para la información detallada sobre las especificaciones de la tabla de la localización y de memoria, vean la posición de memoria y las especificaciones. De este vínculo, ustedes pueden también encontrar algunas pautas y restricciones memoria-relacionadas clasificadas por NPE/NSE.

Otro vínculo provechoso es instrucciones del reemplazo de la memoria para el regulador NPE o NSE y entrada-salida.

Secuencia del cargador

Durante el proceso de cargador, observen el sistema LED. Los LED en la mayor parte de los adaptadores del puerto entran por intervalos en una secuencia irregular. Algunos pueden encenderse, apagarse, y encenderse otra vez por un breve periodo de tiempo. En el regulador entrada-salida, la AUTORIZACIÓN LED de la energía entrada-salida se adelanta inmediatamente.

Observen el proceso de inicialización. Cuando el cargador del sistema es completo (algunos segundos), la red que procesa el motor o el motor de los servicios en red comienza a inicializar los adaptadores del puerto y el regulador entrada-salida. Durante esta inicialización, los LED en cada adaptador del puerto se comportan diferentemente (la mayoría del flash por intervalos).

El LED permitido en cada adaptador del puerto va en cuando se termina la inicialización, y las exhibiciones de pantalla de la consola una bandera de la escritura y del sistema similar a esto:

Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-IK8S-M), Version 12.2(10b),
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Fri 12-Jul-02 07:47 by xxxxx
Image text-base: 0x60008940, data-base: 0x613D4000

Cuando ustedes ponen en marcha el ranurador por primera vez, el sistema incorpora automáticamente la facilidad del comando de la disposición, que determina qué adaptadores del puerto están instalados y les incita proporcionar la información de configuración para cada uno. En el terminal de la consola, después de que el sistema exhiba la configuración de la bandera y de hardware del sistema, ustedes ven este aviso del diálogo de la configuración de sistema:

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]:

Si el sistema no termina cada uno de los pasos en el procedimiento de lanzamiento, vean la localización de averías de la instalación para las extremidades y los procedimientos de localización de averías.

De conmutación de conjunto de bits

Cisco conmutación de proceso de 7200 ayudas de la serie, conmutación rápida, y expedición expresa de Cisco (CEF), pero no apoya ninguna forma de conmutación distribuida. La CPU principal en el NPE realiza todas las tareas de conmutación.

La descripción en esta sección se basa en el libro dentro de la arquitectura de los programas IOS de Cisco, Cisco Press.1

1 - El paquete recibe la etapa

Estos pasos ilustran qué ocurre cuando se recibe un paquete:

Paso 1: El paquete se copia de los medios en una serie de partículas ligadas al anillo de la recepción del interfaz. Las partículas pueden residir en la memoria entrada-salida o la memoria PCI, basada en la velocidad de medios del interfaz, y la plataforma.

Paso 2: El interfaz levanta una interrupción de la recepción a la CPU.

Paso 3: El software IOS de Cisco reconoce la interrupción y comienza a intentar la asignación de partículas para substituir los que está llenados en el anillo de la recepción del interfaz. El software IOS de Cisco comprueba la piscina privada del interfaz primero, y en seguida comprueba la piscina normal pública si no hay ninguno en la piscina privada. Si las suficientes partículas no existen para llenar el anillo de la recepción, se cae el paquete (las partículas del paquete en el anillo de la recepción se limpian con un chorro de agua), y no se incrementa el “ningún almacenador intermediario” contrario.

El software IOS de Cisco también estrangula el interfaz en este caso. Cuando un interfaz se estrangula en los 7200, se no hacen caso todos los paquetes recibidos hasta que el interfaz sea unthrottled. Los unthrottles del software IOS de Cisco el interfaz después de la piscina agotada de la partícula se llenan con las partículas libres.

Paso 4: El software IOS de Cisco liga las partículas del paquete en el anillo de la recepción juntas, y después las liga a un jefe del almacenador intermediario de la partícula. Entonces las liga al anillo en lugar de las partículas del paquete para llenar el anillo de la recepción con las partículas nuevamente asignadas.

2 - Etapa de conmutación de conjunto de bits

Ahora que el paquete está en partículas, el software IOS de Cisco cambia el paquete. Los pasos abajo describen este proceso:

Paso 5: El código de la conmutación primero comprueba el escondrijo de la ruta (rápidamente o CEF) para considerar si puede ayunar interruptor el paquete. Si el paquete se puede cambiar durante la interrupción, salta al paso 6. Si no, continúa preparando el paquete para la conmutación de proceso.

- 5,1: El paquete se une en un almacenador intermediario contiguo (almacenador intermediario del sistema). Si ningún almacenador intermediario libre del sistema existe para aceptar el paquete, se cae, y no se incrementa el “ningún almacenador intermediario” contrario, como indicado en la salida de los interfaces de la demostración ordenen:
- Router#show interfaces
- Ethernet2/1 is up, line protocol is up
- ....
- Output queue 0/40, 0 drops; input queue 0/75, 0 drops
- 5 minute input rate 5000 bits/sec, 11 packets/sec
- 5 minute output rate 0 bits/sec, 0 packets/sec
- 1903171 packets input, 114715570 bytes, 1 no buffer
- Received 1901319 broadcasts, 0 runts, 0 giants, 1 throttles
- ....

Si el software IOS de Cisco no puede asignar un almacenador intermediario del sistema para unirse un almacenador intermediario de la partícula, también estrangula el interfaz e incrementa “estrangula” contrario, como indicado en el comando del interfaz de la demostración hagan salir el ejemplo arriba. Se no hace caso todo el tráfico de la entrada mientras que se estrangula un interfaz. Los restos del interfaz estrangulamientos hasta software IOS de Cisco tienen almacenadores intermediarios libres del sistema disponibles para el interfaz.

- 5,2: Cuando se une el paquete, se hace cola para la conmutación de proceso, y el proceso que maneja este tipo de paquete se programa para funcionar. La interrupción de la recepción entonces se despide.
- 5,3: Asuman que esto es un paquete IP. Cuando el proceso de entrada IP funciona, consulta la tabla de encaminamiento y descubre el interfaz el extranjero. Consulta las tablas asociadas al interfaz el extranjero y localiza el jefe del MAC que necesita ser colocado en el paquete.
- 5,4: Después de que el paquete se haya cambiado con éxito, se copia en la coleta de salida para el interfaz el extranjero.
- 5,5: De aquí, el software IOS de Cisco procede a la etapa del transmitir.

Paso 6: El código de la conmutación del software IOS de Cisco (ayunan o CEF) reescribe el jefe del MAC en el paquete para su destinación. Si el nuevo jefe del MAC es más grande que el jefe original, el software IOS de Cisco asigna una nueva partícula de la piscina F/S y la inserta al principio de la cadena de partículas para sostener el jefe más grande.

3 - El paquete transmite la etapa: Conmutación rápida y CEF

Ahora ustedes tienen un paquete con éxito cambiado, con su jefe del MAC reescrito. El paquete transmite la etapa funciona diferentemente, basado encendido si el software IOS de Cisco rápido cambia el paquete (rápidamente o CEF), o el proceso cambia el paquete. Las secciones siguientes cubren el paquete transmiten la etapa en los ambientes rápidos y de proceso de la conmutación para Cisco los ranuradores de 7200 series.

Estos pasos describen el paquete transmiten la etapa en un ambiente rápido de la conmutación:

Paso 7: El software IOS de Cisco primero comprueba la coleta de salida del interfaz. Si la coleta de salida no está vacía o el anillo del transmitir del interfaz es lleno, el software IOS de Cisco hace cola el paquete en la coleta de salida, y despide la interrupción de la recepción. El paquete consigue eventual transmitió cualquiera cuando llega el paquete de otros proceso-cambiar, o cuando el interfaz publica una interrupción del transmitir. Si la coleta de salida está vacía, y el anillo del transmitir tiene sitio, el software IOS de Cisco continúa al paso 8.

Paso 8: El software IOS de Cisco liga cada uno de las partículas del paquete al anillo del transmitir del interfaz, y despide la interrupción de la recepción.

Paso 9: Los medios del interfaz que el regulador vota su transmiten el anillo, y detectan un nuevo paquete que se transmitirá.

Paso 10: Los medios del interfaz que el regulador copia el paquete de su transmiten el anillo a los medios, y levantan una interrupción del transmitir a la CPU.

Paso 11: El software IOS de Cisco reconoce la interrupción del transmitir, y libera todas las partículas del paquete transmitido del anillo del transmitir, y las vuelve a su piscina de la partícula que origina.

Paso 12: Si algunos paquetes están esperando en la coleta de salida del interfaz (probablemente porque el anillo del transmitir era lleno hasta ahora), el software IOS de Cisco quita los paquetes de la coleta, y liga sus partículas o los almacenadores intermediarios contiguos al transmitir suenan para que el regulador de los medios considere.

Paso 13: El software IOS de Cisco despide la interrupción del transmitir.

4 - El paquete transmite la etapa: Conmutación de proceso

Estos pasos describen el paquete transmiten la etapa en un ambiente de proceso de la conmutación:

Paso 14: El software IOS de Cisco comprueba el tamaño del paquete siguiente en la coleta de salida y lo compara al espacio dejado en el anillo del transmitir del interfaz. Si bastante espacio existe en el anillo del transmitir, el software IOS de Cisco quita el paquete de la coleta de salida, y liga su almacenador intermediario contiguo (o partículas) al anillo del transmitir.

Nota: Si los paquetes múltiples existen en la coleta de salida, el software IOS de Cisco intenta drenar la coleta, y pone todos los paquetes en el anillo del transmitir del interfaz.

Paso 15: Los medios que el regulador del interfaz vota su transmiten el anillo, y detectan un nuevo paquete que se transmitirá.

Paso 16: Los medios del interfaz que el regulador copia el paquete de su transmiten el anillo a los medios, y levantan una interrupción del transmitir a la CPU.

Paso 17: El software IOS de Cisco reconoce la interrupción del transmitir y libera el almacenador intermediario contiguo (o partículas) del paquete transmitido del anillo del transmitir, y las vuelve a su piscina que origina.

1" desarrollo profesional CCIE: Arquitectura de los programas interior IOS de Cisco" por Vijay Bollapragada, Curtis Murphy, blanco de Russ (ISBN 1-57870-181-3).

Apéndice B

GENERALIDADES EQUIPOS HUAWEI OPTIX OSN 3500

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

CARACTERÍSTICAS

a) Plataforma económicamente eficiente:

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

b) Configuración flexible:

-Compatibilidad con STM-64/16
-Soporta actualización on-line de 2.5G a 10G

c) Alta capacidad en la planificación:

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

d) Provisión multiservicio

1) Interfaces

-STM-1 (O/E);
-STM-4/16/64 estandard o concatenados;
-E1/T1/E3/T3/E4;
-ATM
-IMA, SAN y otros.

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

e) Alta integración

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

f) Robusto

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

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

g) Tecnología WDM incorporada

-Provee dos canales ópticos para tarjetas ADM

h) Completos mecanismos de protección de red

-Recuperación de mallas

-Mecanismos distribuidos de recuperación de rutas de protección.

-Incorpora cinco tipos de esquemas de servicios con SLA, “diamond”, “gold”, “silver”, “cooper” e “iron”.

-Protección SDH

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

-Protección de servicio de datos

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

-Soporta protección de anillo VP-RING para servicios ATM

i) Completos mecanismos de protección de equipo

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

-Protección de energía y térmico (TPS)

j) Características físicas

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

NIVELES DE SERVICIO ASON EN EQUIPOS HUAWEI OSN 3500

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

Un servicio de nivel “Diamond” provee “conexiones permanentes” (PC) 1+1. A nivel SDH, esta opera bajo protección SNCP Si se corta la fibra por donde está pasando el tráfico, el servicio

conmutará el tráfico a la fibra de respaldo en menos de 50ms. Al mismo tiempo, el sistema buscará una nueva ruta de protección para el enlace. Este nivel es usado principalmente para tráfico de muy alta prioridad, Clientes estratégicos, gobierno, fuerzas armadas y todo enlace crítico para la empresa.

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

Nivel “Silver” provee protección de ruta conmutada, es decir, la restauración se produce en tiempo real. Los tiempos de conmutación fluctúan entre 60ms y 400ms. Es eficiente en servicios no críticos. Existen dos clasificaciones más, “Cooper” e “Iron”, las cuales no proveen protección pero permiten utilizar el ancho de banda disponible de la red.

SELECCIÓN DE TRÁFICO Y NIVELES DE SERVICIOS

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

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

Anexo C

Configuración Global Equipos Networking

Configuración equipo P01GYE - Guayaquil

```
P01GYE#sh runn
Building configuration...

Current configuration : 4398 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P01GYE
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!
!
ip cef
no ip domain lookup
!
!
mpls label range 16 800000
mpls label protocol ldp
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
class-map match-any CM-VoIP
 match mpls experimental topmost 5
 match ip precedence 5
class-map match-any CM-Controlred
 match mpls experimental topmost 6  7
 match ip precedence 6  7
class-map match-any CM-Video
 match mpls experimental topmost 4
 match ip precedence 4
class-map match-any CM-Datoscriticos
 match mpls experimental topmost 2  3
 match ip precedence 2  3
class-map match-any CM-Datosnocriticos
 match mpls experimental topmost 1
 match ip precedence 1
!
!
policy-map PM-QoSBB
 class CM-VoIP
  police rate percent 15
    conform-action transmit
    exceed-action drop
  priority percent 15
 class CM-Controlred
  bandwidth percent 3
 class CM-Video
  bandwidth percent 20
  queue-limit 20
 class CM-Datoscriticos
  bandwidth percent 20
  random-detect
  random-detect precedence 2   20    50
  random-detect precedence 3   30    60
 class CM-Datosnocriticos
  bandwidth percent 15
  random-detect
  random-detect precedence 1   40    70
 class class-default
  fair-queue
```

```
 random-detect
 random-detect precedence 0   80    200
!
!
!
!
interface Loopback199
 description #### Loopback ID ####
 ip address 10.116.254.20 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 description ### link P01UIO ###
 mtu 1532
 bandwidth 10000000
 ip address 10.116.253.2 255.255.255.252
 no ip redirects
 no ip proxy-arp
 load-interval 30
 negotiation auto
 mpls ip
 service-policy output PM-QoSBB
!
interface GigabitEthernet2/0
 description ### link P01CUE ###
 mtu 1532
 bandwidth 10000000
 ip address 10.116.253.9 255.255.255.252
 no ip redirects
 no ip proxy-arp
 load-interval 30
 negotiation auto
 mpls ip
 service-policy output PM-QoSBB
!
interface GigabitEthernet3/0
 description #### Link1-PE01GYE ####
 mtu 1532
 bandwidth 10000000
```

```
 ip address 10.116.253.161 255.255.255.252
 no ip redirects
 no ip proxy-arp
 load-interval 30
 negotiation auto
 mpls ip
 service-policy output PM-QoSBB
!
router ospf 1
 router-id 10.116.254.20
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 redistribute connected
 network 10.116.253.2 0.0.0.0 area 0
 network 10.116.253.9 0.0.0.0 area 0
 network 10.116.253.161 0.0.0.0 area 0
 network 10.116.254.20 0.0.0.0 area 0
!
router bgp 666
 bgp router-id 10.116.254.20
 no bgp default ipv4-unicast
 bgp cluster-id 0.0.0.1
 bgp log-neighbor-changes
 neighbor 10.116.254.10 remote-as 666
 neighbor 10.116.254.10 description P01UIO
 neighbor 10.116.254.10 update-source Loopback199
 neighbor 10.116.254.11 remote-as 666
 neighbor 10.116.254.11 description PE01UIO
 neighbor 10.116.254.11 update-source Loopback199
 neighbor 10.116.254.21 remote-as 666
 neighbor 10.116.254.21 description PE01GYE
 neighbor 10.116.254.21 update-source Loopback199
 neighbor 10.116.254.30 remote-as 666
 neighbor 10.116.254.30 description P01CUE
 neighbor 10.116.254.30 update-source Loopback199
 neighbor 10.116.254.31 remote-as 666
 neighbor 10.116.254.31 description PE01CUE
 neighbor 10.116.254.31 update-source Loopback199
 !
 address-family vpnv4
 neighbor 10.116.254.10 activate
 neighbor 10.116.254.10 send-community both
 neighbor 10.116.254.10 route-reflector-client
 neighbor 10.116.254.11 activate
```

```
 neighbor 10.116.254.11 send-community both
 neighbor 10.116.254.11 route-reflector-client
 neighbor 10.116.254.11 next-hop-self
 neighbor 10.116.254.21 activate
 neighbor 10.116.254.21 send-community both
 neighbor 10.116.254.21 route-reflector-client
 neighbor 10.116.254.21 next-hop-self
 neighbor 10.116.254.30 activate
 neighbor 10.116.254.30 send-community both
 neighbor 10.116.254.30 route-reflector-client
 neighbor 10.116.254.30 next-hop-self
 neighbor 10.116.254.31 activate
 neighbor 10.116.254.31 send-community both
 neighbor 10.116.254.31 route-reflector-client
 neighbor 10.116.254.31 next-hop-self
 exit-address-family
!
!
no ip http server
!
!
!
!
!
mpls ldp router-id Loopback199 force
!
!
control-plane
!
!
!
!
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end
```

Configuración equipo PE01GYE - Guayaquil

```
PE01GYE#sh runn
Building configuration...

Current configuration : 3985 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE01GYE
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!
!
ip cef
no ip domain lookup
!
!
ip vrf espol
 rd 666:100000
 route-target export 666:100000
 route-target import 666:100000
!
mpls label range 16 800000
mpls label protocol ldp
!
!
!
!
!
!
!
!
```

```
!
!
class-map match-any CM-VoIP
 match mpls experimental topmost 5
 match ip precedence 5
class-map match-any CM-Controlred
 match mpls experimental topmost 6  7
 match ip precedence 6  7
class-map match-any CM-Video
 match mpls experimental topmost 4
 match ip precedence 4
class-map match-any CM-Datoscriticos
 match mpls experimental topmost 2  3
 match ip precedence 2  3
class-map match-any CM-Datosnocriticos
 match mpls experimental topmost 1
 match ip precedence 1
!
!
policy-map 1280kbps
 class class-default
  police cir 1280000 bc 40000 be 40000
    exceed-action drop
policy-map 128kbps
 class class-default
  police cir 128000 bc 4000 be 4000
    exceed-action drop
policy-map 256kbps
 class class-default
  police cir 256000 bc 8000 be 8000
    exceed-action drop
policy-map PM-QoSBB
 class CM-VoIP
  police rate percent 15
    conform-action transmit
    exceed-action drop
  priority percent 15
 class CM-Controlred
  bandwidth percent 3
 class CM-Video
  bandwidth percent 20
  queue-limit 20
 class CM-Datoscriticos
  bandwidth percent 20
```

```
  random-detect
  random-detect precedence 2   20    50
  random-detect precedence 3   30    60
 class CM-Datosnocriticos
  bandwidth percent 15
  random-detect
  random-detect precedence 1   40    70
 class class-default
  fair-queue
  random-detect
  random-detect precedence 0   80    200
!
!
!
interface Loopback199
 description #### Loopback ID ####
 ip address 10.116.254.21 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 no ip address
 duplex full
!
interface GigabitEthernet1/0
 description #### Link1-P01GYE ####
 mtu 1532
 ip address 10.116.253.162 255.255.255.252
 no ip redirects
 no ip proxy-arp
 load-interval 30
 negotiation auto
 mpls ip
 mpls mtu 1524
 service-policy output PM-QoSBB
!
interface FastEthernet2/0
 ip vrf forwarding espol
 ip address 192.168.1.1 255.255.255.252
 duplex full
 service-policy input 128kbps
 service-policy output 128kbps
!
router ospf 1
 router-id 10.116.254.21
```

```
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 network 10.116.253.162 0.0.0.0 area 0
 network 10.116.254.21 0.0.0.0 area 0
!
router bgp 666
 bgp router-id 10.116.254.21
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 10.116.254.10 remote-as 666
 neighbor 10.116.254.10 description P01UIO
 neighbor 10.116.254.10 update-source Loopback199
 neighbor 10.116.254.20 remote-as 666
 neighbor 10.116.254.20 description P01GYE
 neighbor 10.116.254.20 update-source Loopback199
 neighbor 10.116.254.30 remote-as 666
 neighbor 10.116.254.30 description P01CUE
 neighbor 10.116.254.30 update-source Loopback199
 !
 address-family vpnv4
 neighbor 10.116.254.10 activate
 neighbor 10.116.254.10 send-community both
 neighbor 10.116.254.10 next-hop-self
 neighbor 10.116.254.10 route-map RM-RRin in
 neighbor 10.116.254.20 activate
 neighbor 10.116.254.20 send-community both
 neighbor 10.116.254.20 next-hop-self
 neighbor 10.116.254.20 route-map RM-RRin in
 neighbor 10.116.254.30 activate
 neighbor 10.116.254.30 send-community both
 neighbor 10.116.254.30 next-hop-self
 neighbor 10.116.254.30 route-map RM-RRin in
 exit-address-family
 !
 address-family ipv4 vrf espol
 redistribute connected
 redistribute static
 no synchronization
 exit-address-family
!
ip route vrf espol 10.6.0.0 255.255.0.0 192.168.1.2 name Espol_GYE
!
no ip http server
!
```

```
ip bgp-community new-format
!
!
route-map RM-RRin permit 50
!
!
!
control-plane
!
!
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end

PE01GYE#
```

Configuración equipo CE - Guayaquil

```
espol#sh runn
Building configuration...

Current configuration : 1146 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname espol
!
logging queue-limit 100
!
memory-size iomem 25
ip subnet-zero
```

```
!
!
!
ip cef
ip audit notify log
ip audit po max-events 100
!
!
!
 class-map match-all best_effort
   description Todo lo demas
 class-map match-all voz
  match  precedence 5
 class-map match-all datoscriticos
  match access-group 100
!
!
 policy-map QoS_out
  class best_effort
   set precedence 1
  class voz
   set precedence 5
  class datoscriticos
   set precedence 3
!
!
!
interface Ethernet0
 ip address 10.6.1.1 255.255.0.0
 service-policy input QoS_out
 half-duplex
!
interface FastEthernet0
 description ### enlace wan a espol Quito ###
 ip address 192.168.1.2 255.255.255.252
 speed auto
 full-duplex
!
router eigrp 100
 network 10.6.0.0 0.0.255.255
 network 192.168.1.0 0.0.0.3
 neighbor 192.168.1.1 FastEthernet0
 no auto-summary
!
```

```
ip classless
ip route 10.6.0.0 255.255.0.0 Null0
no ip http server
!
!
access-list 100 permit icmp any any
!
line con 0
 password tesis
 login
line aux 0
line vty 0 4
 password tesis
 login
!
end

espol#
```

Configuración equipo P01UIO - Quito

```
P01UIO>ena
P01UIO#show running
Building configuration...

Current configuration : 4329 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P01UIO
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
```

```
!
!
ip cef
no ip domain lookup
!
!
mpls label range 16 800000
mpls label protocol ldp
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
class-map match-any CM-VoIP
 match mpls experimental topmost 5
 match ip precedence 5
class-map match-any CM-Controlred
 match mpls experimental topmost 6  7
 match ip precedence 6  7
class-map match-any CM-Video
 match mpls experimental topmost 4
 match ip precedence 4
class-map match-any CM-Datoscriticos
 match mpls experimental topmost 2  3
 match ip precedence 2  3
class-map match-any CM-Datosnocriticos
 match mpls experimental topmost 1
 match ip precedence 1
!
!
policy-map PM-QoSBB
 class CM-VoIP
  police rate percent 15
    conform-action transmit
    exceed-action drop
```

```
  priority percent 15
 class CM-Controlred
  bandwidth percent 3
 class CM-Video
  bandwidth percent 20
  queue-limit 20
 class CM-Datoscriticos
  bandwidth percent 20
  random-detect
  random-detect precedence 2   20    50
  random-detect precedence 3   30    60
 class CM-Datosnocriticos
  bandwidth percent 15
  random-detect
  random-detect precedence 1   40    70
 class class-default
  fair-queue
  random-detect
  random-detect precedence 0   80    200
!
!
!
!
interface Loopback199
 description #### Loopback ID ####
 ip address 10.116.254.10 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 description ### link P01GYE ###
 mtu 1532
 bandwidth 10000000
 ip address 10.116.253.1 255.255.255.252
 load-interval 30
 negotiation auto
 mpls ip
 service-policy output PM-QoSBB
!
interface GigabitEthernet2/0
```

```
 description ### link P01CUE ###
 mtu 1532
 bandwidth 10000000
 ip address 10.116.253.5 255.255.255.252
 load-interval 30
 negotiation auto
 mpls ip
 service-policy output PM-QoSBB
!
interface GigabitEthernet3/0
 description ### link PE01UIO ###
 mtu 1532
 bandwidth 10000000
 ip address 10.116.253.97 255.255.255.252
 load-interval 30
 negotiation auto
 mpls ip
 service-policy output PM-QoSBB
!
router ospf 1
 router-id 10.116.254.10
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 redistribute connected
 network 10.116.253.1 0.0.0.0 area 0
 network 10.116.253.5 0.0.0.0 area 0
 network 10.116.253.97 0.0.0.0 area 0
 network 10.116.254.10 0.0.0.0 area 0
!
router bgp 666
 bgp router-id 10.116.254.10
 no bgp default ipv4-unicast
 bgp cluster-id 0.0.0.2
 bgp log-neighbor-changes
 neighbor 10.116.254.11 remote-as 666
 neighbor 10.116.254.11 description PE01UI
 neighbor 10.116.254.11 update-source Loop
 neighbor 10.116.254.20 remote-as 666
 neighbor 10.116.254.20 description P01GYE
 neighbor 10.116.254.20 update-source Loop
 neighbor 10.116.254.21 remote-as 666
 neighbor 10.116.254.21 description PE01GY
 neighbor 10.116.254.21 update-source Loop
 neighbor 10.116.254.30 remote-as 666
```

```
 neighbor 10.116.254.30 description P01CUE
 neighbor 10.116.254.30 update-source Loop
 neighbor 10.116.254.31 remote-as 666
 neighbor 10.116.254.31 description PE01CU
 neighbor 10.116.254.31 update-source Loop
 !
 address-family vpnv4
 neighbor 10.116.254.11 activate
 neighbor 10.116.254.11 send-community bot
 neighbor 10.116.254.11 route-reflector-cl
 neighbor 10.116.254.11 next-hop-self
 neighbor 10.116.254.20 activate
 neighbor 10.116.254.20 send-community bot
 neighbor 10.116.254.20 route-reflector-cl
 neighbor 10.116.254.20 next-hop-self
 neighbor 10.116.254.21 activate
 neighbor 10.116.254.21 send-community bot
 neighbor 10.116.254.21 route-reflector-cl
 neighbor 10.116.254.21 next-hop-self
 neighbor 10.116.254.30 activate
 neighbor 10.116.254.30 send-community bot
 neighbor 10.116.254.30 route-reflector-cl
 neighbor 10.116.254.30 next-hop-self
 neighbor 10.116.254.31 activate
 neighbor 10.116.254.31 send-community bot
 neighbor 10.116.254.31 route-reflector-cl
 neighbor 10.116.254.31 next-hop-self
 exit-address-family
!
!
no ip http server
!
!
!
!
!
mpls ldp router-id Loopback199 force
!
!
control-plane
!
!
!
!
```

```
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end

P01UIO#
```

Configuración equipo PE01UIO – Quito

```
PE01UIO>ena
PE01UIO#show running
Building configuration...

Current configuration : 4187 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE01UIO
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!
!
ip cef
no ip domain lookup
!
```

```
!
ip vrf espol
 rd 666:100000
 route-target export 666:100000
 route-target import 666:100000
!
mpls label range 16 800000
mpls label protocol ldp
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
class-map match-any CM-VoIP
 match mpls experimental topmost 5
 match ip precedence 5
class-map match-any CM-Controlred
 match mpls experimental topmost 6  7
 match ip precedence 6  7
class-map match-all best_efford
  description todo lo demas
class-map match-all voz
 match  precedence 5
class-map match-any CM-Video
 match mpls experimental topmost 4
 match ip precedence 4
class-map match-any CM-Datoscriticos
 match mpls experimental topmost 2  3
 match ip precedence 2  3
class-map match-any CM-Datosnocriticos
 match mpls experimental topmost 1
 match ip precedence 1
class-map match-all datoscriticos
 match access-group 101
!
```

```
!
policy-map 128kbps
 class voz
  set precedence 5
 class best_efford
  set precedence 1
 class datoscriticos
  set precedence 2
 class class-default
  police cir 128000 bc 4000 be 4000
    exceed-action drop
policy-map 256kbps
 class class-default
  police cir 256000 bc 8000 be 8000
    exceed-action drop
policy-map PM-QoSBB
 class CM-VoIP
  police rate percent 15
    conform-action transmit
    exceed-action drop
  priority percent 15
 class CM-Controlred
  bandwidth percent 3
 class CM-Video
  bandwidth percent 20
  queue-limit 20
 class CM-Datoscriticos
  bandwidth percent 20
  random-detect
  random-detect precedence 2   20    50
  random-detect precedence 3   30    60
 class CM-Datosnocriticos
  bandwidth percent 15
  random-detect
  random-detect precedence 1   40    70
 class class-default
  fair-queue
  random-detect
  random-detect precedence 0   80    200
!
!
!
!
interface Loopback199
```

```
 description #### Loopback ID ####
 ip address 10.116.254.11 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 description ### Espol Quito ###
 ip vrf forwarding espol
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 description #### Link1-P01UIO ####
 mtu 1532
 ip address 10.116.253.98 255.255.255.252
 load-interval 30
 negotiation auto
 mpls ip
 mpls mtu 1524
 service-policy output PM-QoSBB
!
interface FastEthernet2/0
 description ### Espol Quito ###
 ip vrf forwarding espol
 ip address 192.168.1.5 255.255.255.252
 duplex half
 service-policy input 128kbps
 service-policy output 128kbps
!
router ospf 1
 router-id 10.116.254.11
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 network 10.116.253.98 0.0.0.0 area 0
 network 10.116.254.11 0.0.0.0 area 0
!
router bgp 666
 bgp router-id 10.116.254.11
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 10.116.254.10 remote-as 666
 neighbor 10.116.254.10 description P01UIO
 neighbor 10.116.254.10 update-source Loopback199
 neighbor 10.116.254.20 remote-as 666
```

```
 neighbor 10.116.254.20 description P01GYE
 neighbor 10.116.254.20 update-source Loopback199
 neighbor 10.116.254.30 remote-as 666
 neighbor 10.116.254.30 description P01CUE
 neighbor 10.116.254.30 update-source Loopback199
 !
 address-family vpnv4
 neighbor 10.116.254.10 activate
 neighbor 10.116.254.10 send-community both
 neighbor 10.116.254.10 next-hop-self
 neighbor 10.116.254.10 route-map RM-RRin in
 neighbor 10.116.254.20 activate
 neighbor 10.116.254.20 send-community both
 neighbor 10.116.254.20 next-hop-self
 neighbor 10.116.254.20 route-map RM-RRin in
 neighbor 10.116.254.30 activate
 neighbor 10.116.254.30 send-community both
 neighbor 10.116.254.30 next-hop-self
 neighbor 10.116.254.30 route-map RM-RRin in
 exit-address-family
 !
 address-family ipv4 vrf espol
 redistribute connected
 redistribute static
 no synchronization
 exit-address-family
!
!
no ip http server
!
ip bgp-community new-format
!
!
access-list 101 permit icmp any any
!
route-map RM-RRin permit 50
!
!
!
!
control-plane
!
!
!
```

```
!
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end

PE01UIO#
```

Configuración equipo P01CUE – Cuenca

```
P01CUE>ena
P01CUE#show running
Building configuration...

Current configuration : 4400 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P01CUE
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!
!
ip cef
no ip domain lookup
!
```

```
!
mpls label range 16 800000
mpls label protocol ldp
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
class-map match-any CM-VoIP
 match mpls experimental topmost 5
 match ip precedence 5
class-map match-any CM-Controlred
 match mpls experimental topmost 6  7
 match ip precedence 6  7
class-map match-any CM-Video
 match mpls experimental topmost 4
 match ip precedence 4
class-map match-any CM-Datoscriticos
 match mpls experimental topmost 2  3
 match ip precedence 2  3
class-map match-any CM-Datosnocriticos
 match mpls experimental topmost 1
 match ip precedence 1
!
!
policy-map PM-QoSBB
 class CM-VoIP
  police rate percent 15
    conform-action transmit
    exceed-action drop
  priority percent 15
 class CM-Controlred
  bandwidth percent 3
 class CM-Video
  bandwidth percent 20
```

```
  queue-limit 20
 class CM-Datoscriticos
  bandwidth percent 20
  random-detect
  random-detect precedence 2   20    50
  random-detect precedence 3   30    60
 class CM-Datosnocriticos
  bandwidth percent 15
  random-detect
  random-detect precedence 1   40    70
 class class-default
  fair-queue
  random-detect
  random-detect precedence 0   80    200
!
!
!
!
interface Loopback199
 ip address 10.116.254.30 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 description ### link P01GYE ###
 mtu 1532
 bandwidth 10000000
 ip address 10.116.253.10 255.255.255.252
 no ip redirects
 no ip proxy-arp
 load-interval 30
 negotiation auto
 mpls ip
 service-policy output PM-QoSBB
!
interface GigabitEthernet2/0
 description ### Link P01UIO ###
 mtu 1532
 bandwidth 10000000
 ip address 10.116.253.6 255.255.255.252
```

```
 no ip redirects
 no ip proxy-arp
 load-interval 30
 negotiation auto
 mpls ip
 service-policy output PM-QoSBB
!
interface GigabitEthernet3/0
 description ### Link PE01CUE ###
 mtu 1532
 bandwidth 10000000
 ip address 10.116.253.225 255.255.255.252
 no ip redirects
 no ip proxy-arp
 load-interval 30
 negotiation auto
 mpls ip
 service-policy output PM-QoSBB
!
router ospf 1
 router-id 10.116.254.30
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 redistribute connected
 network 10.116.253.6 0.0.0.0 area 0
 network 10.116.253.10 0.0.0.0 area 0
 network 10.116.253.225 0.0.0.0 area 0
 network 10.116.254.30 0.0.0.0 area 0
!
router bgp 666
 bgp router-id 10.116.254.30
 no bgp default ipv4-unicast
 bgp cluster-id 0.0.0.3
 bgp log-neighbor-changes
 neighbor 10.116.254.10 remote-as 666
 neighbor 10.116.254.10 description P01UIO
 neighbor 10.116.254.10 update-source Loopback199
 neighbor 10.116.254.11 remote-as 666
 neighbor 10.116.254.11 description PE01UIO
 neighbor 10.116.254.11 update-source Loopback199
 neighbor 10.116.254.20 remote-as 666
 neighbor 10.116.254.20 description P01UIO
 neighbor 10.116.254.20 update-source Loopback199
 neighbor 10.116.254.21 remote-as 666
```

```
 neighbor 10.116.254.21 description PE01UIO
 neighbor 10.116.254.21 update-source Loopback199
 neighbor 10.116.254.31 remote-as 666
 neighbor 10.116.254.31 description PE01CUE
 neighbor 10.116.254.31 update-source Loopback199
 !
 address-family vpnv4
 neighbor 10.116.254.10 activate
 neighbor 10.116.254.10 send-community both
 neighbor 10.116.254.10 route-reflector-client
 neighbor 10.116.254.10 next-hop-self
 neighbor 10.116.254.11 activate
 neighbor 10.116.254.11 send-community both
 neighbor 10.116.254.11 route-reflector-client
 neighbor 10.116.254.11 next-hop-self
 neighbor 10.116.254.20 activate
 neighbor 10.116.254.20 send-community both
 neighbor 10.116.254.20 route-reflector-client
 neighbor 10.116.254.20 next-hop-self
 neighbor 10.116.254.21 activate
 neighbor 10.116.254.21 send-community both
 neighbor 10.116.254.21 route-reflector-client
 neighbor 10.116.254.21 next-hop-self
 neighbor 10.116.254.31 activate
 neighbor 10.116.254.31 send-community both
 neighbor 10.116.254.31 route-reflector-client
 neighbor 10.116.254.31 next-hop-self
 exit-address-family
!
!
no ip http server
!
!
!
!
!
mpls ldp router-id Loopback199 force
!
!
control-plane
!
!
!
!
```

```
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end
```

Configuración equipo PE01UIO - Cuenca

```
PE01CUE>ena
PE01CUE#show running
Building configuration...

Current configuration : 3309 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE01CUE
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
!
!
ip cef
no ip domain lookup
!
!
mpls label range 16 800000
mpls label protocol ldp
```

```
!
!
!
!
!
!
!
!
!
!
!
!
!
!
class-map match-any CM-VoIP
 match mpls experimental topmost 5
 match ip precedence 5
class-map match-any CM-Controlred
 match mpls experimental topmost 6  7
 match ip precedence 6  7
class-map match-any CM-Video
 match mpls experimental topmost 4
 match ip precedence 4
class-map match-any CM-Datoscriticos
 match mpls experimental topmost 2  3
 match ip precedence 2  3
class-map match-any CM-Datosnocriticos
 match mpls experimental topmost 1
 match ip precedence 1
!
!
policy-map PM-QoSBB
 class CM-Controlred
  bandwidth percent 3
 class CM-Video
  bandwidth percent 20
  queue-limit 20
 class CM-Datoscriticos
  bandwidth percent 20
  random-detect
  random-detect precedence 2   20    50
  random-detect precedence 3   30    60
 class CM-Datosnocriticos
  bandwidth percent 15
```

```
  random-detect
  random-detect precedence 1   40    70
 class CM-VoIP
  police rate percent 15
    conform-action transmit
    exceed-action drop
  priority percent 15
 class class-default
  fair-queue
  random-detect
  random-detect precedence 0   80    200
!
!
!
!
interface Loopback199
 description #### Loopback ID ####
 ip address 10.116.254.31 255.255.255.255
 ip ospf network point-to-point
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 description #### Link1-P01CUE ####
 mtu 1532
 ip address 10.116.253.226 255.255.255.252
 no ip redirects
 no ip proxy-arp
 load-interval 30
 negotiation auto
 mpls ip
 mpls mtu 1524
 service-policy output PM-QoSBB
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex half
!
router ospf 1
 router-id 10.116.254.31
```

```
 log-adjacency-changes
 auto-cost reference-bandwidth 10000
 network 10.116.253.226 0.0.0.0 area 0
 network 10.116.254.31 0.0.0.0 area 0
!
router bgp 666
 bgp router-id 10.116.254.31
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 10.116.254.10 remote-as 666
 neighbor 10.116.254.10 description P01UIO
 neighbor 10.116.254.10 update-source Loopback199
 neighbor 10.116.254.20 remote-as 666
 neighbor 10.116.254.20 description P01GYE
 neighbor 10.116.254.20 update-source Loopback199
 neighbor 10.116.254.30 remote-as 666
 neighbor 10.116.254.30 description P01CUE
 neighbor 10.116.254.30 update-source Loopback199
 !
 address-family vpnv4
 neighbor 10.116.254.10 activate
 neighbor 10.116.254.10 send-community both
 neighbor 10.116.254.10 next-hop-self
 neighbor 10.116.254.10 route-map RM-RRin in
 neighbor 10.116.254.20 activate
 neighbor 10.116.254.20 send-community both
 neighbor 10.116.254.20 next-hop-self
 neighbor 10.116.254.20 route-map RM-RRin in
 neighbor 10.116.254.30 activate
 neighbor 10.116.254.30 send-community both
 neighbor 10.116.254.30 next-hop-self
 neighbor 10.116.254.30 route-map RM-RRin in
 exit-address-family
!
!
no ip http server
!
ip bgp-community new-format
!
!
!
route-map RM-RRin permit 50
!
!
```

```
!
!
control-plane
!
!
!
!
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
!
!
end

PE01CUE#
```