UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SERVICIO VPN-MPLS INTERNACIONAL

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

REYNALDO DAVILA BUENDIA

PROMOCIÓN

1975-II

LIMA – PERÚ

2006

SERVICIO VPN-MPLS INTERNACIONAL

Dedico este trabajo a:

Mis padres, inspiración plena de lucha y sacrifico,

Mi Esposa, por el apoyo incondicional en mi carrera,

Y mis hijos esperanza de superación.

SUMARIO

El presente trabajo tiene como objetivo describir el servicio VPN-MPLS Internacional, la cual es un nuevo tipo de acceso que permite la interconexión de redes locales globalmente distribuidas, soportado por Plataformas IP-MPLS , lo cual facilita permite la integración de oficinas y aplicaciones en el ámbito corporativo mundial. Este servicio facilita la creación de redes privadas virtuales que garantizan una alta disponibilidad y seguridad en las comunicaciones de los clientes de este servicio.

En el capitulo I se ofrece una explicación del funcionamiento de una plataforma IP-MPLS, comparándolo con otras tecnologías, demostrando las ventajas en escalabilidad y la transferencia de las comunicaciones IP.

El capitulo II se refiere a los servicios que se ofrecen en una Red IP-MPLS , tal como el de la comunicación a Internet y VPN locales.

El capitulo III se trata de la descripción de los servicios que se ofrecen en toda red local IP-MPLS, destacándose los de acceso a Internet y los del servicio VPN..

El capitulo IV de describe la interconexión entre las redes IP-MPLS presentando los escenarios utilizados en los servicios VPN internacional.

El capítulo V , se refiere a las plantillas utilizadas en la configuración de los equipos de clientes y de red para brindar el Servicio VPN Internacional.

El capítulo VI menciona la metodología para solucionar problemas que ocurren en este servicio

El capitulo VII , hace referencia a la utilización de los enlaces de respaldo que se utiliza para garantizar la continuidad del servicio VPN Internacional.

ÍNDICE

PRÓLOGO

Las comunicaciones hoy en dia, estan consideradas como un elemento importante en la vida del hombre , ya que el desarrollo de esta necesidad nos hace mantener dentro del progreso y dinamica que actualmente se establece en la economia globalizada Esta corriente esta permitiendo que las empresas o instituciones comerciales , educativas o de otra indole , se expandan hacia otros paises , con lo cual crean una necesidad de interconectarse entre si al igual que lo vienen haciendo en su entorno local , manteniendo o superando los mismo beneficios que cuentan actualmente como son el de la salida hacia el mundo Internet , manteniendo una alta seguridad en sus comunicaciones entre sus oficinas.

Actualmente estamos asistiendo a un proceso de globalización de los mercados empresariales, lo que hace estrategico que toda Empresa que interviene en este proceso cuente con todas las ventajas competitivas una de ellas es la que se refiere a las Telecomunicaciones.

VPN MPLS Internacional es un servicio de interconexión de redes locales globalmente distribuidas soportado sobre infraestructura MPLS, que permite una òptima integración de oficinas y aplicaciones en el àmbito corporativo mundial, permitiendo un abaratamiento de los costes y mejora en el rendimiento de las comunicaciones de las Empresas Multinacionales.

El trabajo pretende dar una visión de la provision de lo servicios VPN MPLS presente Internacional, caracterizado por las configuraciones en los elementos de red que intervienen en este servicio.

CAPITULO I
FUNCIONAMIENTO DE UNA RED IP MPLS

1.1. Introduccion

El crecimiento imparable de la Internet, así como la demanda sostenida de nuevos y más sofisticados servicios, supone cambios tecnológicos fundamentales respecto a las Prácticas habituales desarrolladas a mitad de los años 90. Nuevas tecnologías de transmisión sobre fibra óptica, tales como Dense Wavelength Division Multiplexing (DWDM), proporcionan una eficaz alternativa al ATM para multiplexar múltiples servicios sobre circuitos individuales. Además, los tradicionales conmutadores ATM están siendo desplazados por una nueva generación de routers con funciones especializadas en el transporte de paquetes en el núcleo de las redes.

Esta situación se complementa con una nueva arquitectura de red de reciente aparición, conocida como Multi-Prototocol Label Switching (MPLS). Uno de los factores de éxito de la Internet actual está en la acepción de los protocolos TCP/IP como estándar de facto para todo tipo de servicios y aplicaciones.

La Internet ha desplazado a las tradicionales redes de datos y ha llegado a ser el modelo de red pública del siglo XXI. Pero si bien es cierto que la Internet puede llegar a consolidarse como el modelo de red pública de datos a gran escala, también lo es que no llega a satisfacer ahora todos los requisitos de los usuarios, principalmente los de aquellos de entornos corporativos, que necesitan la red para el soporte de aplicaciones críticas. Una carencia fundamental de la Internet es la imposibilidad de seleccionar diferentes niveles de servicio para los

distintos tipos de aplicaciones de usuario. La Internet se valora más por el servicio de acceso y distribución de contenidos que por el servicio de transporte de datos, conocido como de "best-effort". Si el modelo Internet ha de consolidarse como la red de datos del próximo
milenio, se necesita introducir cambios tecnológicos fundamentales, que permitan ir más allá del nivel best-effort y puedan proporcionar una respuesta más determinística y menos aleatoria.

Junto a los últimos avances tecnológicos en transmisión por fibra óptica (principalmente DWDM), que lleva a conseguir anchos de banda demagnitudes muy superiores, y en tecnología de integración de circuitos ASIC (Application Specific Integrated Circuits), que permite aumentar enormemente la velocidad de proceso de información en la red, hemos de considerar la arquitectura MPLS, sustrato para la inclusión en la red de nuevas aplicaciones y para poder ofrecer diferentes niveles de servicio, en un entorno de mayor fiabilidad y con las necesarias garantías.

MPLS es un estándar emergente del IETF que surgió para consensuar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los 90. Como concepto, MPLS es a veces un tanto difícil de explicar. Como protocolo es bastante sencillo, pero lasimplicaciones que supone su implementación real son enormemente complejas.Según el énfasis (o interés) que se ponga a la hora de explicar sus características y utilidad, MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM. También como un protocolo para hacer túneles (sustituyendo a las técnicas habituales de "tunneling"). O bien, como una técnica para acelerar el encaminamiento de paquetes, incluso,para eliminar por completo el routing. En realidad, MPLS hace un poco de todo eso, ya que integra sin discontinuidades los niveles 2(transporte) y 3 (red), combinando eficazmente las funciones de control del routing con la simplicidad y rapidez de la conmutación de nivel 2

Pero, ante todo y sobre todo, debemos considerar MPLS como el avance más reciente en la evolución de las tecnologías de routing y forwarding en las redes IP, lo que implica una evolución en la manera de construir y gestionar estas redes.

Los problemas que presentan las soluciones actuales de IP sobre ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes separadas y tecnológicamente diferentes, quedan resueltos con MPLS. Al combinar en uno solo lo mejor de cada nivel (la inteligencia del routing con la rapidez del switching), MPLS ofrece nuevas posibilidades en la gestión de backbones, así como en la provisión de nuevos servicios de valor añadido. Para poder entender mejor las ventajas de la solución MPLS, vale la pena revisar antes los esfuerzos anteriores de integración de los niveles 2 y 3 que han llevado finalmente a la adopción del estándar MPLS.

1.2. Convergencia de niveles: IP sobre ATM

A mediados de los 90 IP fue ganando terreno como protocolo de red a otras arquitecturas en uso (SNA, IPX, AppleTalk, OSI...). Por otro lado, hay que recordar que los backbones IP que los proveedores de servicio (NSP) habían empezado a desplegar en esos años estaban construidos a base de routers conectados por líneas dedicadas T1/E1 y T3/E3. El crecimiento explosivo del Internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. Las respuestas de los NSPs fue el incremento del número de enlaces y de la capacidad de los mismos. Del mismo modo, los NSPs se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Con los protocolos habituales de encaminamiento (basados en métricas del menor número de saltos), ese aprovechamiento del ancho de banda global no resultaba efectivo. Había que idear otras alternativas de ingeniería de tráfico.

Como consecuencia, se impulsaron los esfuerzos para poder aumentar el rendimiento de los routers tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los routers IP.

A favor de integrar los niveles 2 y 3 estaba el hecho de las infraestructuras de redes ATM que estaban desplegando los operadores de telecomunicaciones.

Estas redes ofrecían entonces (1995-97) una buena solución a los problemas de crecimiento de los NSPs. Por un lado, proporcionaba mayores velocidades (155 Mpbs) y, por otro, las características de respuesta determinísticas de los circuitos virtuales ATM posibilitaban la implementación de soluciones de ingeniería de tráfico. El modelo de red "IP sobre ATM"(IP/ATM) pronto ganó adeptos entre la comunidad de NSPs, a la vez que facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a la Internet al por mayor.

El funcionamiento IP/ATM supone la superposición de una topología virtual de routers IP sobre una topología real de conmutadores ATM. El backbone ATM se presenta como una nube central (el núcleo) rodeada por los routers de la periferia. Cada router comunica con el resto mediante los circuitos virtuales permanentes (PVCs) que se establecen sobre la topología física de la red ATM. Los PVCs actúan como circuitos lógicos y proporcionan la conectividad necesaria entre los routers de la periferia. Estos, sin embargo, desconocen la topología real de la infraestructura ATM que sustenta los PVCs. Los routers ven los PVCs como enlaces punto a punto entre cada par. En la figura 1.1 se representa un ejemplo en el que se puede comparar la diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta mostrada en la figura 1.2.

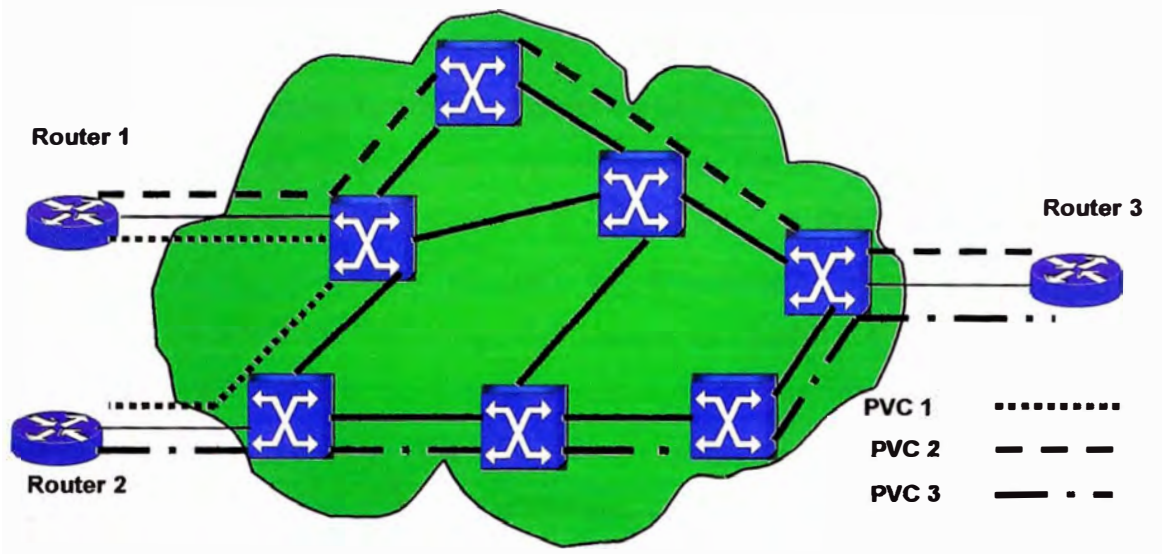

Fig. 1.1 Topologia física (nivel 2)

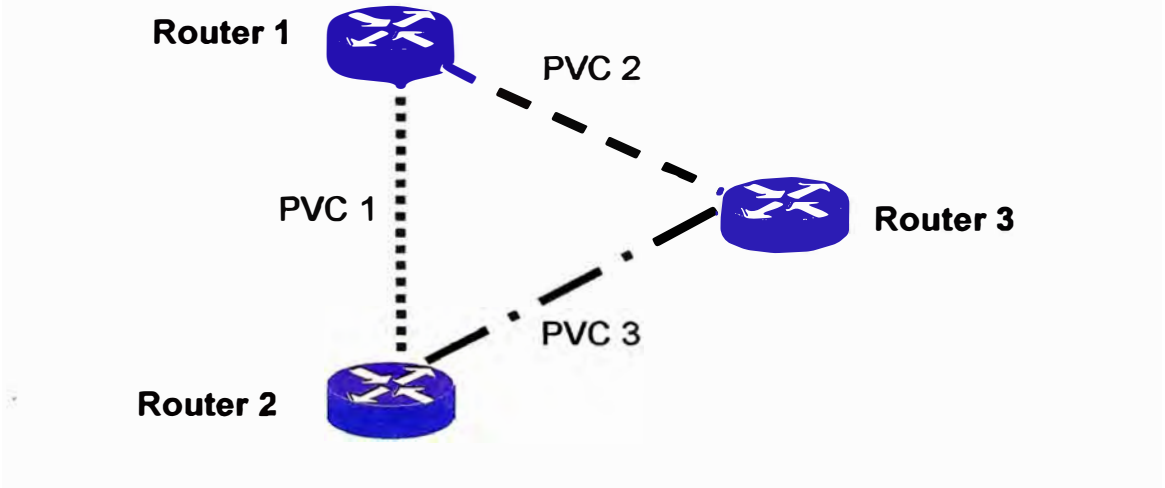

Fig. 1.2 Topologia lògica (nivel 3)

La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y routing) y el envío de las celdas por hardware (conmutación). En realidad, los PVCs se establecen a base de intercambiar etiquetas en cada conmutador de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los correspondientes PVCs. (Más adelante se verá que el intercambio de etiquetas es uno de los componentes fundamentales en la arquitectura MPLS). Las etiquetas tienen solamente significado local en los conmutadores y son la base de la rapidez en la conmutación de celdas.

La potencia de esta solución de topologías superpuestas está en la infraestructura ATM del backbone; el papel de los routers IP queda relegado a la periferia, que, a mitad de los 90, tenían una calidad cuestionable, al estar basados en funcionamiento por software. En la figura 1.3 se representa el modelo IP/ATM con la separación de funciones entre los que es routing IP en el nivel 3 (control y envío de paquetes) y lo que es conmutación en el nivel 2 (control/señalización y envío de celdas). Aunque se trata de una misma infraestructura física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y, lo que quizás es más sorprendente, concebidas para dos finalidades totalmente distintas.

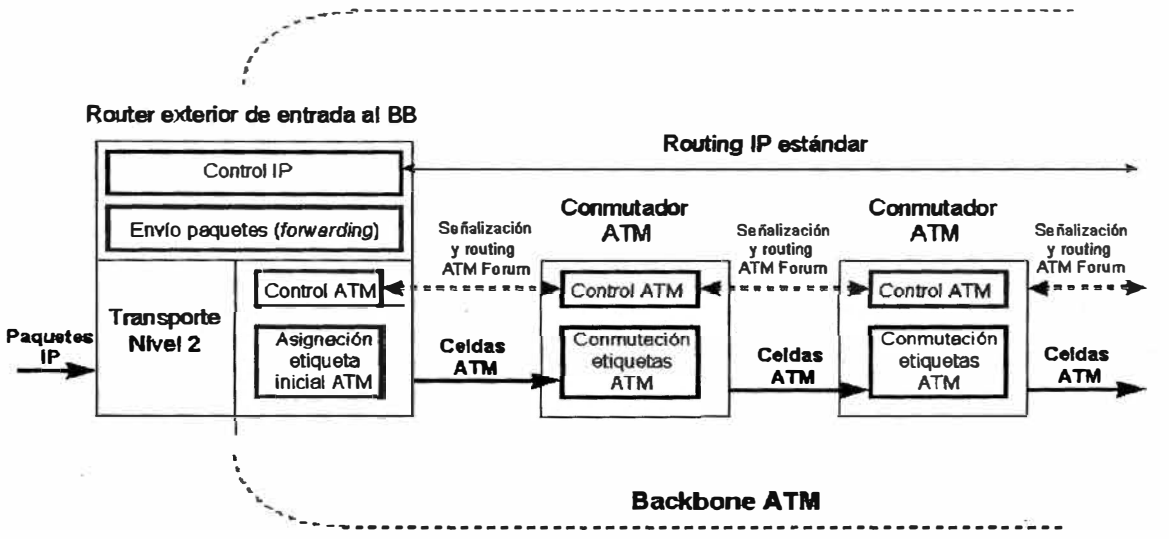

Fig.1.3. Modelo funcional IP sobre ATM

La solución de superponer IP sobre ATM permite aprovechar la infraestructura ATM existente. Las ventajas inmediatas son el ancho de banda disponible a precios competitivos y la rapidez de transporte de datos que proporcionan los conmutadores. En los casos de NSPs de prımer nivel (la mayor parte telcos), ellos poseen y operan el backbone ATM al servicio de sus redes IP. Los caminos físicos de los PVCs se calculan a partir de la necesidades del tráfico IP, utilizando la clase de servicio ATM UBR (Unspecified Bit Rate), ya que en este caso el ATM se utiliza solamente como infraestructura de transporte de alta velocidad (no hay necesidad de apoyarse en los mecanismos inherentes del ATM para control de la congestión y clases de servicio).

La ingeniería de tráfico se hace a base de proporcionar a los routers los PVCs necesarios, con una topología lógica entre routers totalmente mallada. El "punto de encuentro" entre la red IP y la ATM está en el acoplamiento de los subinterfaces en los routers con los PVCs, a través de los cuales se intercambian los routers la información de encaminamiento correspondiente al protocolo interno IGP.

Lo habitual es que, entre cada par de routers, haya un PVC principal y otro de respaldo, que entra automáticamente en funcionamiento cuando falla el principal.

Sin embargo, el modelo IP/ATM tiene también sus inconvenientes: hay que gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio unos mayores costes de gestión global de sus redes. Existe, además, lo que se llama la "tasa impuesta por la celda", un overhead aproximado del 20% que causa e transporte de datagramas IP sobre las celdas ATM y que reduce en ese mismo porcentaje el ancho de banda disponible. Por otro lado, la solución IP/ATM presenta los típicos problemas de crecimiento exponencial nx(n-1) al aumentar el número de nodos IP sobre una topología completamente mallada.

Por ejemplo, en una red con 5 routers externos con una topología Virtual totalmente mallada sobre una red ATM. Son necesarios 5 x 4 = 20PVCs (uno en cada sentido de transmisión). Si se

añade un sexto router se necesitan 10 PVCs más para mantener la misma estructura (6 x 5 = 30). Una pega adicional del crecimiento exponencial de rutas es el mayor esfuerzo que tiene que hacer el correspondiente protocolo IGP.

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

1.3. Convergencia hacia IP: conmutacion IP

La convergencia continuada hacia IP de todas las aplicaciones existentes,junto a los problemas de rendimiento derivados de la solución IP/ATM, llevaron posteriormente (1997-98) a que varios fabricantes desarrollasen técnicas para realizar la integración de niveles de forma efectiva, sin las discontinuidades señalas anteriormente. Esas técnicas se conocieron como "conmutación IP" (IP switching) o "conmutación multinivel" (multilayer switching). Una serie de tecnologías privadas —entre las que merecen citarse: IP Switching de Ipsilon Networks, Tag Switching de Cisco, Aggregate Route-Base IP Switching (ARIS) de IBM, IP Navigator de Cascade/Ascend/Lucent y Cell Switching Router (CSR) de Toshiba, condujeron finalmente a la adopción del actual estándar MPLS del IETF. El problema que presentaban tales soluciones era la falta de interoperatividad, ya que usaban diferentes tecnologías privadas para combinar la conmutación de nivel 2 con el encaminamiento IP (nivel 3).

Se resume a continuación los fundamentos de esas soluciones integradoras, ya que permitirá luego comprender mejor la esencia de la solución MPLS.

Todas las soluciones de conmutación multinivel (incluido MPLS) se basan en dos componentes básicos comunes:

la separación entre las funciones de control (routing) y de envío(forwarding) el paradigma de intercambio de etiquetas para el envío de datos

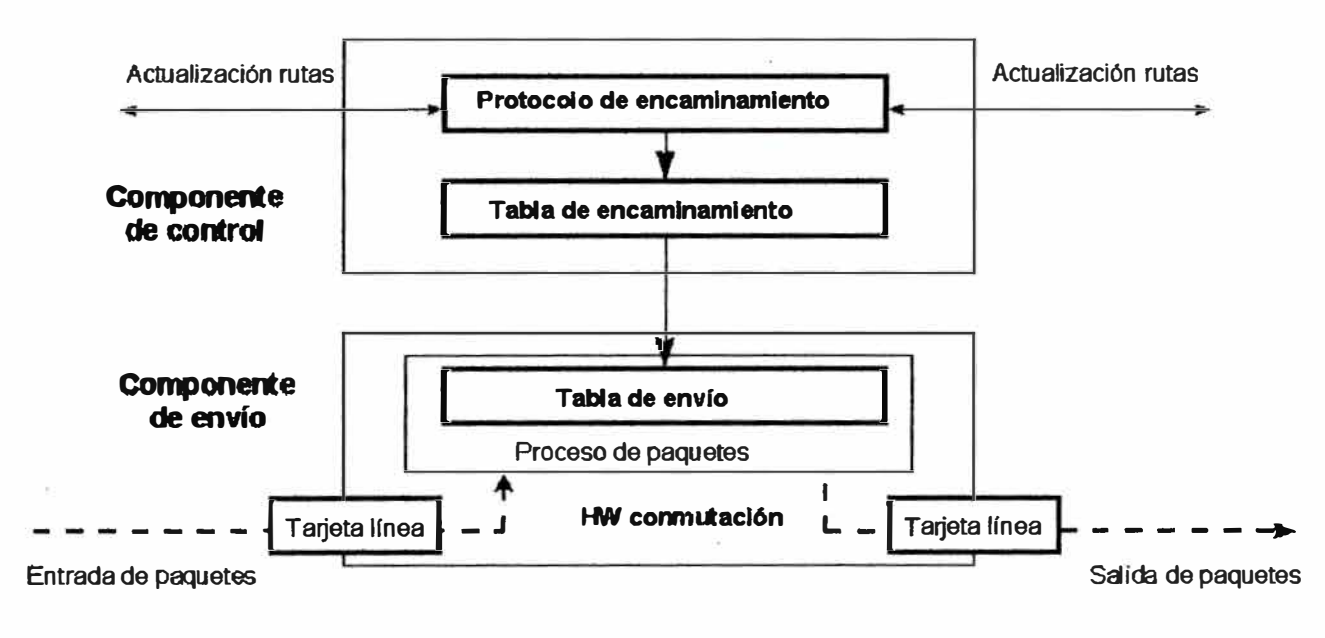

Fig. 1.4. Separación funcional de encaminamiento y envío

En la figura 1.4 se representa la separación funcional de esas dos componentes, una de control y la otra de envío. La componente de control utiliza los protocolos estándar de encaminamiento (OSPF, IS-IS y BGP-4) para el intercambio de información con los otros routers para la construcción y el mantenimiento de las tablas de encaminamiento. Al llegar los paquetes, la componente de envío busca en la tabla de envío, que mantiene la componente de control, para tomar la decisión de encaminamiento para cada paquete. En concreto, la componente de envío examina la información de la cabecera del paquete, busca en la tabla de envío la entrada correspondiente y dirige el paquete desde el interfaz de entrada al de salida a través del correspondiente hardware de conmutación.

Al separar la componente de control (encaminamiento) de la componente de envío, cada una de ella se puede implementar y modificar independientemente. El único requisito es que la componente de encaminamiento mantenga la comunicación con la de envío mediante la tabla de envío de paquetes y actualice la información. El mecanismo de envío se implementa mediante el intercambio de etiquetas, similar a lo visto para

ATM. La diferencia está en que ahora lo que se envía por el interfaz físico de salida son paquetes "etiquetados". De este modo, se está integrando realmente en el mismo sistema las funciones de conmutación y de encaminamiento.

En cuanto a la etiqueta que marca cada paquete, decir que es un campo de unos pocos bits, de longitud fija, que se añade a la cabecera del mismo y que identifica una "clase equivalente de envío" (Forwarding Equivalence Class, FEC). Una FEC es un conjunto de paquetes que se envían sobre el mismo camino a través de una red, aun cuando sus destinos finales sean diferentes. Por ejemplo, en el encaminamiento convencional IP por prefijos de red (longest-match) una FEC serían todos los paquetes unicast cuyas direcciones de destino tengan el mismo prefijo. Realmente, una etiqueta es similar a un identificador de conexión (como el VPI/VCI de ATM o el DLCI de Frame Relay). Tiene solamente significado local y, por consiguiente, no modifica la información de la cabecera de los paquetes; tan sólo los encapsula, asignando el tráfico a los correspondientes FEC.

El algoritmo de intercambio de etiquetas permite así la creación de "caminos virtuales" conocidos como LSP (Label-Switched Paths), funcionalmente equivalentes a los PVCs de ATM y Frame Relay. En el fondo, lo que hace es imponer una conectividad entre extremos a una red no conectiva por naturaleza, como son las redes IP, pero todo ello sin perder la visibilidad del nivel de red (de aquí los nombres de conmutación IP o conmutación multinivel). Esta es la diferencia básica con el modelo IP/ATM. Al hablar de MPLS con más detalle se entenderán mejor estas peculiaridades.

1.4. La convergencia real: MPLS

Ya se dijo anteriormente que el problema principal que presentaban las diversas soluciones de conmutación multinivel era la falta de interoperatividad entre productos privados de diferentes fabricantes. Además de ello, la mayoría de esas soluciones necesitaban ATM como transporte, pues no podían operar sobre infraestructuras de transmisión mixtas (Frame Relay,

PPP, SONET/SDH y LANs). Se quería obtener un estándar que pudiera funcionar sobre cualquier tecnología de transporte de datos en el nivel de enlace. De aquí que el Grupo de Trabajo de MPLS que se estableció en el IETF en 1977 se propuso como objetivo la adopción de un estándar unificado e interoperativo.

Durante el tiempo en que se ha desarrollado el estándar, se han extendido algunas ideas falsas o inexactas sobre el alcance y objetivos de MPLS. Hay quien piensa que MPLS se ha desarrollado para ofrecer un estándar a los vendedores que les permitiese evolucionar los conmutadores ATM a routers de backbone de altas prestaciones. Aunque esta puede haber sido la finalidad original de los desarrollos de conmutación multinivel, los recientes avances en tecnologías de silicio ASIC permite a los routers funcionar con una rapidez similar para la consulta de tablas a las de los conmutadores ATM. Si bien es cierto que MPLS mejora notablemente el rendimiento del mecanismo de envío de paquetes, éste no era el principal objetivo del grupo del IETF. Los objetivos establecidos por ese grupo en la elaboración del estándar eran:

MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM

MPLS debía soportar el envío de paquetes tanto unicast como multicast.

MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP.

MPLS debía permitir el crecimiento constante de la Internet.

MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

También ha habido quien pensó que el MPLS perseguía eliminar totalmente el encaminamiento convencional por prefijos de red. Esta es otra idea falsa y nunca se planteó como objetivo del grupo, ya que el encaminamiento tradicional de nivel 3 siempre sería un requisito en la Internet por los siguientes motivos:

El filtrado de paquetes en los cortafuegos (FW) de acceso a las LAN corporativas y en los límites de las redes de los NSPs es un requisito fundamental para poder gestionar la red y los servicios con las

necesarias garantías de seguridad. Para ello se requiere examinar la información de la cabecera de los paquetes, lo que impide prescindir del uso del nivel 3 en ese tipo de aplicaciones.No es probable que los sistemas finales (hosts) implementen MPLS. Necesitan enviar los paquetes a un primer dispositivo de red (nivel 3)

Que pueda examinar la cabecera del paquete para tomar luego las correspondientes decisiones sobre su envío hasta su destino final. En este primer salto se puede decidir enviarlo por routing convencional o asignar una etiqueta y enviarlo por un LSP.

Las etiquetas MPLS tienen solamente significado local (es imposible mantener vínculos globales entre etiquetas y hosts en toda la Internet).

Esto implica que en algún punto del camino algún dispositivo de nivel 3 debe examinar la cabecera del paquete para determinar con exactitud por dónde lo envía: por routing convencional o entregándolo a un LSR, que lo expedirá por un nuevo LSP.

Del mismo modo, el último LSR de un LSP debe usar encaminamiento de nivel 3 para entregar el paquete al destino, una vez suprimida la etiqueta, como se verá seguidamente al describir la funcionalidad MPLS.

1.5 Descripcion funcional del MPLS

La operación del MPLS se basa en las componentes funcionales de envío y control, aludidas anteriormente, y que actúan ligadas íntimamente entre sí. Empecemos por la primera.

a) Funcionamiento del envío de paquetes en MPLS

La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP por la red.

Los LSPs son simplex por naturaleza (se establecen para un sentido del tráfico en cada punto de entrada a la red); el tráfico dúplex requiere dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un

"conmutador de etiquetas" (Label-Swiching Router) otro, a través del dominio MPLS. Un LSR no es sino un router especializado en el envío de paquetes etiquetados por MPLS.

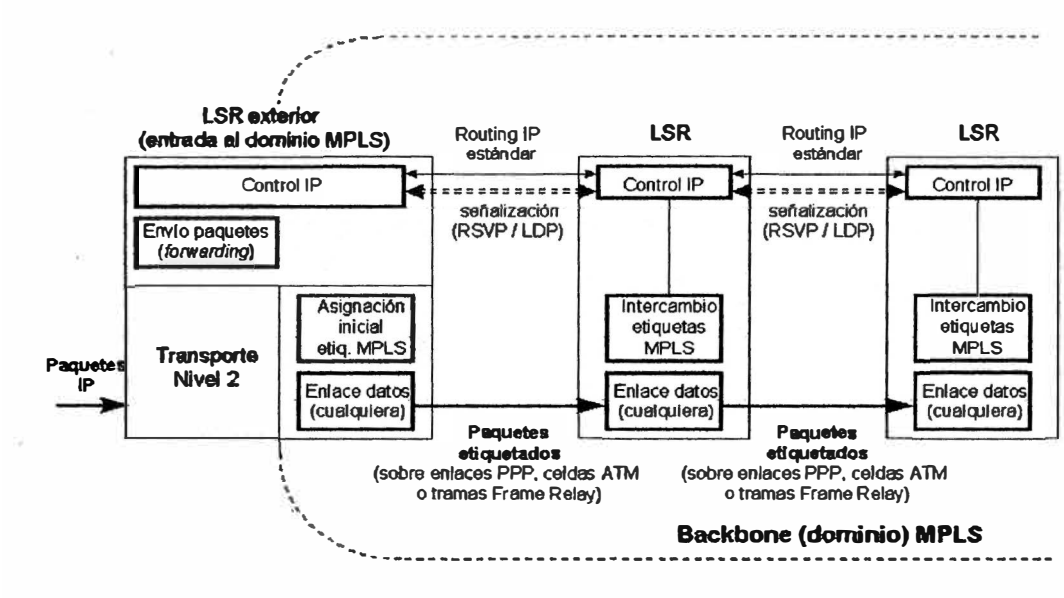

Fig. 1.5. Esquema funcional del MPLS

En la figura 1.5 se puede ver la funcionalidad del MPLS. Compárese con los esquemas vistos antes en las figuras 1.3 y 1.4 para observar las analogías y diferencias. Al igual que en las soluciones de conmutación multinivel, MPLS separa las dos componentes funcionales de control (routing) y de envío (forwarding). Del mismo modo, el envío se implementa mediante el intercambio de etiquetas en los LSPs. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de encaminamiento definidos por el ATM Forum; en lugar de ello, en MPLS o bien se utiliza el protocolo RSVP o bien un nuevo estándar de señalización (el Label Distribution Protocol, LDP, del que se tratará más adelante). Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera. Si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. Ahora ya no hay que administrar dos

arquitecturas diferentes a base de transformar las direcciones IP y las tablas de encaminamiento en las direcciones y el encaminamiento ATM: esto lo resuelve el procedimiento de intercambio de etiquetas MPLS.

El papel de ATM queda restringido al mero transporte de datos a base de celdas.Para MPLS esto es indiferente, ya que puede utilizar otros transportes como Frame Relay, o directamente sobre líneas punto a punto. Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs interiores del dominio MPLS. Un LSR es como un router que funciona a base de intercambiar etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control (recuérdese el esquema de la figura 3), según se verá más adelante. Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por ese interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola). En la figura 1.6 se ilustra un ejemplo del funcionamiento de un LRS del núcleo MPLS. A un paquete que llega al LSR por el interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

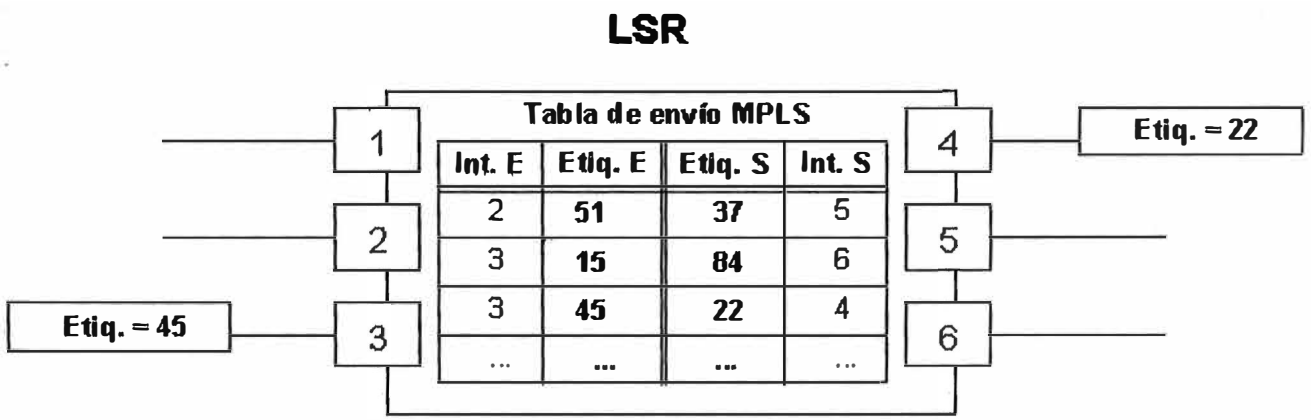

Fig. 1.6 Detalle de la tabla de envío de un LSR

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la figura 1.7 el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP.

Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar el paquete al LSR de cola (salida), ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas quita ésta y envía el paquete por routing convencional.

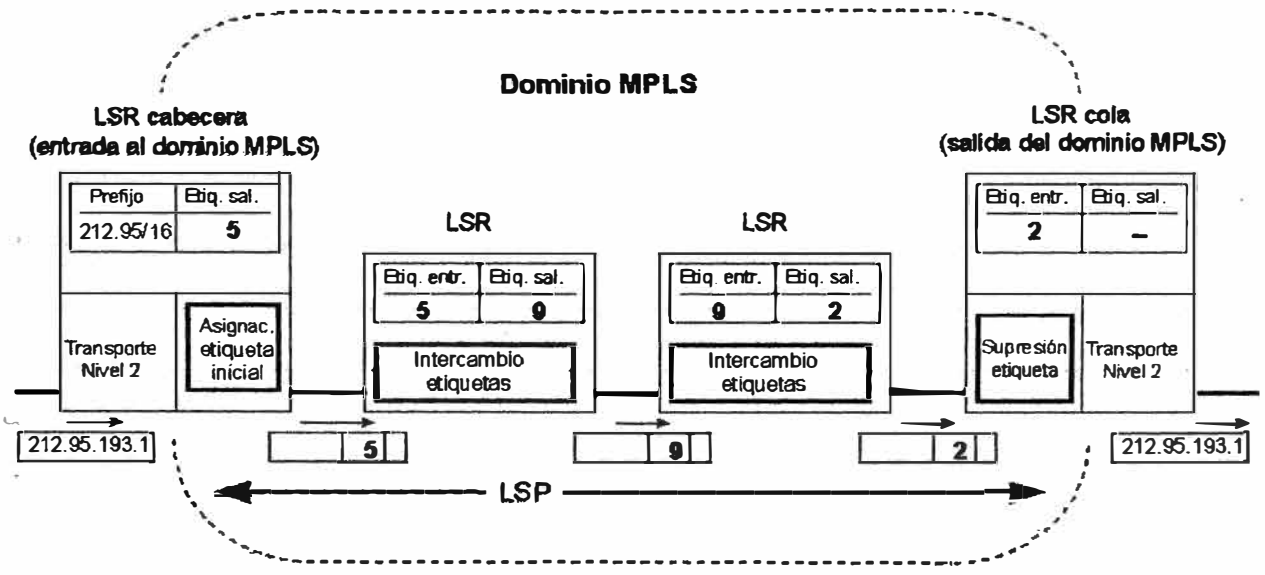

Fig. 1.7 Ejemplo de envío de un paquete por un LSP

Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no "mira" sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los

caminos LSP. Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3. Según las especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. Por ello, si el protocolo transporte de datos contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de Frame Relay), se utilizan esos campos nativo para las etiquetas. Sin embargo, si la tecnología de nivel 2 empleada no soporta un campo para etiquetas (p.ej. enlaces PPP o LAN), entonces se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete (nivel 3).

En la figura 1.8 se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Según se muestra en la figura, los 32 bits de la cabecera MPLS se reparten en:

20 bits para la etiqueta MPLS, 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamdo CoS), 1 bit de stack para poder apilar etiquetas de forma jerárquica (S) y 8 bits para indicar el TTL (time-to-live) que sustenta la funcionalidad estándar TTL de las redes IP. De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.

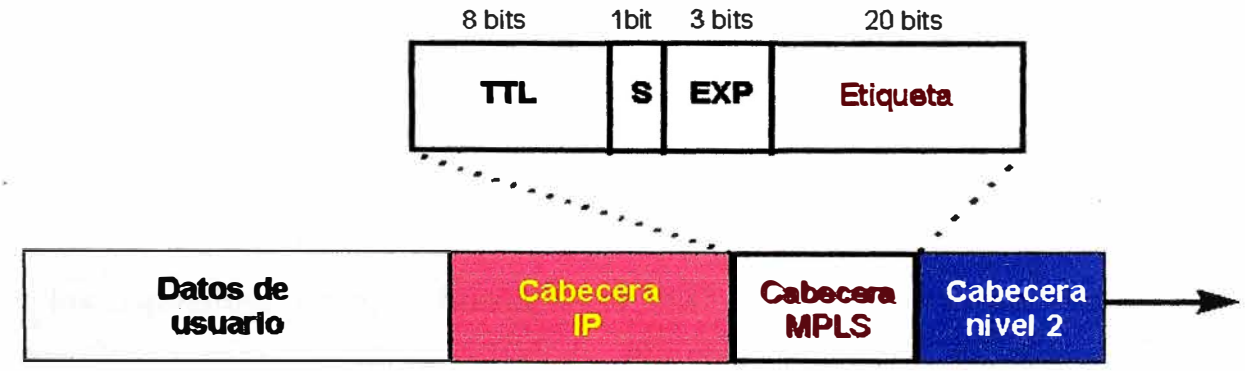

Fig. 1.8 Estructura de la cabecera genérica MPLS

b) Control de la información en MPLS

Hasta ahora se ha visto el mecanismo básico de envío de paquetes a través de los LSPs mediante el procedimiento de intercambio de etiquetas según las tablas de los LSRs. Pero queda por ver dos aspectos fundamentales:

Cómo se generan las tablas de envío que establecen los LSPs Cómo se distribuye la información sobre las etiquetas a los LSRs El primero de ellos está relacionado con la información que se tiene sobre la red: topología, patrón de tráfico, características de los enlaces, etc.

Es la información de control típica de los algoritmos de encaminamiento.MPLS necesita esta información de routing para establecer los caminos virtuales LSPs. Lo más lógico es utilizar la propia información de encaminamiento que manejan los protocolos internos IGP (OSPF, IS-IS,RIP...) para construir las tablas de encaminamiento (recuérdese que los LSR son routers con funcionalidad añadida). Esto es lo que hace MPLS precisamente: para cada "ruta IP" en la red se crea un "camino de etiquetas" a base de concatenar las de entrada/salida en cada tabla de los LSRs; el protocolo interno correspondiente se encarga de pasar la información necesaria.

El segundo aspecto se refiere a la información de "señalización" (las comillas se ponen por el impacto que puede suponer este término para los puristas del mundo IP, de naturaleza no conectiva). Pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; unos de ellos es el protocolo RSVP del Modelo de Servicios Integrados del IETF (recuérdese que ése era uno de los requisitos). Pero, además, en el IETF se están definiendo otros nuevos, específicos para la distribución de etiquetas, cual es el caso del Label Distribution Protocol (LDP).

Consúltese las referencias correspondientes del IETF.

c) Funcionamiento global MPLS

Una vez vistos todos los componentes funcionales, el esquema global de funcionamiento es el que se muestra en la figura 1.9, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de routers IP. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de routers a una distancia de un sólo salto. Funcionalmente es como si estuvieran unidos todos en una topología mallada (directamente o por PVCs ATM). Ahora, esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de routers).La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP. Todo ello abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario, tal como se explica en la sección siguiente.

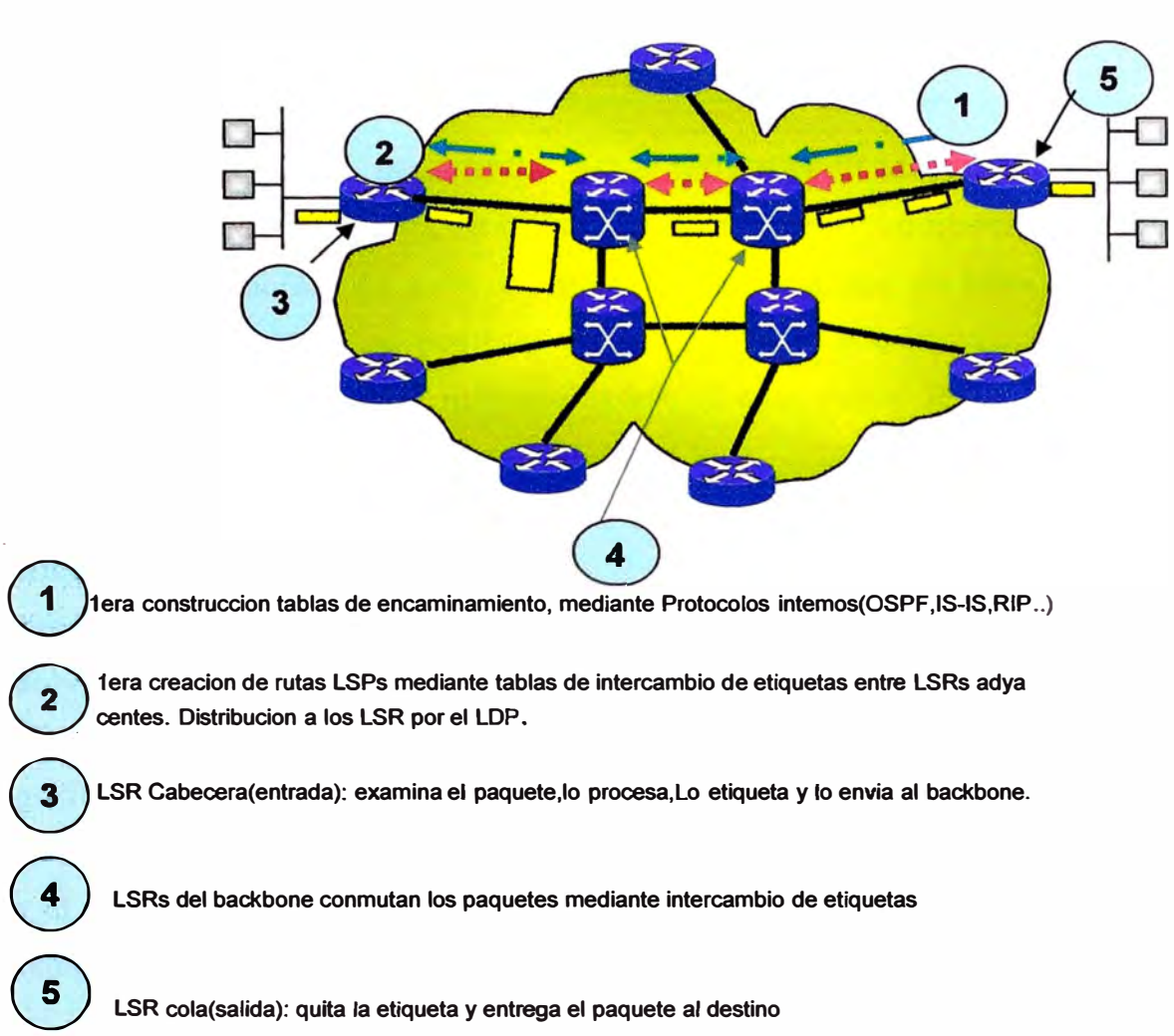

Fig. 1.9 Funcionamiento de una red MPLS

1.6. Aplicaciones de MPLS

Las principales aplicaciones que hoy en día tiene MPLS son:

Ingeniería de tráfico

Diferenciación de niveles de servicio mediante clases (CoS)

Servicio de redes privadas virtuales (VPN)

Veamos brevemente las características de estas aplicaciones y las ventajas que MPLS supone para ello frente a otras soluciones tradicionales.

1.6.1 Ingenieria de tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. A comienzos de los 90 los esquemas para adaptar de forma efectiva los flujos de tráfico a la topología física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos).
En el esquema de la figura 1.10 se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

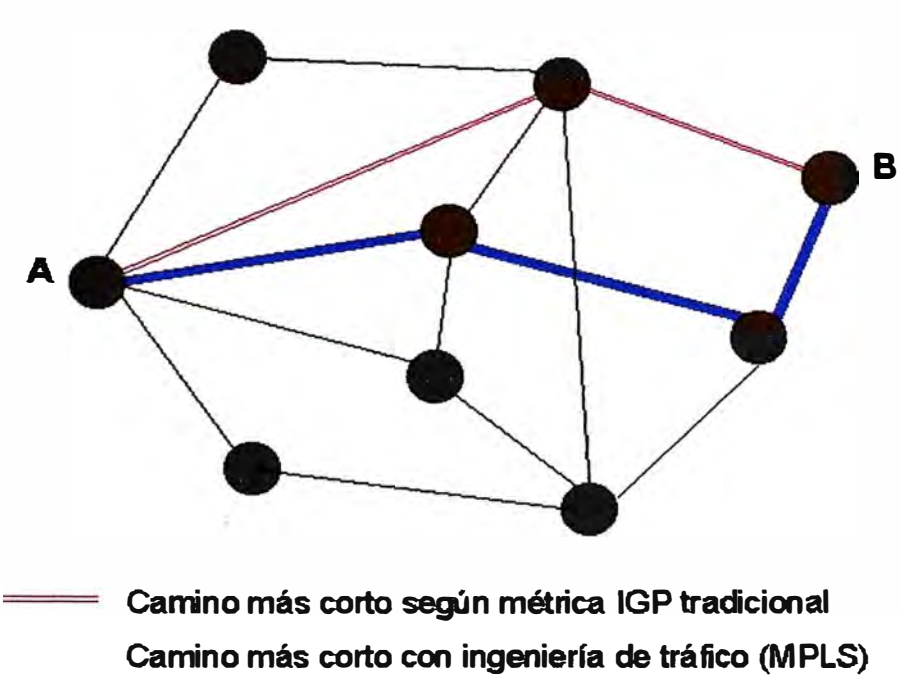

Fig. 1.10 Comparación entre camino más corto IGP con ingeniería de tráfico

El camino más corto entre A y B según la métrica normal IGP es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes hagan aconsejable la utilización del camino alternativo indicado con un salto más. MPLS es una herramienta efectiva para esta aplicación en grandes backbones, ya que: Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP. Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.

Permite hacer "encaminamiento restringido" (Constraint-based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costes de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

1.6.2. Clases de servicio (CoS)

MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ del IETF. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de vídeo y voz interactiva. Para ello se emplea el campo ToS (Type of Service), rebautizado en DiffServ como el octeto DS. (Véase más información sobre el modelo DiffServ en las referencias correspondientes a

QoS). Esta es la técnica QoS de marcar los paquetes que se envían a la red. MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De es te modo, una red MPLS puede transportar distintas clases de tráfico, ya que: el tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. P. ej., un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort, tres niveles de servicio, primera, preferente y turista, que, lógicamente, tendrán distintos precios.

1.6.3. Redes privadas virtuales (VPNs)

Una red privada virtual (VPN) se construye a base de conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet. En esta sección se va a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PCVs entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR).

Algo similar se puede hacer con ATM , con diversas clases de garantías. Los inconvenientes de este tipo de solución es que la configuración de las rutas se

basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión (y los mayores costes asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los CPEs del cliente y restablecer todos los PVCs. (Algo similar a lo que se vio en la solución IP sobre ATM de la sección 2). Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los NSPs, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e implantación y unos menores costes de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos. El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN. No es el objetivo de esta sección
una exposición completa de IP VPNs sobre túneles; se pretende tan sólo resumir sus características para poder apreciar luego las ventajas que ofrece MPLS frente a esas soluciones. Se puede obtener más información sobre IP VPN con túneles en las referencias correspondientes a VPNs con MPLS.Los túneles IP en conexiones dedicadas (no se va a tratar aquí de las conexiones conmutadas de acceso) se pueden establecer de dos maneras:

en el nivel 3, mediante el protocolo IPSec del IETF
en el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un NSP.

En las VPNs basadas en tuneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte

por la red del proveedor. Es relativamente sencillo de implementar, bien sea en dispositivos especializados, tales como
cortafuegos, como en los propios routers de acceso del NSP. Además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos NSPs que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, sólo vale para paquetes IP nativos, IPSec no admite otros protocolos.

En los túneles de nivel 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del NSP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de
direcciones, estableciendo grupos cerrados de usuarios, si así lo desean. (Además de encapsular los paquetes, se puede cifrar la información por mayor seguridad, pero en este caso limitando las opciones QoS). A diferencia de la opción anterior, la operación de túneles de nivel 2 está condicionada a un único proveedor. A pesar de las ventajas de los túneles IP sobre los PVCs, ambos enfoques tienen unas características comunes que las hacen menos eficientes frente a la solución MPLS:

están basadas en conexiones punto a punto (PVCs o túneles) la configuración es manual la provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales la gestión de QoS es posible en cierta medida, pero no se puede mantener
extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte Realmente, el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, a base de túneles extremos a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren

añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS. Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo. Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada rutas MPLS sino que ve una internet privada (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

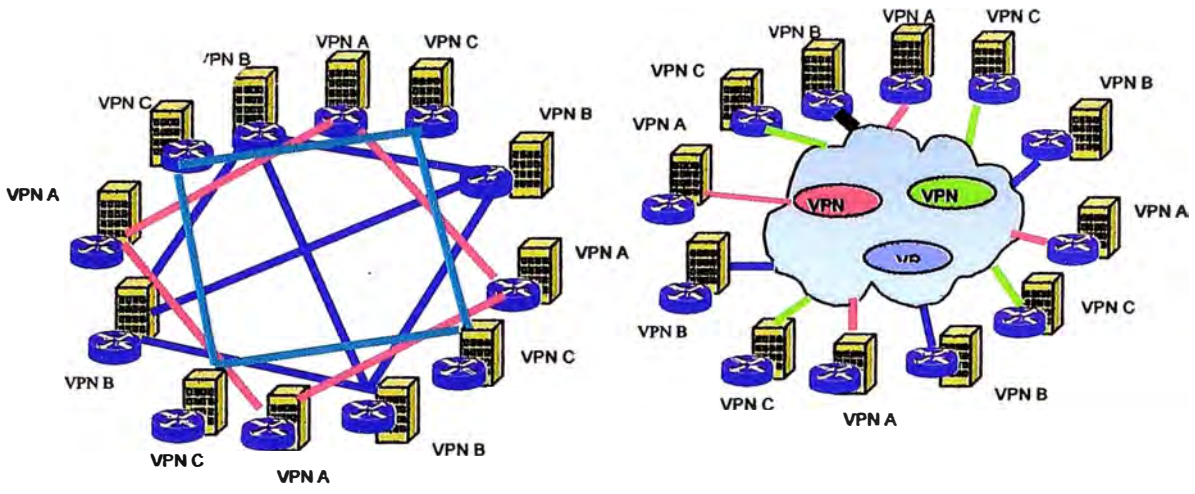

Fig. 1.11 Modelo "superpuesto" (túneles/PVCs) vs. modelo "acoplado"(MPLS).

En la figura 1.11 se representa una comparación entre ambos modelos. La diferencia entre los túneles IP convencionales (o los circuitos virtuales) y los "túneles MPLS" (LSPs) está en que éstos se crean dentro de la red, a base de LSPs, y no de extremo a extremo a través de la red.

Como resumen, las ventajas que MPLS ofrece para IP VPNs son: proporcionan un modelo "acoplado" o "inteligente", ya que la red MPLS "sabe" de la existencia de VPNs (lo que no ocurre con túneles ni PVCs)evita la complejidad de los túneles y PVCs la provisión de servicio es sencilla: una nueva conexión afecta a un solo router. tiene mayores opciones de crecimiento modular,permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada permite aprovechar las posibilidades de ingeniería de tráfic o para poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación...), lo que es necesario para un servicio completo VPN.

En el momento actual, todos los NSPs tienen ante sí el enorme reto de gestionar redes cada vez más complejas y extensas, con una mayor gama de servicios y con creciente demanda de ancho de banda, calidad y garantías.

Para los backbones, las posibilidades que ofrecen la extensión de infraestructuras de fibra óptica y las nuevas tecnologías de transmisión DWDM son enormes.

En este contexto, la evolución natural hacia redes IP y aplicaciones TCP/IP han llevado a desarrollar la arquitectura MPLS como una de las opciones más prometedoras para proporcionar los nuevos servicios del siglo XXI.

MPLS es el último paso en la evolución de las tecnologías de conmutación multinivel (o conmutación IP). La idea básica de separar lo que es el envío de los datos (mediante el algoritmo de intercambio de etiquetas) de los procedimientos de encaminamiento estándar IP, ha llevado a un acercamiento de los niveles 3 y 2, con el consiguiente beneficio en cuanto a rendimiento y flexibilidad de esta arquitectura. Por otro lado, el hecho de que MPLS pueda funcionar sobre cualquier tecnología de transporte —no sólo sobre infraestructuras ATM— va a facilitar de modo significativo la migración para la próxima generación de la Internet óptica, en la que se acortará la distancia entre el nivel de red IP y la fibra.

MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas actuales de encaminamiento IP (típicamente limitadas a encaminar por dirección de destino. Además de poder hacer ingeniería de tráfico IP, MPLS permite mantener clases de servicio y soporta con gran eficacia la creación de VPNs. Por todo ello, MPLS aparece ahora como la gran promesa y esperanza para poder mantener el ritmo actual de crecimiento de la Internet.

CAPITULO II

CONFIGURACION DE SERVICIOS EN UNA RED IP MPLS

En Una Plataforma IP-MPLS, se puede utilizar para brindar diversos servicios de Datos , los mismos que seran ofrecidos a los clientes de acuerdo a la sgts. Clasificacion:

2.1 Configuracion de servicios internet

Los servicios Internet permitiran básicamente la Interconexión de los Terminales (PC) o Hosts con los Proveedores Internacionales de Internet.
Este Servicio se brinda prncipalmente a los diversos Niveles Economicos, los mismos que van desde una Cabina INTERNET, pasando por las medianas y Grandes Empresas.
A continuación pasaremos a describir las principales consideraciones en las configuraciones de los Servicios INTERNET

2.1.1 Servicio ofrecido a las cabinas públicas

Se muestra en la figura 2.1, el diagrama de la Interconexión Tipica de un enlace ofrecido a las Cabinas Publicas. Aquí se puede observar en la Plantilla de la figura 2.2 el comando para habilitar la funcion del NAT (Network Acess Translater. Esta funcion consiste en posibilitar el empleo de direcciones Privadas para conexión a INTERNET, realizando la conversión de las direccione IP privadas en direcciones IP publicas.

- **Funcionabilidad NAT (Network Address Translation)**

Fue una solución que fue desarrollada para preservar el limitado numero de direcciones IP, esta definido por la recomendación RFC 3022, En su configuración mas básica , NAT opera conectando un router a dos redes, tal como se muestra en la figura 2.2 , donde una de ellas (INSIDE) tienen la direccion Privada que tienen que Transformarse en direcciones Públicas (OUTSIDE).

La Translación opera en el Ruteo, asi que solo se configura en el CE (Router Cliente).

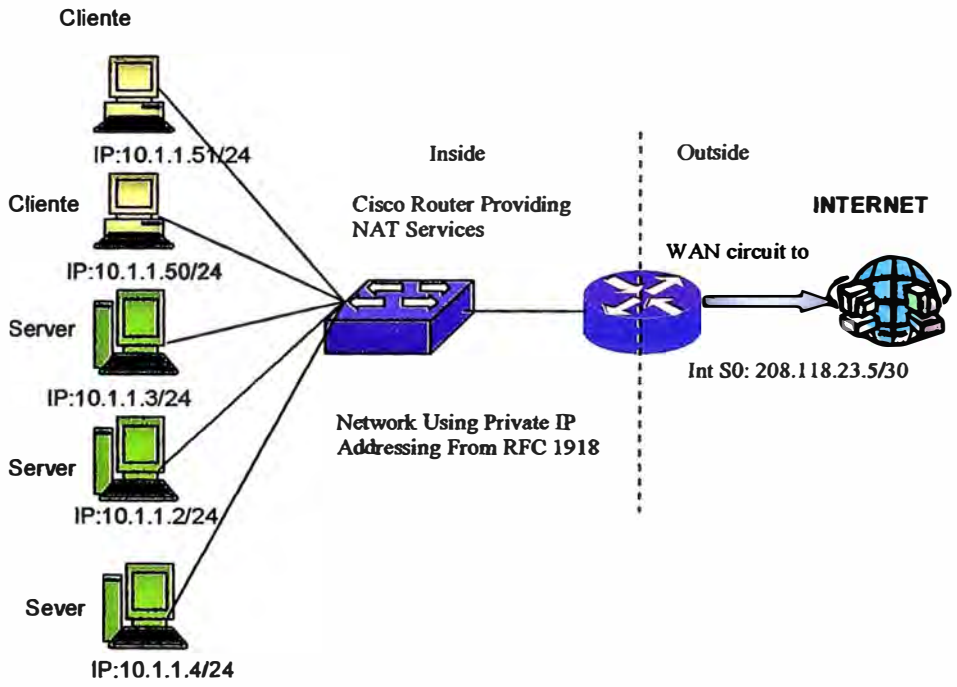

Fig. 2.1 Conexión de cabina publica a Internet

- **Plantilla de configuracion en el PE, para una cabina publica**

Configuración en el Router PE del Service Provider:

Interface Serial10/0/0:5

description CABINA INTERNET CD=37827

ip address 172.22.0.29 255.255.255.252 ---**WAN DE RED**
ip verify unicast reverse-path
no ip redirects
no ip proxy-arp
encapsulation ppp
ip route-cache policy
ip policy route-map INFPLATA
no peer neighbor-route
fair-queue
no cdp enable
ip route 208.118.23.3 255.255.255.240 172.22.0.30 --**LAN DE RED MASK WAN USER**

- **Configuracion en el router CE del cliente**

ip subnet-zero

interface Ethernet0
ip address 10.1.1.0 17 255.255.255.0 secondary ----------**LAN PARA NAT**-------
ip address 208.118.23.4 255.255.255.240 ----------**LAN PUBLICA CLIENTE**----
ip nat inside

interface Serial0
description "CABINET"
ip address 172.22.0.30 255.255.255.252
ip nat outside
encapsulation ppp
no fair-queue

ip nat inside source list 1 interface Ethernet0 overload ------**NAT**------
ip nat inside source static 10.10.10.99 200.107.158.254
no ip http server
ip classless

ip route 0.0.0.0 0.0.0.0 172.22.0.29 ---**STATIC ROUTING DEFAULT HACIA RED--**

access-list 1 permit 10.10.10.0 0.0.0.255

2.1.2 Servicio Internet para las empresas e instituciones comerciales

Este servicio tiene como proposito principal, al igual que el servicio ofrecido a las Cabinas Publicas, brindar a los clientes la salida a INTERNET, la diferencia Principal se encuentra en que en este servicio, se permite la configuración de Tunneling que permite la creación de VPN`s a traves de las redes de INTERNET , Tambien es posible la creación de Filtros en el CE de Filtros de algunos aplicativos con ACCESS-LIST. Otra ventaja es la de proporcionar enlaces de respaldo de los accesos a un mismo Router PE de la Red del Service Provider Local.

- **Access list**

Son mecanismos Para un manejo selectivo de Trafico en el Router ,mas alla de la reglas establecidas por el Tradicional FORWARDING,basado en el destino. Son Mecanismos que pueden configurarse para Filtrar o Testear paquetes para determinar si son Forwardeados a su destino final o son descartados.
Hay 2 tipos de access list los cuales son:

- Access List Estándar: Verifica las direcciones origen que podria ser ruteado El resultado permite o niega la salida para un protocolo entero.
- Access List Extended:. Verifica tanto las direcciones de origen y destino .Tambien puede verificar para determinados protocolos, los numeros de puertos y otros parámetros , permitiendo al Administrador mas control y flexibilidad.

- **Procesos de un access list**

En la figura 2.2, se muestra un diagrama que define el Proceso de Access List. Cuando se trata de Trafico, las principales acciones son permitir(permit) o denegar (deny) el acceso de paquetes a traves de una Interface.
Acces List especializados pueden alterar campos en estos paquetes, como es la Precedencia IP para marcar paquetes en QoS.
Cuando se usan Distribute List, con paquete de ruteo, los access List controlan que información de ruteo ingresa o sale de un proceso de ruteo (routing).

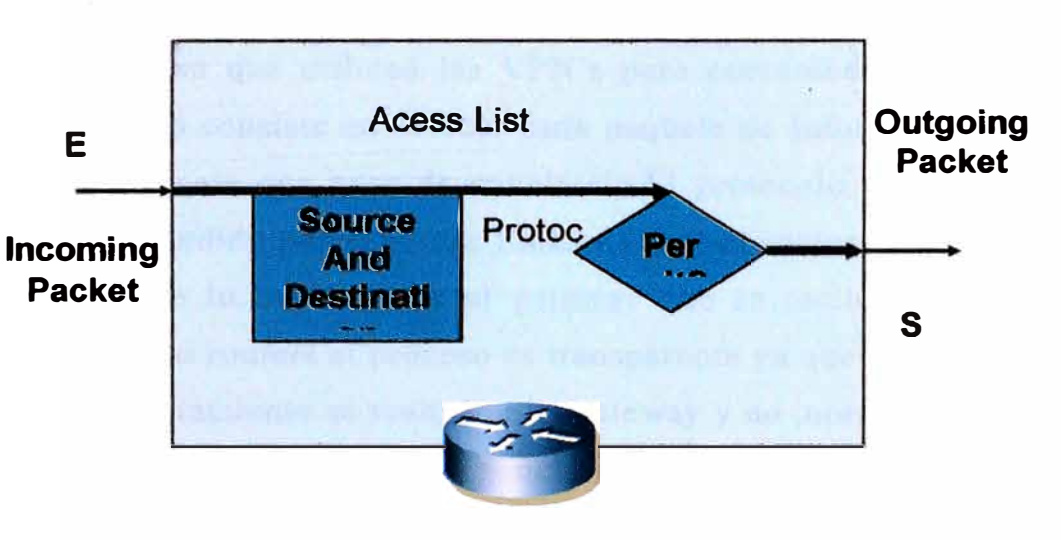

Fig. 2.2 Proceso de access list

- **Implementacion de access list**

Existen 2 pasos importantes en la implementación de un Access List:
-Definir el Access List
-Aplicar el Access List a una Interface o Proceso
Existen varias consideraciones en la configuración de los Acces list:

- ☐ Se puede crear multiples Access List en un router.
- ☐ Se puede aplicar el mismo Access List a multiples interfaces.

- Puede aplicar un Acces list en cada direcciòn por interface.
- El numero de access list indica que protocolo se filtra.
- El orden de las sentencias del Access list controlan la verificación.
- Las sentencias mas restrictivas deben ir primero.
- Hay un "deny any" implicito como ultima sentencia, entonces, debe haber al menos una sentencia "permit".
- Los Access list filtran trafico que circula por el router no se palica a trafico originado en el router.

- **Tunneling**

Es el proceso que utilizan las VPN`s para comunicarse a travès de Internet. Este proceso consiste en colocar cada paquete de Información que se transmite en otro paquete que hace de envoltorio.El protocolo que define el envoltorio solo es entendido por el router Emisor y por el router receptor, es decir por el gateway que lo envia y por el gateway que lo recibe .Para los clientes que utilizan estos routers el proceso es transparente ya que el empaquetamiento y el desampaquetamiento se realiza en el gateway y no ,normalmente en el PC.
En la figura 2.3 , se observa el funcionamiento del proceso de Tunneling.

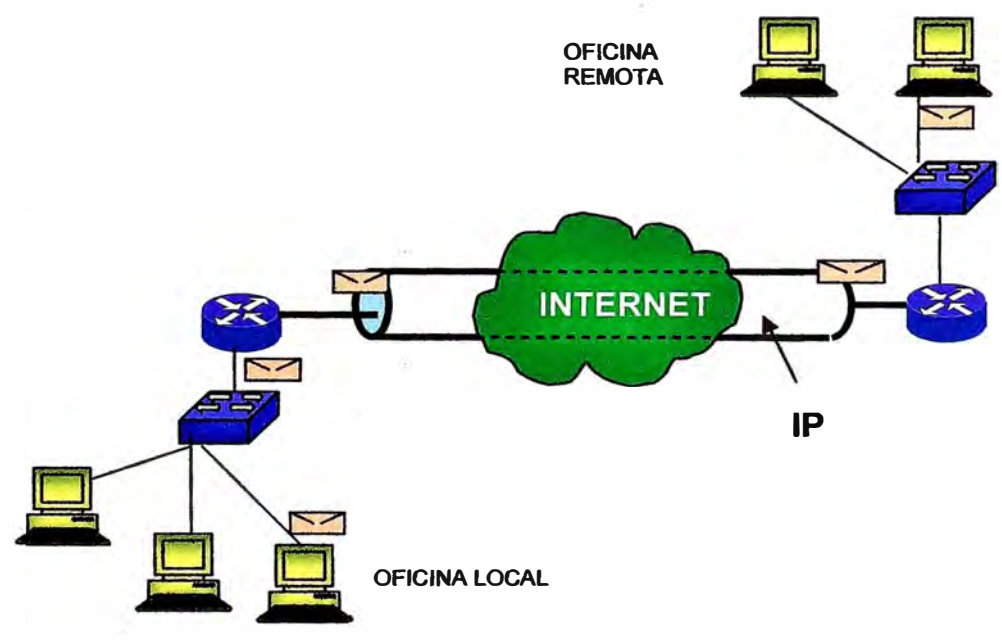

Fig. 2.3 Proceso de Tunneling

El proceso de Tunneling, se basa en tres protocolos:
-El protocolo del carrier: Es el protocolo usado por la red que esta transportando la información.

-El protocolo del encapsulamiento (empaquetamiento):Es el protocolo que aplica al envoltorio del paquete enviado, y segùn el tipo serà mas o menos seguro, pudiendo ser GRE, IPSec, L2F, PPTP, L2TP, siendo el IPSec el màs seguro .
-El protocolo pasajero: Es el protocolo del paquete de información que se envia dentro del envoltorio, es decir, el paquete original de información. Estos protocolos "pasajeros" son IPX, NetBeui e IP.El Acceso fisico, utiliza como medio de transporte a las plataformas o redes TDM, Transmisiones, satelite, lo cuales posibilitan conectar el Router del Cliente a la red IP MPLS.

2.2 Servicio IP-VPN

Es un servicio de Comunicación de datos mediante datagramas IP con calidad de servicio (QoS) y que permite la Interconexión de todos contra todos de un grupo cerrado de usuarios en el modo de INTRANET, se garantiza un servicio de Conectividad privada.

2.2.1.- Calidad de servicio

La calidad de servicio IP se inicia desde el domicilio del cliente, donde se encuentra instalado una PC o estacion IP, el LAN switch y el router. En el servicio VPN soportado por una plataforma IP/MPLS, se garantiza la calidad de servicio IP a lo largo de toda la red.
El router EDC, debe garantizar la calidad de servicio entre la LAN y al puerta de acceso en la red.
Las funciones Básicas de la calidad de servicio son:

- Clasificacion de Tràfico
- Marking Precedente
- Queuieng y Scheduling
- Drop Priority en caso de congestion

2.2.2 Modelos de calidad de servicio

En el servicio IPVPN, el modelo de calidad de servicio de la red es el Diffserv. Donde los Nodos de la red proveen calidad basados en el IP ToS de los paquetes de datos del cliente. En el Modelo Diffserv, la Red clasifica los flujos en base al campo DSCP del paquetes IP(ToS) y específicamente a los bits IP Precedence, entrante en la red bajo la sgte. clasificaciòn:

TABLA Nº 2.1 Calidad de servicio

Calidad	IP Precedence
Oro	2
Plata	1
Bronce	0

La Tabla Nº 2.1 se utiliza para configurar la calidad de servicio en una Plataforma IPVPN-MPLS

Se ha utilizado la sgts Tabla Estandar (Tabla Nº 2.2) , bajo recomendación RFC IP 2547, para definir la calidad de servicio IPVPN.

TABLA Nº 2.2 Tabla Estandar de calidad de servicio

Nombre	IP Precedence
Routine	0
Priority	1
Inmediate	2
Flash	3
Flash-override	4
Critical	5
Internet	6
Network	7

Para el servicio VPN , se establece clases de servicio de acuerdo a las necesidades de cada Proveedor de Servicios.

En esta Tabla los paquetes IP con Precedence 6 o 7 son reservados para control de red. No se usan en el CE.

En el modelo Diffeserv, las funciones de Clasificación, Queueing y Drop Priority las hace el router EDC.

Este mecanismo permite que el uso del enlace a la red se adecue a la calidad IPN y permite que el uso del enlace a la red se adecue a la calidad IP y permite que la red establezca los mecanismos de contrato de cliente basado en el ToS para las calidades Oro, Plata y Bronce

El router PE aprenderá los prefijos desde el Router CE , atraves de una configuracion Estatica ,una configuración BGP o una configuración por RIP intercambiando rutas con el CE. Despues de aprender los Prefijos, el PE los convierte dentro de un prefijo VPN-IPv4 por combinación de estos con un RD de 8 bytes. El prefijo generado es un miembro del VPN-IPv4 address family. Esto sirve unicamente para identificar la direccion del cliente.

El RD usado para generar el prefijo VPN-IPv4 es asociado con el VRF configurado en el router PE.

El protocolo BGP propaga la información referida a los prefijos VPN-IPv4 entre los routers PE. De esta forma se asegura que las rutas para un determinado VPN son aprendido por otros miembros que pertenecena esa VPN, posibilitando a los miembros de la VPN a comunicarse unos con otros.

CAPITULO III
PROVISION INTERNACIONAL DE SERVICIOS DE DATOS OFRECIDOS EN REDES IP - MPLS

Los Servicios Internacionales de Datos, que se ofrecen actualmente a los clientes son básicamente: X25 , Clear Channel(Canales dedicados de datos), Frame Relay . ATM, Internet, VPN. Los servicios que están soportados por una Plataforma MPLS son: Los acceso a INTERNET y el VPN INTERNACIONAL.

3.1 Descripción de la provisión de los servicios internet

Servicio de conexión a INTERNET a traves de una Plataforma IP-MPLS, presenta los sgts escenario de conexiòn:

3.1.1 Agregación de trafico IP

- ☐ Clientes con conexión directa, con acceso a internet
- ☐ Clientes con conexión directa, con acceso a internet, con respaldo
- ☐ Clientes con conexión directa, con dos o màs proveedores de internet sin respaldo
- ☐ Clientes con conexión directa, con dos o màs proveedores de internet con respaldo

a. Clientes con conexión directa con acceso internet

En este escenario se considera la conexión directa a nodos de Borde (RI) , de los routers de los clientes y para el servicio de concentración de sus respectivos usuarios, para este escenario se plantea un esquema de enrutamiento estático.para la configuración de los equipos terminales.

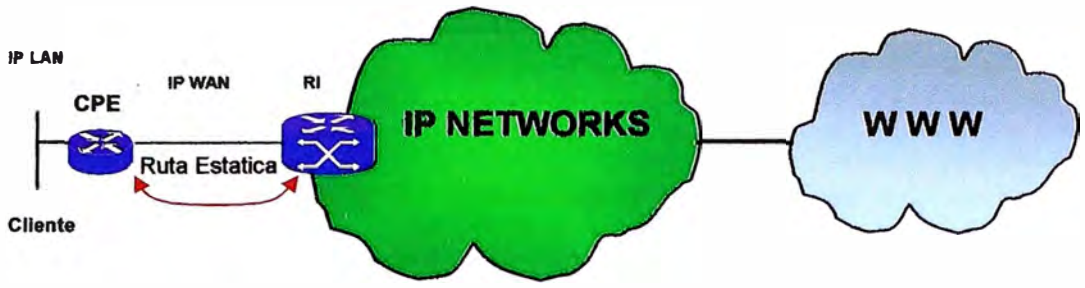

Fig. 3.1 Conexión directa a Internet

En este escenario se dispondra de una Base de Datos de direcciones IP Privadas denominado IP WAN asi como tambien se dispondra de un rango con Pooles de direcciones Pùblicas denominadas IP LAN.

La Tabla 3.1 muestra un ejemplo de direcciones IP privadas , las mismas que serviran para la asignación de direcciones IPWAN , realacionandolos con la identificación del circuito digital (C) y Nombre del Router de Red donde pertenece dicho Pool.

TABLA Nº 3.1 Direcciones IP WAN Privadas

	WAN-WAS	CD	PE	WAN-SIS	CD	PE
1	172.22.0.2	Prueba	WASRI1	172.22.16.2	Prueba	SISRI2
2	172.22.0.6	28419	WASRI1	172.22.16.6	38789	SISRI2
3	172.22.0.10	27483	WASRI1	172.22.16.10	36208	SISRI2
4	172.22.0.14	38002	WASRI1	172.22.16.14	27278	SISRI2
5	172.22.0.18	27345	WASRI1	172.22.16.18	35105	SISRI2
6	172.22.0.22	27514	WASRI1	172.22.16.22	44458	SISRI2
7	172.22.0.26	27480	WASRI1	172.22.16.26	39173	SISRI2
8	172.22.0.30	37827	WASRI1	172.22.16.30	40046	SISRI2
9	172.22.0.34	27573	WASRI1	172.22.16.34	90000	SISRI2

Posteriormente, se asignarà la direccion IPLAN, la misma que se eligirà de la Tabla N° 3.2 de asignación IPLAN:

TABLA N° 3.2 Direcciones IP LAN Publicas

	LAN-WAS	MASCARA	CD	RAZON SOCIAL	CAR	SERVICIO
1	200.60.127.1	/240	10041	DETRIX	64	PLATA
2	200.60.127.17	/240	28419	COSMOS CALLAO	64	PLATA
3	200.60.127.33	/240	27483	NISSAN MOTORS	128	ORO
4	200.60.127.49	/240	38002	BAYER	256	ORO
5	200.60.127.65	/240	27345	COSMOS S.A	64	ORO
6	200.60.127.81	/240	27514	BANCO ITALIANO	512	PLATA
7	200.60.127.97	/240	27480	DISTRIB. INCA	64	ORO
8	200.60.127.113	/240	37827	TEXAS COMPANY	64	PLATA
9	200.60.127.129	/240	27573	LOS ANDES S.I.L	128	ORO

Con estos datos, se abre una sesion TELNET con el router de borde donde se configurara De acuerdo a la Plantilla aprobada para este servicio.

- **Plantilla en el pe para el servicio de conexión directa a internet**

```
WASRI1#sh run int s5/0/0/2:3
Building configuration...

Current configuration : 378 bytes
!
interface Serial5/0/0/2:3
 description INTERNET|INFO|CD=38002|0|BAYER|128|0,128,0,0|Elmer Fauccet
 ip address 172.22.0.13 255.255.255.252
 ip verify unicast reverse-path
```

```
 no ip redirects
 no ip proxy-arp
 encapsulation ppp
 ip route-cache policy
 ip route-cache flow
 ip policy route-map INFORO
 load-interval 30
 no peer neighbor-route
 fair-queue
 no cdp enable
end

WASRI1#
```

- **Plantilla en el ce para el servicio de conexión directa a internet**

```
BAYER#sh conf
Using 1599 out of 29688 bytes

version 12.3
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
!
hostname BAYER  PERU

boot-start-marker
boot-end-marker

logging buffered 16000 debugging
enable password 7 06252B751818514E
```

```
!
no aaa new-model
ip subnet-zero
!
!
no ip domain lookup
!
!
ip cef
!
!
!
!
interface FastEthernet0
 ip address 200.60.127.49 255.255.255.240
 no ip redirects
 no ip proxy-arp
 speed auto
 no keepalive
!
interface Serial0
 ip address 172.22.0.14 255.255.255.252
 no ip redirects
 no ip proxy-arp
 encapsulation ppp
 no fair-queue
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.22.0.13
no ip http server
!
!
```

```
snmp-server community pubBAYER RO
snmp-server community privBAYER RW
snmp-server trap-source FastEthernet0
snmp-server enable traps tty
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps syslog
snmp-server host 200.48.10.11 pubBAYER

control-plane

banner motd ^CCC
##########################################################################

            ENLACE INTERNET 128 K
      BAYER - OFICINA PRINCIPAL
            CD 38002  - CALLAO

##########################################################################
^C
!
line con 0
 stopbits 1
line aux 0
line vty 0 4
 password 7 1311121E0E0A0B24222729
 login
!
```

!

end

BAYER_PERU#

3.1.2 Clientes VPN con modulos de seguridad

En este escenario se considera el funcionamiento de un acceso hacia INTERNET desde una VPN , dentro del cual no se publica hacia Internet ningún tipo de servidor, pero cuenta con una red LAN con estaciones que bajan tràfico desde Internet.

El acceso a este servicio se realiza a traves de la red IPMPLS, dàndole la posibilidad de salida a Internet a las VPN de los clientes, con el componente adicional de seguridad perimetrica ,tal como se muestra en la Fig. 3.2.

El acceso a la plataforma de seguridad de la red que proporciona el acceso seguro a Internet se realiza utilizando la red IP/MPLS , conectando una VLAN del segmento interno de una plataforma de Firewall como un punto de la VPN del cliente.

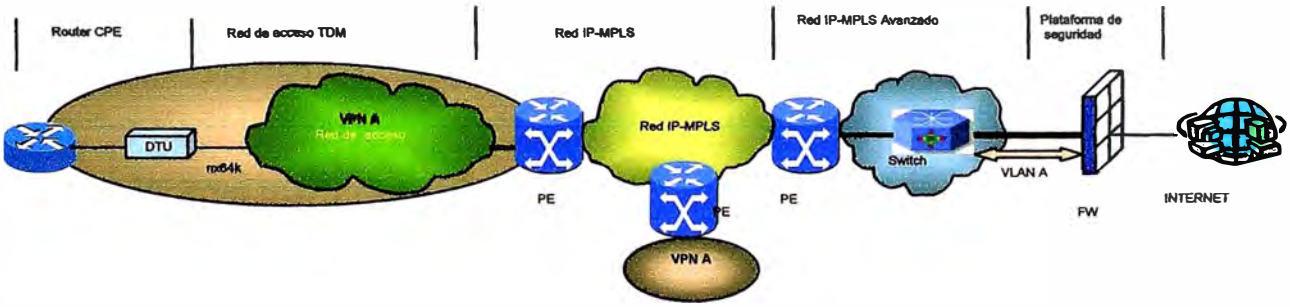

Fig. 3.2 VPN con salida a Internet con Modulo de seguridad

La Provisión de la salida a Internet para los circuitos VPN , se realiza desde el acceso físico, realizándose la conexión del equipo del cliente (CE) hacia el nodo PE mas cercano.

La red IP-MPLS se convierte en la red de acceso y transporte hasta el nodo donde se centraliza el componente de seguridad perimétrica (Firewalls).

Los Switch`s componentes de la Red IP-MPLS avanzado, permiten la conexión desde los nodos PE`s hacia la Plataforma de seguridad perimétrica (Firewall). Cada VLAN es asociado a un Firewall Virtual diferente en la Plataforma de seguridad Perimétrica, de este

modo se garantiza que los traficos de las VPN`s sean aislados unos de otros La Plataforma de seguridad Perimetrica esta referida a un sistema de Firewalls .Su funcionabilidad principal es la de proporcionar un Firewall Virtual a cada Cliente.
El sistema de Firewalls, específicamente el Firewall que se encuentra activo se convierte en el default Gateway de la VPN, con la finalidad de proporcionar el acceso a Internet

3.2 Provision de circuitos VPN remotos con las redes VPN locales

Se define como un servicio de constitución e interconexión de Redes Privadas Virtuales sobre Redes IP.
La VPN opera en capa 3, este servicio permitirà la conexión de las oficinas de Empresas Internacionales operando en diversos paises. Este servicio permitirà la disminuciòn de los costes de las comunicaciones VPN evitando contratar lineas punto a punto o circuitos virtuales Frame Relay.
Los estàndares en los que se apoya el servicio son:

- RFC 2547 bis. Define los mecanismos para proporcionar el servicio VPN MPLS.
- RFC 1771 Border Gateway Protocol(BGP4)
- RFC 1997. BGP Communities Attribute
- RFC 2283 Multiprotocol Extensions for BGP4
- RFC 2796 BGP route Reflection.
- RFC 2842 Capabilities Advertisement with BGP4
- RFC 3031 Multiprotocol Label Switching Architecture
- RFC 3032 PLS Label Stack Enconding
- RFC 3035 PLS using Label Distribution Protocol(LDP) and ATM VC Switching
- RFC 3036 LDP Specification

El funcionamiento del Servicio Internacional, esta soportado en una Plataforma MPLS, a Nivel de Nodos y los equipamientos en cada uno de los Países que componen esta Red.
En la figura 3.3 , se muestra un esquema con el Modelo de Arquitectura que se repetirá en cada unos de los países involucrados.

P, PE :Nodos de Red IPMPLS

P:Provider Core LSR(Label Switch Router
PE:Provider Edge LSR
C:Customer Edge

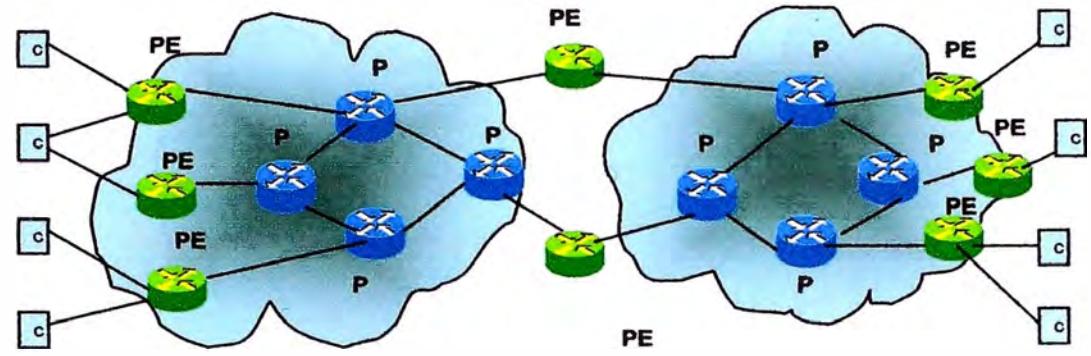

Fig. 3.3 Equipos componentes en la Plataforma MPLS Internacional

En este modelo, se identificara a los sgts elementos:

- El Nodo IP denominado PE (Provider Edge), es el que proporciona el acceso al cliente, aquí es donde se configura los perfiles requeridos por los clientes para el funcionamiento del Servicio VPN.

- El Nodo IP denominado P (Provider core LSR) , es el donde se realiza el Switching de los Circuitos Virtuales Layer 2 (Label Switched Paths –LSPs) generados por los PE`s , este es un nodo IP/LSR que conmuta tràfico IP proveniente de otros Nodos PE`s.

- Como elemento instalado en el domicilio del cliente, se encuentra el Router C, conocido por Customer Edge.

El backbone de la Red Internacional esta compuesto por Routers de Tecnología Cisco y Juniper. Estos equipos actuaran como router`s PE y P. Estos Nodos se encuentran Instalados en 2 Zonas Geograficas: Zona America y Zona Europa, tal como se muestra en la Fig 3.4 . El Protocolo de que rige para posibilitar el Intercambio de rutas que permitirà el

encaminamiento del Trafico Internacional es BGP. Existen Routers, en las 2 Zonas, que cumplen lan funciòn de Reflectores de Rutas lo que permitirà el intercambio de rutas enter Europa y America

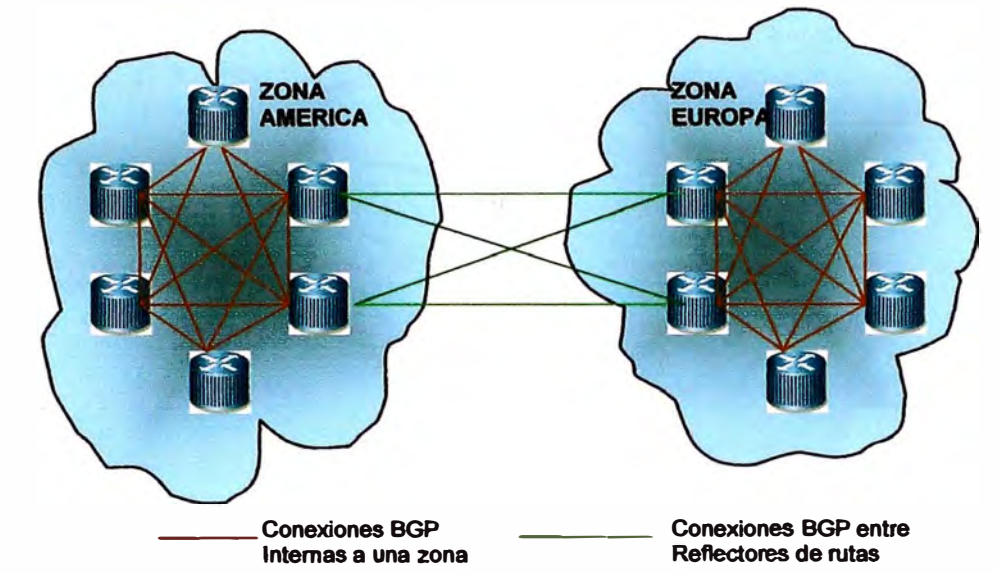

Fig. 3.4 arquitectura del servicio VPN MPLS Internacional

Donde básicamente se observa a los routers de acceso a la Red IP-MPLS y los equipos de Cliente EDC.

Los Routers de acceso a la Red IP-MPLS son de Tecnología Cisco u otro homologados para con los requisitos tecnicos exigidos.

La salida a Internet de los usuarios de una VPN se realizarà a traves de una de las sedes de la VPN que disponga de su propia salida a Internet, tal como se muestra en la Fig 3.5.

Los EDC enviaràn mediante protocolo de routing a los routers que actùan como PE`s la información de los rangos de direcciones de la VPN incluidos dentro de su sede .En el caso en que la sede sea el de la salida a INTERNET, tambien enviarà la ruta por defecto, a fin de que el resto de las sedes de la VPN sepan en que punto existe una salida a INTERNET. Esta información serà redistribuida en BGP-4 por el PE , para ser enviada a los demàs PE`s de la Red IP-MPLS.

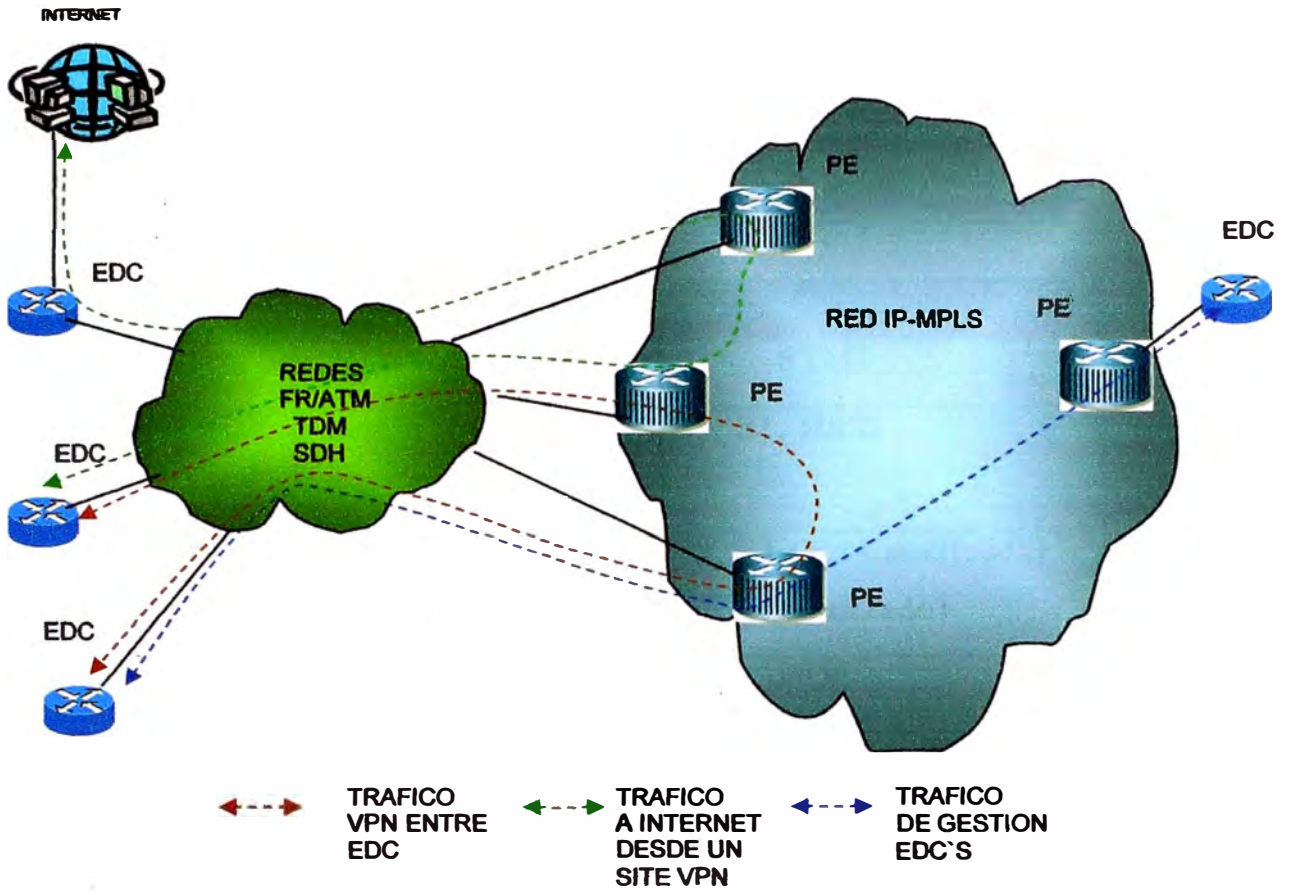

Fig. 3.5 Salida a Internet desde una VPN

Los Routers de acceso al servicio VPN MPLS INTERNACIONAL son aquellos a los que se conectan los equipos de cliente, y cuya función en la red MPLS es la de PE`s.

La versión de Software de los equipos Cisco es la que se muestra en la Tabla Nº 3.3

TABLA Nº 3.3 Software de los Routers

Router	Versión de SW
Cisco	12.0(25)SI o superior

Los routers soportan las sgts Interfaces mostradas en la Tabla N° 3.4

TABLA N° 3.4 Interfaces de acceso

	Tipo de acceso	Ancho de Banda
EDC's	ATM	STM1
	Frame-Relay	E3, E1, HSSI
	PPP	E3, E1 (No Canalizada) y E1(Canalizado)
	Ethernet	10M-100M
Red	POS	STM16,STM4, STM1

Los Equipos de Cisco que se utilizaràn como PE`s seràn los routers de la familia 7500 y se dispone de tres modelos de router: El 7005, el 7007 y el 7513.Cada uno de estos equipos dispone de ranuras para instalar tarjetas interfaces de red. El Cisco7513, que se muestra en la figura 3.6, dispone de dos ranuras para las tarjetas Router Switch Processor (RSP) y once ranuras para interface de red. Cada uno de estos equipos dispone de un Bus de alta velocidad (Cisco Extended Bus o CyBus) , que interconecta las mencionadas tarjetas.Estos equipos permiten el procesamiento distribuido: La RSP se encarga de Labores de mantenimiento de las tablas de rutas , y los protocolos de encaminamiento, mientras que las tarjetas de interface de red se encargan de la conmutación de los paquetes de trafico.

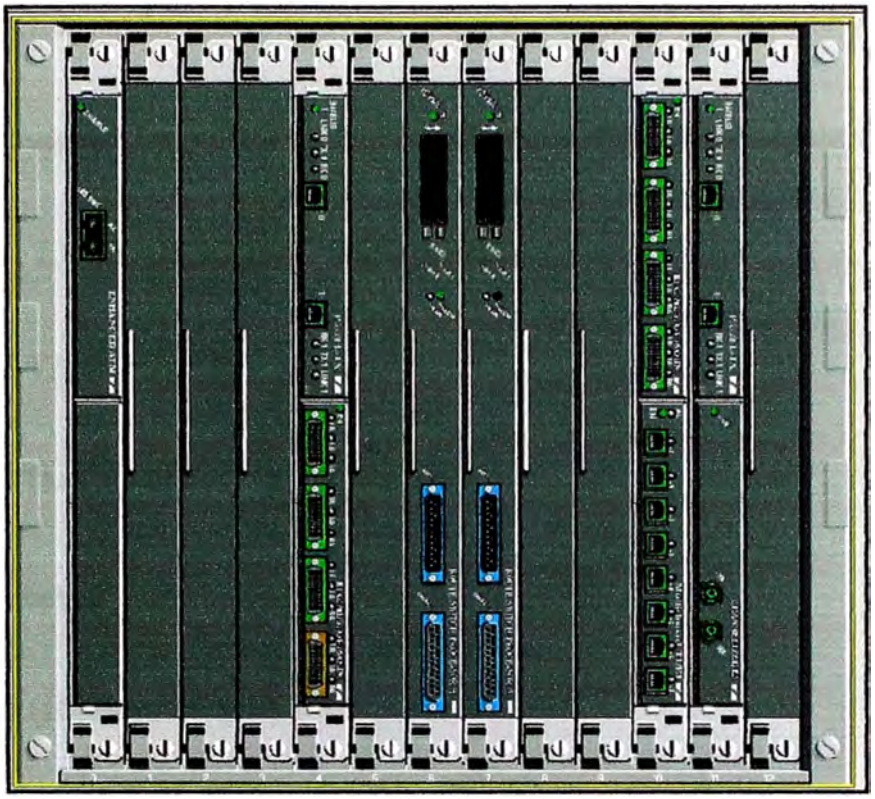

Fig. 3.6 Router cisco 7513

Existen tres tipos de tarjetas RSP, cuyas características se muestran en la TABLA Nº 3.5

TABLA 3.5 Tarjetas RSP

Procesador	Memoria DRAM	Memoria flash SIMM	Memoria Flash PCMCIA	Memoria NVRAM
RSP 2	32 a 128 MB	8 MB	16 o 20 MB	128 KB
RSP 4+	64 a 256 MB	8 MB	16 o 20 MB	128 KB
RSP 8	64 A 256 MB	16 MB	20 O 40 MB	2 MB

La IOS del router reside en la memoria Flash, bien en la SIMM de la RSP bien en la PCMCIA.

Las Interfaces de red soportadas por los routers de la familia 7500 son las siguientes

- ATM(T1, E1, T3, E3, OC3/STM1, OC12/STM4)
- Multichannel T3, E3, T1 y E1
- DPT OC12/STM4
- Gigabit Ethernet
- Fast Ethernet (100BaseT y MII)
- Ethernet(10BaseT, AUI y 10BaseFL)
- Token ring
- FDDI
- HSSI
- ISDN PRI
- Serial (T3, E3, T1 y E1)

Estas interfaces de red van montadas sobre tarjetas VIP(versátil Interface processor) en forma de Port Adapters que se insertan en dichas tarjetas. Cada tarjeta puede soportar hasta 2 Port Adapters, dependiendo de la configuración y tipo de tarjeta VIP.

Los modelos de tarjeta VIP que permiten procesamiento distribuido, son mostrados en la tabla Nº 3.6.

TABLA N° 3.6 Tarjetas VIP

Tarjeta	Memoria RAM
VIP2-40	32 MB DRAM y 2MB SRAM
VIP2-50	32 a 128 MB DRAM y 4 a 8 MB SRAM
VIP4-50	64 a 256 MB SDRAM
VIP4-80	64 a 256 MB SDRAM

Los ports adapters que se instalan sobre las VIP dependen del tipo de conexión del EDC a la red.

3.2.1 Plantilla de configuracion VPN local en los routers PE

Para proceder a brindar el Servicio VPN Internacional es necesario provisionar los circuitos VPN local, para lo cual una vez configurado los parámetros en los Routers de red, como son la asignación de la vrf (vpn routing forwarding) de cada cliente asi como los parámetros de ruteo RIP o BGP , se procederà a utilizar las direcciones IP privadas asignadas a cada cliente, tal como se muestra en la Tabla N° 3.7. Se asignara un nombre a la vrf creada a cada cliente, asignandose un pool de direcciones IP con mascara: 255.255.255.252, si se requiere contar con mas direcciones IP WAN, entonces se asignara los pooles adicionales a un mismo circuito.

TABLA Nº 3.7 Direcciones IP Wan para Circuitos VPNs.

CLIENTE	CD	IP PRIVADA							NODO	IP PRIVADA							NODO
FENIX	46780	10	.	128		222		162	WASPE1	10	.	129	.	222		162	WASPE2
FENIX		10	.	128		222		166	WASPE1	10	.	129	.	222		166	WASPE2
FENIX		10	.	128		222		170	WASPE1	10	.	129	.	222		170	WASPE2
FENIX		10	.	128		222		174	WASPE1	10	.	129	.	222		174	WASPE2
FENIX		10	.	128		222		178	WASPE1	10	.	129	.	222		178	WASPE2
FENIX		10	.	128		222		182	WASPE1	10	.	129	.	222		182	WASPE2
FENIX		10	.	128		222		186	WASPE1	10	.	129	.	222		186	WASPE2
FENIX		10	.	128		222		190	WASPE1	10	.	129	.	222		190	WASPE2
MOTTA	46881	10	.	128		222		194	WASPE1	10	.	129	.	222		194	WASPE2
MOTTA		10	.	128		222		198	WASPE1	10	.	129	.	222		198	WASPE2
MOTTA		10	.	128		222		202	WASPE1	10	.	129	.	222		202	WASPE2
MOTTA		10	.	128		222		206	WASPE1	10	.	129	.	222		206	WASPE2
MOTTA		10	.	128		222		210	WASPE1	10	.	129	.	222		210	WASPE2
MOTTA		10	.	128		222		214	WASPE1	10	.	129	.	222		214	WASPE2
MOTTA		10	.	128		222		218	WASPE1	10	.	129	.	222		218	WASPE2
MOTTA		10	.	128		222		222	WASPE1	10	.	129	.	222		222	WASPE2
UNION	45332	10	.	128		222		226	WASPE1	10	.	129	.	222		226	WASPE2
UNION		10	.	128		222		230	WASPE1	10	.	129	.	222		230	WASPE2
UNION		10	.	128		222		234	WASPE1	10	.	129	.	222		234	WASPE2
UNION		10	.	128		222		238	WASPE1	10	.	129	.	222		238	WASPE2
UNION		10	.	128		222		242	WASPE1	10	.	129	.	222		242	WASPE2
UNION		10	.	128		222		246	WASPE1	10	.	129	.	222		246	WASPE2
UNION		10	.	128		222		250	WASPE1	10	.	129	.	222		250	WASPE2
UNION		10	.	128		222		254	WASPE1	10	.	129	.	222		254	WASPE2

CAPITULO IV
INTERCONEXION ENTRE REDES IP-MPLS

4.1. El protocolo BGP (Border Gateway Protocol)

Este Protocolo es utilizado para el intercambio entre sistemas autonomos. Un sistema autonomo AS es un grupo de redes bajo una administración comùn y comparte una misma estrategia comùn de ruteo.

Un sistema autonomo (AS) es identificado por un numero de 16 bits, y es seleccionado del rango de 1 a 65535. Los numeros AS pùblicos son asignados por los mismos organismos que asignan direcciones IP :ARIN, RIPÊ NCC, APNIC. Para los Clientes que requieren AS Para correr BGP en sus redes privadas, se ha reservado el rango: 64512-65535.

En la Fig. 4.1 se muestra el Interdomain routing, que es el ruteo entre Sistema Autonomo, esta basado en una serie de politicas

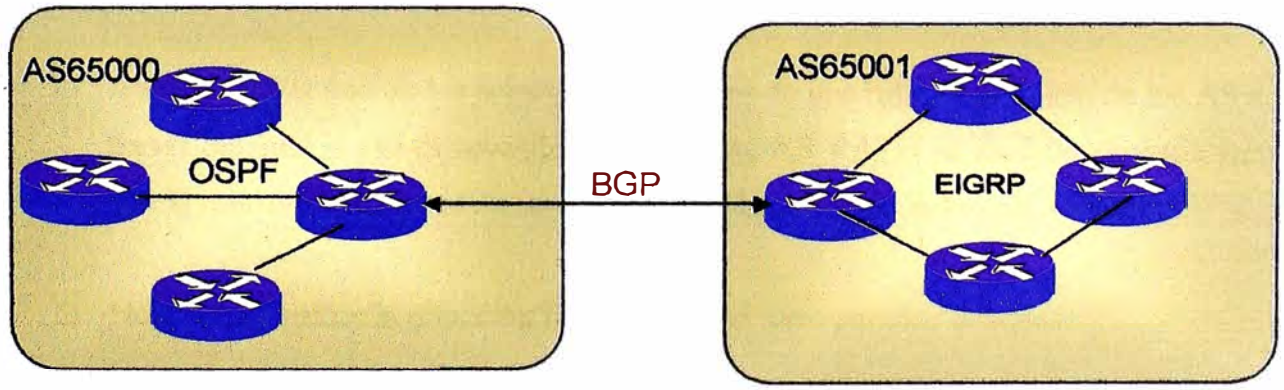

Fig. 4.1 Ruteo entre Sistemas Autonomos

El protocolo BGP , es un medio para pasar información entre As`s .tiene todas las funciones que soportaran las politicas de diversos Interdomain routing, contrariamente a los protocolos de ruteo interno que solo se preocupan de encontrar la ruta mas optima entre dos puntos sin considerar politicas de ruteo alguno. Cuando un router recive una actualizaciòn BGP, este analizarà los atributos atachados y los comparara con los atributos atachados a los mismos Subnet IP cuando los recivio de diferentes fuentes. El router entonces hace una decisión sobre cual fuente indica la mejor ruta a un determinado IP subnet.La mejor ruta es propagada, acompañado con su atributos principales, a otro BGP neighbors.
Estas funciones denominados Atributos BGP , y pueden ser categorizados en :

4.1.1 Atributos well-known mandatorios

Estos atributos siempre deben estar presentes en todos los mensajes de actualizaciòn (Update). Todos estos atributos son propagados a otros neighbors.

Entre los principales atributos Well-known Mandatarios que deben estar presentes son:

- ORIGEN, Especifica el origen de una ruta BGP, este atributo es colocado cuando la ruta es injectado dentro del BGP. Si la información acerca deun Subnet IP es inyectado usando el comando **network o** via agregación (sumarizaciòn de ruta con BGP), el atributo origen es configurado a unknown o incompleto.

- AS_PATH, Es uno de los principales atributos de una ruta, es una lista de los AS a traves del cual la red es accesible. El atributo AS PATH es modificado cada vez que la información acerca de un particular Subset IP pasa sobre un AS border.

- Next_Hop, Indica la direcciòn IP del proximo salto para los destinos.

neighbor 200.48.175.130 next-hop-self

4.1.2 Los atributos well-known discretionary

Estos atributos son opcionales, estos podrían estar presentes en los mensajes de actualización (update messages).

- Local Preferente, es usado en el proceso de selección de rutas. Una ruta con una alto valor de Local Preferente es preferido sobre una ruta con un valor bajo.

- El Atomic Aggrégate es atachado a una ruta que es creado como el resultado de la sumarizaciòn de rutas (Llamado Agregación en BGP).informa al neighbor AS que el router originador esta agregando rutas.

- Maximum-prefix , limita el anuncio del numero maximo de prefijos o redes desde el neighbor.

  neighbor 172.20.0.225 maximum-prefix 100

- Send-Community, El atributo Communities es una forma de agrupar destinos dentro de comunidades y aplicar decisiones de ruteo. Específicamente el comando Send-Community, Establece que los atributos de las Comunidades es transmitido al neighbor en la direccion IP que se acompaña en este atributo:

  neighbor 200.48.175.130 send-community

- Update-Source, Permite que las sesiones BGP internas usen una Interface Operacional para conexiones TCP.

  neighbor 172.20.0.225 update-source POS4/0.101

- advertisement-interval, Establece el minimo intervalo (en segundos) entre los envios de las actualizaciones de ruteo.

  neighbor 172.20.32.5 advertisement-interval 10

- soft-reconfiguration inbound, Este es una de las formas para realizar un Reset de las conexiones BGP de un determinado peer, iniciando el almacenamiento de las tablas de actualizacion del inbound routing desde el neighbor especificado o un grupo de peer´s. Desde ese punto direccionará una copia de la tabla BGP routing para el neighbor especificado o grupo de Peer´s que son mantenido en este router.

```
router bgp 100
 neighbor 131.108.1.1 remote-as 200
 neighbor 131.108.1.1 soft-reconfiguration inbound

router bgp 6147
 no synchronization
 bgp router-id 200.48.175.138
 bgp log-neighbor-changes
neighbor 172.22.120.22 remote-as 65002
 neighbor 172.22.120.22 description --- ULIMA CD=36996 AS=65002 --
 neighbor 172.22.120.22 next-hop-self
 neighbor 172.22.120.22 send-community
 neighbor 172.22.120.22 default-originate
 neighbor 172.22.120.22 soft-reconfiguration inbound
 neighbor 172.22.120.22 distribute-list ONLYDEFAULT out
 neighbor 172.22.120.22 route-map from _ULIMA in
 neighbor 172.22.120.26 remote-as 65002
 neighbor 172.22.120.26 description --- ULIMA CD=38608 AS=65002 --
 neighbor 172.22.120.26 next-hop-self
 neighbor 172.22.120.26 send-community
 neighbor 172.22.120.26 default-originate
 neighbor 172.22.120.26 soft-reconfiguration inbound
 neighbor 172.22.120.26 distribute-list ONLYDEFAULT out
 neighbor 172.22.120.26 route-map from _ULIMA in
```

4.1.3 El establecimiento de la sesion BGP

El Establecimiento de las sesion BGP, pasan por varios estados , entre las cuales figuran las sgts.:

- Estado IDLE, inicialmente toda sesión BGP , se encuentra en este estado

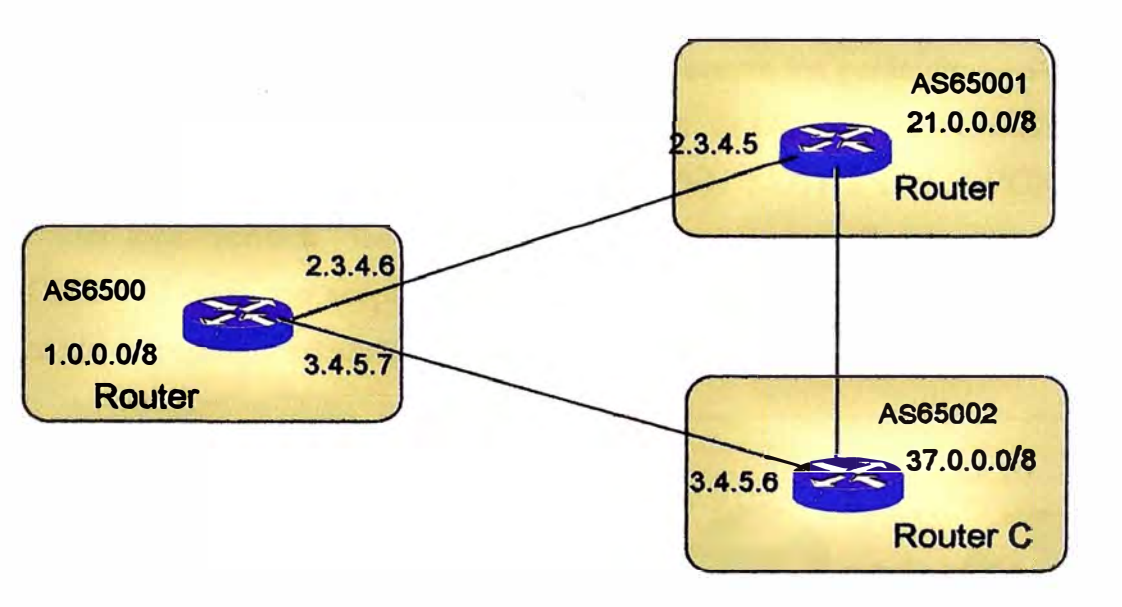

Fig. 4.2 Topologia BGP.

Rtr-A#show ip bgp sum

BGP table version is 1, main routing table version 1

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State
2.3.4.5	4	65001	0	0	0	0	0	never	Idle
3.4.5.6	4	65002	0	0	0	0	0	never	Idle

En este ejemplo podemos observar los listados de cada uno de los Neighbor con los que se conecta el Router A, figurando la direccion IP correspondiente. Tambien se muestra la versión de la sesiòn BGP, el Sistema Autonomo AS remoto, los contadores de intercambio de mensajes, el tiempo desde el ùltimo cambio producido en la sesiòn BGP y el Estado actual.

- Antes que un intento de conexión sea hecho, la sesion BGP tiene que haber cambiado del estado de IDLE al estado ACTIVE, esto sucede cuando la direccion IP de un Router remoto es alcanzable sobre una interface directamente conectado.
- La primera información BGP transmitida es el mensaje BGP open (BGP open message).
- La sesion BGP cambia desde el estado ACTIVE al estado OPEN SENT mientras espera
- La respuesta del otro router. Si el router peer acepta los parámetros en el mensaje de OPEN, este responde con su propio mensaje de OPEN. Cuando el Router Local recibe este mensaje cambia de estado de OPEN SENT a OPEN CONFIRM. El router local verifica los parámetros del router peer recibos en su mensaje de OPEN. Si estos son aceptados , se transmite un paquete de Keepalive y de este modo de pasarà al estado Establecido (ESTABLISHED)

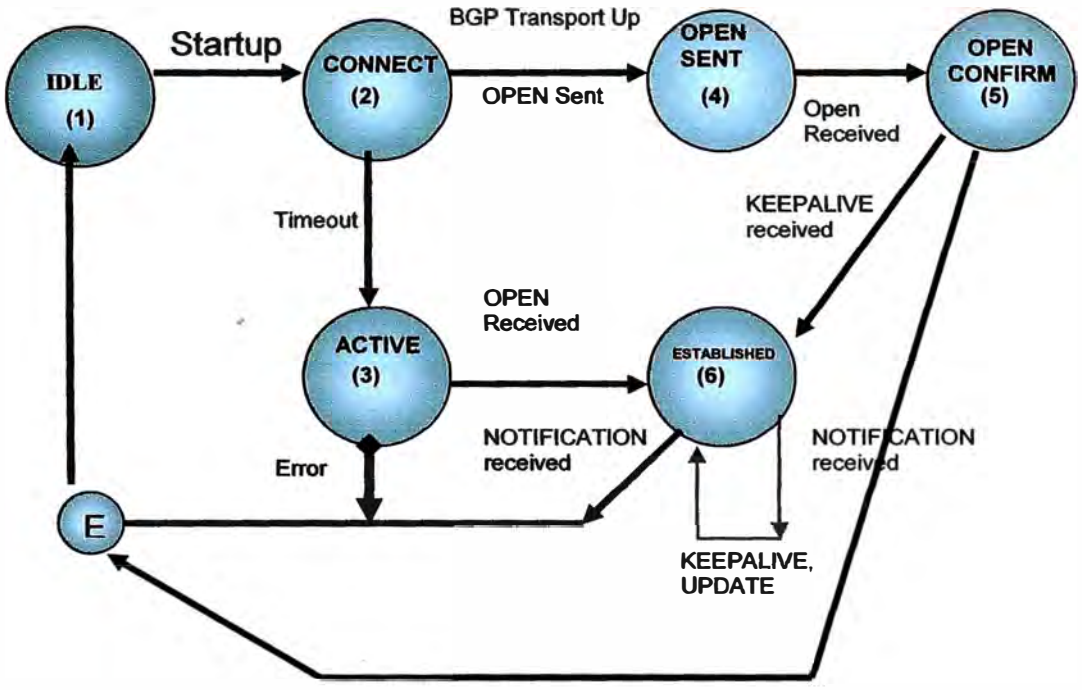

Fig. 4.3 Estados del Establecimiento de la sesiòn BGP.

Los mensajes BGP OPEN contiene los sgts parámetros:

Numero de versión .-El numero de versión mas reciente , a ser utilizado es el BGP versión 4.

- Numero de Sistema Autónomo (AS).-Se refiere al número del sistema autónomo del router local. El router peer verificara esta información. Si este no es el numero AS esperado, entonces la sesiòn BGP se va a Down.

- Hold time.-Es el numero de segundos que puede esperarse entre la recepción de sucesivos mensajes BGP. Si el tiempo es excedido el peer serà considerado caido (DEAD).

- Identificador BGP.-Un número unico que identifica al Router. El Router usarà uno de sus direcciones IP para esto, El Router-ID.
- Parámetros opcionales.-Son valores codificados .Un ejemplo de estos parámetros es la sesiòn autentificada.

-Estado Estable de las sesiones BGP de los Neighbors.-una de las fases de la sesión BGP,es el estado establecido, donde tiene lugar el intercambio de la información.

```
Rtr-A#show ip bgp sum
BGP table version is 10, main routing table version 10
3 network entries (3/6 paths) using 516 bytes of memory
3 BGP path attribute entries using 284 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Neighbor  V  AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcvd
2.3.4.5   4  21  17       22       10      0    0     0:01:47  27
3.4.5.6   4  37  11       17       10      0    0     0:07:07  35
```

Con el comando **show ip bgp summary** se observara que la sesıon se encuentra establecida.

Los contadores indicaran la cantidad de mensajes que se han transmitido y recibido durante la sesiòn. InQ muestra cuantos mensajes han sido recibidos pero aun no han sido procesados.un alto valor de InQ indicarà una falta de recurso de CPU para procesar la entrada. OutQ , muestra cuantos mensajes salientes se encuentran encolados. Un alto valor de OutQ indicarà una falta de ancho de banda para transmitir los mensajes salientes o una sobrecarga del CPU de otro router.

La Columna con la información Tbl/Ver (Table Version) es empleada para indicar los cambios que necesitan ser trasmitidos a los Neighbors. Hay un número de versión para la Tabla del BGP Local. Esto es mostrado en la primera línea el Comando Show. También hay un número de versión mantenido para cada uno de los neighbors. Esto es mostrado en la línea de información de los neighbors.

En la Columna UP/DOWN, se indica el tiempo transcurrido desde el último estado de la Sesión BGP.

En la Columna State/ PfxRcvd, se muestra la cantidad de prefijo o redes anunciadas desde los neighbors.

4.2. Escenarios presentados en la provision internacional

4.2.1.-Escenario de acceso.

El Servicio VPN MPLS Internacional, se define como un servicio de constitución e interconexión de redes Privadas Virtuales sobre redes IP.

Los circuitos VPN operan en capa 3, se caracterizan por utlizar redes IP pùblicas Este servicio permitirà, mediante la conexión de las oficinas de una empresa con presencia internacional a la mencionada red, la comunicación entre sus diferentes delegaciones .iDe este modo las corporaciones se ahorran los costes de contratar lineas punto a punto y/o de establecer circuitos frame relay entre sus oficinas.

Hasta la aparición de la Tecnología MPLS y su estandarizaciòn como soporte de servicios de VPN, la forma màs comùn de implementar este tipo de VPNs es medinateel empleo de tùneles, es decir, encapsulando el tràfico IP generado por la oficinas sobre otro paquete IP

que es transportado desde el origen del tùnel hasta el destino siendo encaminado por la Red pùblica IP. Es decir, los paquetes transmitidos incluyen dos cabeceras IP, una es la original generada por los sistemas finales de la corporación, y la otra es la que permite ecaminar los paquetes IP desde el origen del tùnel hasta el punto de salida del tùnel. Con este mecanismo de tùneles conseguimos los dos objetivos bàsicos de las VPNs:

- El tràfico de cada VPN no se mezcla con el resto, es decir, el tràfico perteneciente a una VPN va ùnicamente dirijido a delegaciones que pertenecen a esa VPN.
- El direccionamiento de cada VPN es indiferente respecto a los demàs VPNs. Es decir , cada VPN puede tener su propio esquema de direccionamiento (con direcciones IP privadas), los mismos que pueden solaparse con el direccionamiento de otras VPNs.

El inconveniente de este modelo de implementar VPN mediante tùneles es la escalabilidad, ya que se necesita generalmente un tùnel (configurado estaticamente) entre dos oficinas de la corporación. Para una Empresa proveedora del servicio es complicado configurar ciento de tùneles en sus routers PE(ruteadores de frontera), para brindar el servicio VPNs de los clientes.

Para evitar esta problemàtica el servicio VPN MPLS INTERNACIONAL se basa en MPLS.

MPLS evita la necesidad de utilizar túneles gracias a que los routers del backbone de la red IP-MPLS no necesitan examinar la cabecera IP para tomar la decisión respecto al reenvío del paquete, sino que lo hacen a traves de la etiqueta que lleva incorporado el paquete IP.

Por este motivo, si los routers de frontera de entrada a la red IP , son capaces de colocar las etiquetas a los paquetes de tal modo que el tràfico de cada VPN se encamine ùnicamente a puntos pertenecientes a la misma VPN se habrà conseguido establecer VPNs totalmente transparentes de cara al backbone de la red, que no necesita tener información del direccionamiento de cada VPN , y ademàs evitamos al tener que configurar múltiples túneles estáticos entre las distintas delegaciones de una misma VPN.

El acceso a la Red IP-MPLS, dependerá de los requerimientos del cliente, principalmente en lo referente a los caudales IP contratados por el cliente para soportar el tràfico a trasmitir o enviar desde cada una de sus dependencias.

Como los escenarios de acceso a este servicio se contemplan las modalidades mostradas en la Tabla Nº 4.1

TABLA Nº 4.1 Tipo de Acceso del servicio VPN

Tipo de acceso	Red de acceso
• Acceso FR • Acceso ATM • Acceso PPP • Acceso xADSL	• Acceso a través de un Proveedor de servicios de datos local. • Acceso a la Red MPLS Local

- Accesos a través de una Plataforma de datos Multiservicios local , en donde empleando los accesos soportados en los servicios Frame Relay y ATM nacionales se conectaran a los equipos implementados como nodos de Red internacional. El circuito de acceso remoto estarà provisionado por el operador remoto con las caracteristicas tecnicas configuradas por este.
- Acceso a la red MPLS Local, donde existen Redes IP-MPLS , permitiràn una mayor capilaridad del servicio en dicho pais. Este tipo de acceso serìa el mas eficiente cuando nos encontramos con numerosos sites VPNs dentro de un pais ya que permite concentrar el tràfico Internacional de todas las oficinas nacionales, en la proporción que el cliente necesite y por lo tanto economizar el coste al cliente.

Fig. 4.4 Acceso Frame relay /ATM

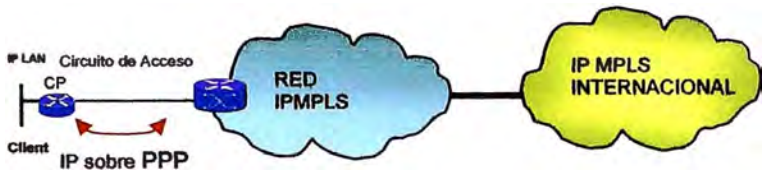

Fig. 4.5 Acceso IP sobre PPP

Fig. 4.6 Acceso ATM

4.2.2.-Escenario de redundancia

Se ofrecerà al cliente la posibilidad de contratar acceso redundantes a la red y/o al servicio que requieren garantizar una alta prestación en sus oficinas criticas, para lo cual se definen los sgts tipo de redundancia mostrados en la Tabla Nº 4.2.

TABLA Nº 4.2 Escenarios de redundancia

Escenarios de redundancia	EDC	Línea	PE	Caudal IP
Basico	1	1	1	1
Doble línea	1	2	1	2
Doble Línea plus	1	2	2	2
Premium	2	2	2	2

El escenario de balanceo de carga se darà sòlo en el caso de redundancia de Doble Lìnea
El caso de Doble Linea Plus se emplea para dar el respaldo en la linea de acceso y prevenciòn sobre fallo en el PE de la Red IP-MPLS.
El servicio Premium, permite al cliente contar con una redundancia completa, en router EDC, linea de acceso y Router PE de la Red IP-MPLS.

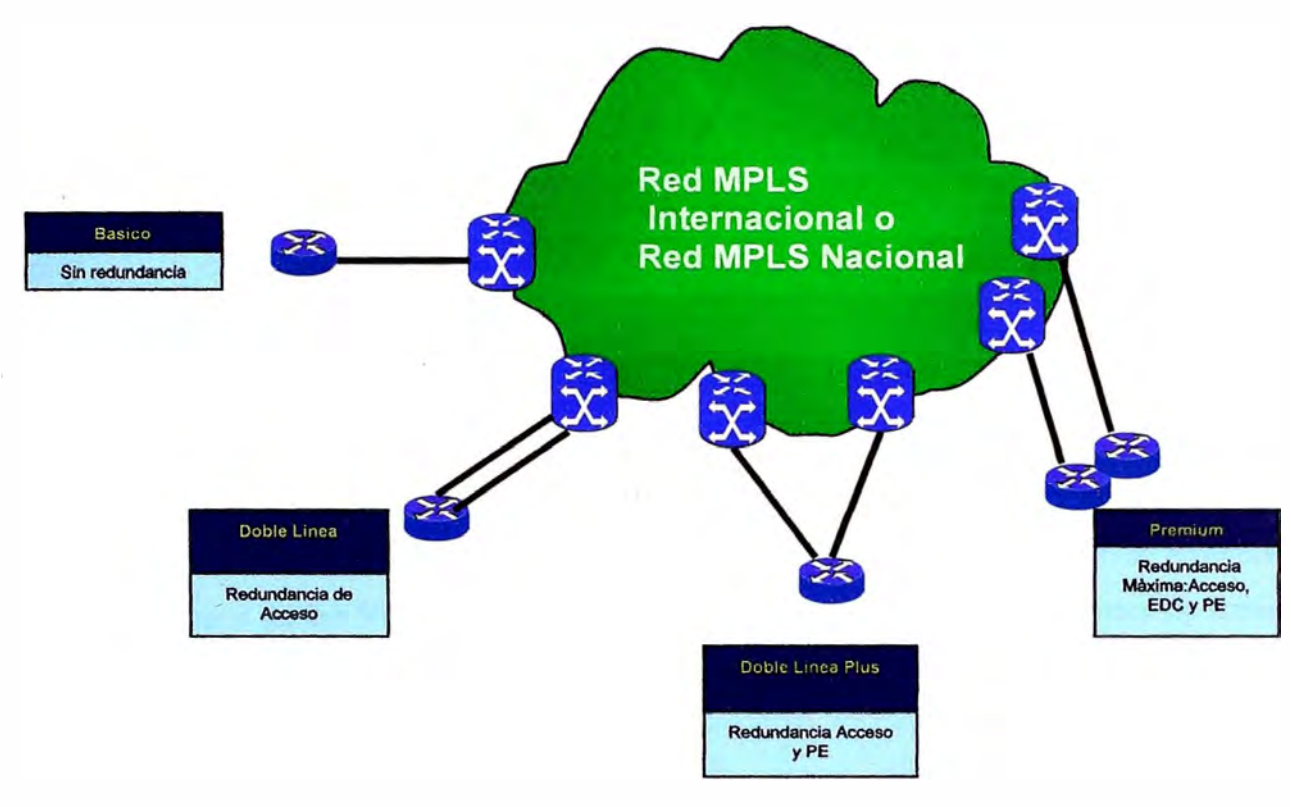

Fig. 4.7 Escenarios de redundancia

4.2.3.-Punto de interconexion entre redes IP-MPLS

En la Provisiòn de los circuitos VPN-MPLS Internacional , es muy importante la configuración del Llamado punto de Interconexión (PoI), que tiene la funciòn de extender la red VPN definida en una red MPLS Local a la Red Internacional MPLS que facilitarà la conexión con otra red MPLS remota en otro pais.
Por lo general se definiràn, al menos, dos PoI entre la red IP/MPLS y la Red IP/MPLS Internacional.

- **Interfaces utilizadas en la interconexion de los PoIs**

La Interfaces que se pueden utilizar, son aquellos en donde se puede configurar subinterfaces, de modo que en cada subinterfaz se defina una VRF. Descartandose el ATM por que introduce el concepto de serializaciòn dependiente de la velocidad del PVC, en vez de la velocidad global de la Interface..
Las Interfaces seleccionadas en los PoIs son:

- **PoS**, con encapsulaciòn frame-relay, para permitir la definición de las interfaces.
- **FastEthernet**, donde se define las vlan, para poder crear los subinterfaces.

- **Protocolo de routing en la interconexion**

El protocolo de routing que se va usar en la interconexión de cada VPN es **eBGP.**
-El nùmero de rutas que se va a admitir, seran limitados a valores definidos de acuerdo a las dimensiones de las VPNs configurados de modo de evitar posibles errores de envios masivos de redes que puedan hacer peligrar la estabilidad de las redes.
Estos valores eran:

- VPNs tamaño medio: 500 rutas (valor por defecto)
- VPNs tamaño grande: 1200 rutas.
- VPNs tamaño extra-grande: 2500 rutas
- VPNs que requieran mas de 2500 rutas seràn considerados como Proyecto especial
- Se empleará el sgt. comando para limitar el numero de rutas:

neighbor **<dir_ip_neighbor>** maximum-prefix **<Maxº Nº redes recibidas>**

neighbor **172.20.0.225** maximum-prefix **500**

-Se deben eliminar del AS-PATH los AS privados

- neighbor **<dir_ip_neighbor>**remove-private-as

-Se debe de anunciar las comunidades (communities)

- neighbor **<dir_ip_neighbor>**send-community both

-Modificaciòn de "timers" de frecuencia de anuncio de las redes a 10 segundos.

- neighbor **<dir_ip_neighbor>**advertisement-interval 10

-Tratamiento de las rutas por defectos y control del enlace principal ò de backup de los PoI.

<u>En el PoI Principal: PoI PPAL</u>

Router bgp <sistema autònomo>

address-family ipv4 vrf vpn_<AS>_<id vpn>
neighbor<dir_ip_ neighbor1> route-map in_default_PoI_ppal in
neighbor<dir_ip_ neighbor1> route-map out_med_ppal out
exit-address-family
exit

<u>En el PoI Backup</u>

Router bgp <sistema autònomo>

address-family ipv4 vrf vpn_<AS>_<id vpn>
neighbor<dir_ip_ neighbor2> route-map in_default_PoI_backup in
neighbor<dir_ip_ neighbor2> route-map out_med_backup out
exit-address-family

```
 exit
 !
route-map in_default_PoI_ppal permit 10
 match ip address ruta_defecto
 match community global_defecto
 set local-preference 200
 set metric 0

 !
 route-map in_default_PoI_ppal permit 30
 set metric 0

 !
 route-map in_default_PoI_backup permit 10
 match ip address ruta_defecto
 match community global_defecto
 set local-preference 200
 set metric 1000

!
 route-map in_default_PoI_backup permit 20
 match ip address ruta_defecto
 set local-preference 50
 set metric 1000

 !
 route-map in_default_PoI_backup permit 30
 set metric 1000

 !
 route-map out_MED_PPAL permit 10
  set metric 0
```

```
!
route-map out_MED_BACKUP permit 10
set metric 1000
```

La configuraciòn de dos PoI's, garantizaran la redundancia de la conectividad entre redes. Por cada VPN, se definirá dos posibilidades de conexión a los PoI`s : uno de ellos será considerado como PoI principal, permaneciendo el otro como backup, tal como se observa en la Fig. 4.8.

El control del PoI principal y backup será realizado mediante el uso del MED.

- Tràfico saliente de la Red IP-MPLS Local: Las redes aprendidas desde la Red IP-MPLS Internacional seràn marcadas con un MED=1000 cuando se reciben a tràves del backup. Con esto se fuerza que todo el tràfico saliente de la Red IP-MPLS Local use el PoI principal.
- Tràfico entrante a la Red IP-MPLS Local: Las redes anunciadas hacia la red IP_MPLS Internacional seràn marcadas con MED=1000 cuando se anuncian a travès del PoI backup. Con esto se fuerza que todo el tràfico entrante a la Red IP-MPLS local use el PoI principal.

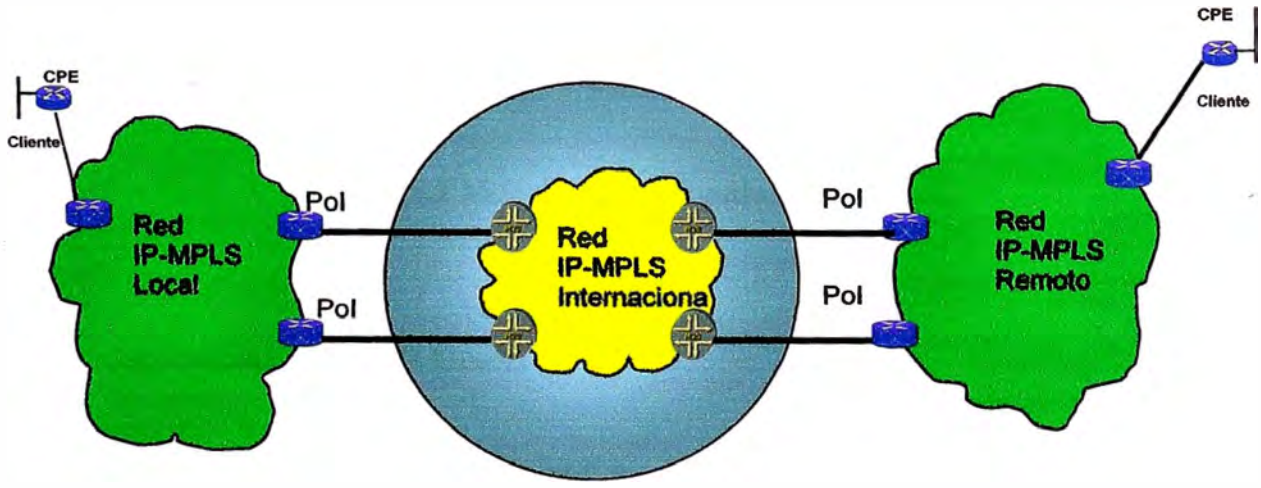

Fig. 4.8 Configuración de los PoIs.

CAPITULO V

PLANTILLAS DE CONFIGURACION PARA LA PROVISION DE ENLACES VPN INTERNACIONAL

Para esta parte vamos a considerar un modelo de un circuito Internacional que se compone de un circuito VPN local Redundante utilizando protocolo BGP, donde el acceso principal se encuentra configurado con una interfaz física V35, tal como de muestra en la Fig. Nº 5.1

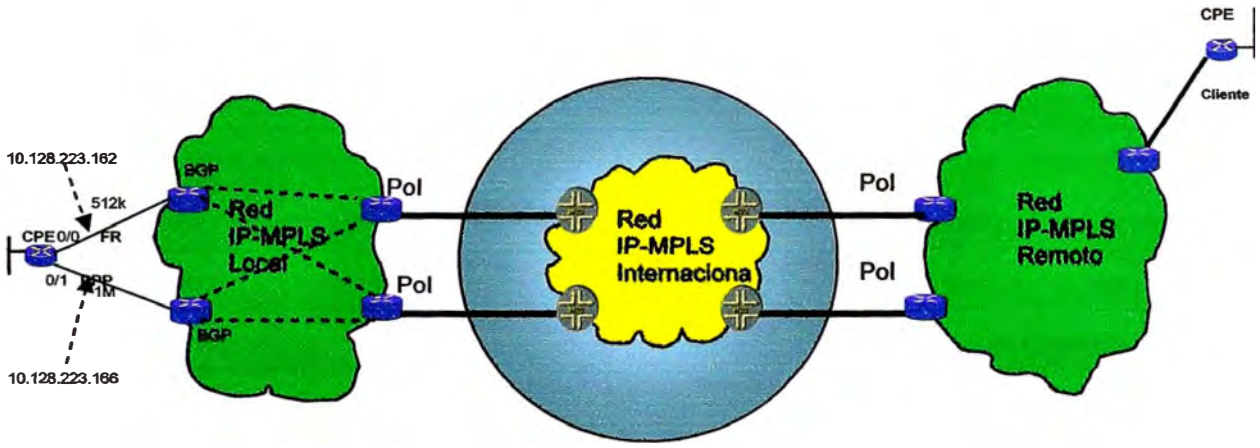

Fig. N° 5.1 Modelo de un circuito Internacional

5.1 Configuracion en los CEs locales

Una vez finalizado la Tramitación del pedido, se procederá a ejecutar la configuración del router local tanto en la Red IP-MPLS Local y en la Red IP-MPLS remota .considerando los parámetros contratados por el cliente en cada una de los paises donde tiene instalado sus oficinas.

5.1.1.-Configuracion PPP de los routers EDC

En el caso que presentamos como ejemplo de una configuración de un Router de cliente al router PE de la red IP-MPLS Local, se considera los sgts parámetros

- se configura la interface serial con Protocolo PPP.
- El protocolo de routing con el PE es BGP

```
UNI  PERU #sh conf
Using 3970 out of 29688 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname UNI  PERU
!
logging buffered 4096 debugging
enable password 7 110A1016141D
!
username operador privilege 15 password 7 104D0E1C0114
voice-card 1
!
ip subnet-zero
!
!
ip telnet tos 0
!
!
class-map match-all DATA
  match access-group 101
```

```
class-map match-all VOZ
  match access-group 100
!
!
policy-map IPVPN_512k
  class VOZ
    priority 384
  class DATA
   bandwidth 128
  class class-default
  fair-queue
policy-map IPVPN_1024k
  class VOZ
    priority 768
  class DATA
   bandwidth 192
  class class-default
   fair-queue
!
!
!
!
!
!
!
!
!
!
!
!
mta receive maximum-recipients 0
!
controller E1 1/0
```

```
!
!
!
!
interface Loopback0
 ip address 201.28.24.37 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.250.73.8 255.255.248.0 secondary
 ip address 10.250.65.8 255.255.248.0
 no ip redirects
 no ip proxy-arp
 ip route-cache policy
 ip policy route-map DATOS
 shutdown
 speed auto
 full-duplex
 no keepalive
 no cdp enable
!
interface Serial0/0
 description *** Enlace WAN del CD 42792 a 512k ***
 bandwidth 512
 ip address 10.128.223.162  255.255.255.252
 no ip redirects
 no ip proxy-arp
 encapsulation frame-relay IETF
 load-interval 30
 frame-relay traffic-shaping
 frame-relay interface-dlci 16
  class VOIP512K
 frame-relay lmi-type ansi
!
```

```
interface Serial0/1
 description *** Enlace WAN del CD 42791 a 1024k ***
 ip address 10.128.223.166  255.255.255.252
  no ip redirects
 no ip proxy-arp
 encapsulation ppp
 service-policy output IPVPN_1024k

router bgp 65513
 no synchronization
 bgp log-neighbor-changes
 network 10.250.64.0 mask 255.255.248.0
 network 10.250.72.0 mask 255.255.248.0
 network 201.28.24.37 mask 255.255.255.255
 neighbor 10.128.223.161 remote-as 6147
 neighbor 10.128.223.161 description -- CD=42792 BACKUP --
 neighbor 10.128.223.161 update-source Serial0/0
 neighbor 10.128.223.161 send-community
 neighbor 10.128.223.161 route-map SET_LP in
 neighbor 10.128.223.161 route-map SET_COMM out
 neighbor 10.128.223.161 filter-list 10 out
 neighbor 10.128.223.165 remote-as 6147
 neighbor 10.128.223.165 description -- CD=42791 PRINCIPAL ---
 neighbor 10.128.223.165 update-source Serial0/1
 neighbor 10.128.223.165 send-community
 neighbor 10.128.223.165 filter-list 10 out
 no auto-summary

ip classless
no ip http server
ip bgp-community new-format
ip as-path access-list 10 permit ^$
ip as-path access-list 10 deny .*
```

```
!
!
ip prefix-list RED_LOCAL seq 5 permit 10.250.64.0/21
ip prefix-list RED_LOCAL seq 10 permit 201.28.24.37/32
ip prefix-list RED_LOCAL seq 15 permit 10.250.72.0/21
!
!
map-class frame-relay VOIP512K
 frame-relay cir 512000
 frame-relay bc 5000
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output IPVPN_512k
 frame-relay fragment 640
access-list 100 permit udp any any range 16384 32767
access-list 100 permit tcp any any eq 1720
access-list 100 permit tcp any eq 1720 any
access-list 100 permit udp any any precedence critical
access-list 100 permit udp any any dscp ef
access-list 101 permit ip any any
!
route-map SET_LP permit 10
 set local-preference 90
!
route-map SET_COMM permit 10
 match ip address prefix-list RED_LOCAL
 set community 6147:90
!
route-map SET_COMM permit 20
!
call rsvp-sync
!
!
```

```
mgcp profile default
!
!
!
dial-peer cor custom
!
!
!
banner motd ^CCC
line vty 0 4
 password 7 094F471A1A0A
 login local
line vty 5 15



_**********************************************************
*                UNI PERU                                  *
*            Av. TUPAC AMARUC S/N                          *
*                                                          *
*             CD 42791      CD 42792                       *
*            IP VPN A 1 M.  IP VPN A 512K                  *
*                                                          *
* ********************************************************
^C
!
line con 0
line aux 0

 login local
!
!
end
```

5.1.2.-Configuracion frame relay de los routers EDC

En esta configuración presentamos a la conexión del enlace del CE con el PE de la Red IP-MPLS local utilizando las sgts características:

- se configura la interface serial con Protocolo Frame relay.
- El protocolo de routing con el PE es BGP

```
UNI  PERU#sh conf
Using 8077 out of 29688 bytes
!
! Last configuration change at 13:04:36 UTC Wed Apr 12 2006 by operador
! NVRAM config last updated at 13:06:11 UTC Wed Apr 12 2006 by operador
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname UNI  PERU
!
logging buffered 4096 debugging
enable password 7 110A1016141D
!
username operador privilege 15 password 7 104D0E1C0114
voice-card 1
!
ip subnet-zero
ip cef
!
!
ip telnet tos 0
!
```

```
!
class-map match-any OURO
 match ip precedence 3
class-map match-all DATA
 match access-group 101
class-map match-any VoIP
 match ip precedence 5
 match ip dscp cs5
 match access-group 100
class-map match-all VOZ
 match access-group 100
class-map match-any SUPORTE
 match ip precedence 2
class-map match-any OURO_IN
   match access-group name OURO
!
!
policy-map CE-to-PE
 class VoIP
  priority 307
  set precedence 5
 class OURO
  bandwidth 400
 class SUPORTE
  bandwidth 16
  set dscp af21
 class class-default
  fair-queue
  random-detect dscp-based
policy-map Traffic_IN
 class OURO  IN
  police cir 307000
    conform-action set-prec-transmit 5
```

```
    exceed-action set-dscp-transmit default
  class class-default
   set dscp default
policy-map IPVPN_512k
  class VOZ
    priority 384
  class DATA
   bandwidth 128
  class class-default
   fair-queue
policy-map IPVPN_1024k
  class VOZ
    priority 307
  class DATA
   bandwidth 400
  class class-default
   fair-queue
!
isdn switch-type primary-qsig
!
!
!
!
!
!
!
!
!
!
!
!
!
mta receive maximum-recipients 0
!
controller E1 1/0
```

```
 framing NO-CRC4
 pri-group timeslots 1-16
!
!
!
!
interface Loopback0
 ip address 201.28.24.37 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip id gk_uni_peru ipaddr 10.236.1.13 1719
 h323-gateway voip h323-id UNI_PERU
 h323-gateway voip tech-prefix 5101
 h323-gateway voip bind srcaddr 201.28.24.37
!
interface Loopback20
 ip address 200.148.171.39 255.255.255.255
!
interface Tunnel20
 ip address 172.16.1.29 255.255.255.252
 tunnel source 201.28.24.37
 tunnel destination 201.28.24.31
!
interface FastEthernet0/0
 ip address 10.250.73.8 255.255.248.0 secondary
 ip address 10.250.65.5 255.255.248.0
 no ip redirects
 no ip proxy-arp
 ip route-cache policy
 ip policy route-map DATOS
 speed auto
 full-duplex
 service-policy input Traffic_IN
 no cdp enable
```

```
!
interface Serial0/0
 description *** Enlace WAN del CD 42792 a 512k ***
 bandwidth 512
 ip address 10.128.223.162 255.255.255.252
 no ip redirects
 no ip proxy-arp
 encapsulation frame-relay IETF
 load-interval 30
 frame-relay traffic-shaping
 frame-relay interface-dlci 16
  class VOIP512K
 frame-relay lmi-type ansi
!
interface Serial0/1
 description *** Enlace WAN del CD 42791 a 1024k ***
 bandwidth 1024
 ip address 10.128.223.166 255.255.255.252
 no ip redirects
 no ip proxy-arp
 encapsulation ppp
 load-interval 30
 service-policy output CE-to-PE
!
interface Serial1/0:15
 no ip address
 no logging event link-status
 isdn switch-type primary-qsig
 isdn overlap-receiving T302 2000
 isdn incoming-voice voice
 isdn send-alerting
 isdn bchan-number-order ascending
 isdn sending-complete
```

```
 no cdp enable
!
router bgp 65513
 no synchronization
 bgp log-neighbor-changes
 network 10.250.64.0 mask 255.255.248.0
 network 10.250.72.0 mask 255.255.248.0
 network 201.28.24.37 mask 255.255.255.255
 neighbor 10.128.223.161 remote-as 6147
 neighbor 10.128.223.161 description -- CD=42792 BACKUP --
 neighbor 10.128.223.161 update-source Serial0/0
 neighbor 10.128.223.161 weight 90
 neighbor 10.128.223.161 send-community
 neighbor 10.128.223.161 route-map SET_LP in
 neighbor 10.128.223.161 route-map PATH out
 neighbor 10.128.223.161 filter-list 10 out
 neighbor 10.128.223.165 remote-as 6147
 neighbor 10.128.223.165 description -- CD=42791 PRINCIPAL ---
 neighbor 10.128.223.165 update-source Serial0/1
 neighbor 10.128.223.165 weight 120
 neighbor 10.128.223.165 send-community both
 neighbor 10.128.223.165 soft-reconfiguration inbound
 neighbor 10.128.223.165 route-map SET_LP in
 neighbor 10.128.223.165 filter-list 10 out
 no auto-summary
!
ip classless
ip route 200.153.1.128 255.255.255.192 Tunnel20
no ip http server
ip bgp-community new-format
ip as-path access-list 10 permit ^$
ip as-path access-list 10 deny .*
!
```

```
!
ip prefix-list RED_LOCAL seq 5 permit 10.250.64.0/21
ip prefix-list RED_LOCAL seq 10 permit 201.28.24.37/32
ip prefix-list RED_LOCAL seq 15 permit 10.250.72.0/21
!
ip access-list extended OURO
 permit tcp any any range 3600 3699
 permit tcp any any range 3200 3299
 permit tcp any any range 9100 9102
 permit tcp any any eq 2108
 permit tcp any any eq 2107
 permit ip host 10.248.16.28 any
 permit ip any host 10.248.16.28
!
!
map-class frame-relay VOIP512K
 frame-relay cir 512000
 frame-relay bc 5000
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output IPVPN_512k
 frame-relay fragment 640
access-list 100 permit udp any any range 16384 32767
access-list 100 permit tcp any any eq 1720
access-list 100 permit tcp any eq 1720 any
access-list 100 permit udp any any precedence critical
access-list 100 permit udp any  any dscp ef
access-list 101 permit ip any any
!
route-map SET_LP permit 10
 set local-preference 90
!
route-map PATH permit 11
```

```
!
ip prefix-list RED_LOCAL seq 5 permit 10.250.64.0/21
ip prefix-list RED_LOCAL seq 10 permit 201.28.24.37/32
ip prefix-list RED_LOCAL seq 15 permit 10.250.72.0/21
!
ip access-list extended OURO
 permit tcp any any range 3600 3699
 permit tcp any any range 3200 3299
 permit tcp any any range 9100 9102
 permit tcp any any eq 2108
 permit tcp any any eq 2107
 permit ip host 10.248.16.28 any
 permit ip any host 10.248.16.28
!
!
map-class frame-relay VOIP512K
 frame-relay cir 512000
 frame-relay bc 5000
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output IPVPN_512k
 frame-relay fragment 640
access-list 100 permit udp any any range 16384 32767
access-list 100 permit tcp any any eq 1720
access-list 100 permit tcp any eq 1720 any
access-list 100 permit udp any any precedence critical
access-list 100 permit udp any  any dscp ef
access-list 101 permit ip any any
!
route-map SET_LP permit 10
 set local-preference 90
!
route-map PATH permit 11
```

```
 set metric 100
!
route-map SET_COMM permit 10
 match ip address prefix-list RED_LOCAL
 set community 6147:90
!
route-map SET_COMM permit 20
!
snmp-server community geredcip RO
snmp-server community GESTION RO
snmp-server trap-source Loopback20
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps tty
snmp-server enable traps isdn  call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps hsrp
snmp-server enable traps config
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps ipmulticast
snmp-server enable traps msdp
snmp-serverenable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps rtr
snmp-server enable traps syslog
snmp-server enable traps dlsw
snmp-server enable traps dial
snmp-server enable traps dsp card-status
```

```
snmp-server enable traps atm subif
snmp-server enable traps pppoe
snmp-server enable traps ipmobile
snmp-server enable traps vtp
snmp-server enable traps voice poor-qov
snmp-server enable traps dnis
snmp-server enable traps xgcp
snmp-server host 200.153.1.138 geredcip
call rsvp-sync
!
voice-port 1/0:15
 cptone PE
 timeouts initial 5
 timeouts interdigit 5
!
!
mgcp profile default
!
!
!
dial-peer cor custom
!
!
!
dial-peer voice 10 voip
 destination-pattern [1-9]T
 session target ras
 fax protocol cisco
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 20 voip
 destination-pattern 015T
```

```
 session target ras
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 3 0voip
 preference 1
 destination-pattern 015T
 session target ipv4:10.23 6.1.10
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 40 voip
 preference 2
 destination-pattern 015T
 session target ipv4:10.23 6.1.11
 ip qos dscp ef signaling
 no vad
!
dial-peer voice 1 pots
 destination-pattern 5101T
 direct-inward-dial
 port 1/0:15
!
gateway
!
rtr responder
banner motd
**************************************************************
*                UNI  PERU                                   *
*             Av. A. BENAVIDES  Callao                       *
*              CD 42791      CD 42792                        *
*             IP VPN A 1 M.  IP VPN A 512K                    *
* ************************************************************
```

```
^C
!
line con 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password 7 094F471A1A0A
 login local
line vty 5 15
 exec-timeout 0 0
 login local
!
ntp clock-period 17208319
ntp server 10.236.0.51 source FastEthernet0/0
!
end

UNI_PERU#
```

5.2 Configuracion en los PEs de la red IP_MPLS locales

En este capitulo trataremos la configuración del circuito VPN Internacional en los PEs de las redes IPMPLS local y remota asì como tambien en la Plataforma Internacional. en estos 3 centros de configuración , se trabajarà con los parámetros ya establecidos con el cliente como son su ancho de banda y la calidad de servicio.

5.2.1.-Asignacion de la direccion WAN

En este paso , se elegirá la dirección IP , que servirá como la dirección WAN que se configurara en la serial del Router del cliente , así como también se configurara en la interface serial asignada al cliente en el PE.

El proveedor asignara un pool de direcciones IP privadas, las mismas que servirà para configurar las direcciones IPWAN de cada una de las oficinas del cliente.

En la Tabla Nº 5.1, observamos como ejemplo, un rango de direcciones IP WAN privadas.

TABLA Nº 5.1 Direcciones IP-WAN

CLIENTE	CD	IP PRIVADA	NODO	IP PRIVADA	NODO
UNI	42792	10.128.223.162	WASPE1	10.129.223.162	WASPE2
UNI	42791	10.128.223.166	WASPE1	10.129.223.166	WASPE2
UNI		10.128.223.170	WASPE1	10.129.223.170	WASPE2
UNI		10.128.223.174	WASPE1	10.129.223.174	WASPE2
UNI		10.128.223.178	WASPE1	10.129.223.178	WASPE2
UNI		10.128.223.182	WASPE1	10.129.223.182	WASPE2
UNI		10.128.223.186	WASPE1	10.129.223.186	WASPE2
UNI		10.128.223.190	WASPE1	10.129.223.190	WASPE2

En este caso , se asignarà dos direcciones IP WAN: uno para el circuito Principal y el otro para el circuito de respaldo , los mismos que se identificaran con un nùmero digital :

CD=42792, IPWAN: 10.128.223.162 con mascara 255.255.255.252

CD=42791, IPWAN: 10.128.223.166 con mascara 255.255.255.252

5.2.2.-Activacion de la VRF de la VPN

Se iniciará la configuración de la VRF , donde el **RD** , es un número de 8 octetos, cuyo propósito es el de permitir crear rutas diferentes a una misma dirección IPv4. Es decir, permite identificar las rutas de una VPN. Dado que el valor de **RD** es único y distinto para

cada VPN. Gracias al **RD**, VPNs diferentes pueden usar las mismas direcciones IPv4 para cada uno de sus oficinas.

El RD està compuesto por un campo de dos bytes denominado "tipo" y 6 bytes para almacenar un valor definido por el proveedor,tal como se observa en la Fig .5.2 .El campo de tipo determina la longitud de los dos subcampos que forman el valor (valor administrativo y número asignado), asì como el significado del campo administrativo. Actualmente hay dos valores par el campo "type" :0 y 1, tal como se muestra en la tabla 5.2

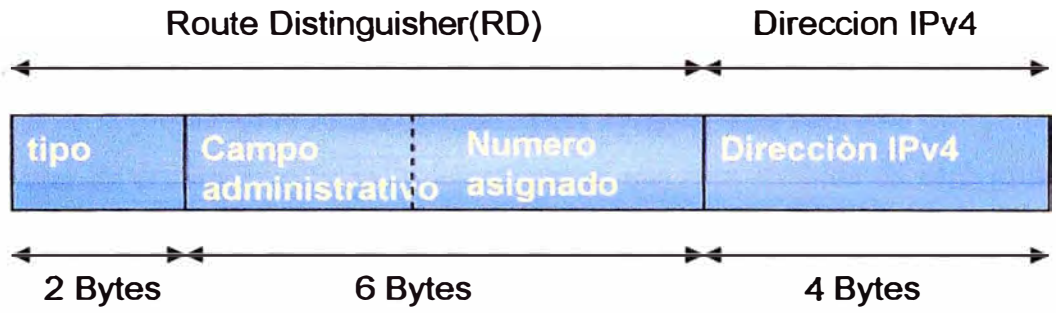

Fig. 5.2 Campo del Route Distinguisher RD

Para,el tipo 0, el subcampo administrativo tiene 2 bytes y el numero asignado 4. El campo administrativo contendrá el Número de Sistema Autónomo, mientras que el nùmero asignado tendrá un valor que lo definira el provedor de servicios Local.

Para el tipo 1 ,el subcampo administrativo tiene 4 bytes y el numero asignado 2. El campo administrativo contendrá una dirección IPv4 (dirección Loopback del PE), y el campo de número asignado tendrá un valor definido por el proveedor de servicios Local.

TABLA N° 5.2 Tipo de subcampo administrativo

TIPO	Nro Bytes Sub Campo administrativo	Nro Bytes Número asignado
0	2	4
1	4	2

En la configuración de la VRF del cliente cargado en el PE , se identifica el Tipo 1 , donde el subcampo administrativo y numero asignado se asociaran con los sgts. Valores:

Subcampo administrativo: 10429 (autonomo system)
Numero asignado:25800 (rd00)

El route Target . Identifica una colección de VRFs a las cuales el PE distribuya las rutas .Un PE utiliza este atributo para importar las rutas remotas dentro de sus VRFs
Antes de distribuir las rutas locales a otros PEs, el PE de acceso añade a cada ruta local aprendida de los CEs , el atributo de Route Target. El valor de RT se define mediante la política de exportación definida para la VRF.
Al conjunto de valores de RT que un router de acceso asocia a una ruta recibida de una oficina de la propia VPN se denomina Export Targets. Y al conjunto de valores de RT que un router de acceso emplea para determinar si una ruta recibida de otro router de acceso puede crear una entrada en la tabla de routing especifica (VRF) para la VPN asociada a la mencionada oficina se denomina Import Target.
Antes de instalar las rutas que provienen de otro PE, cada VRF del PE de salida asocia una politica de importación de target. Un PE instalará una ruta VPN-IPv4 en una VRF si el atributo de Route target asociado al anuncio coincide con uno de los RT importados por el PE de dicha VRF.

Para la Interconexión entre las Redes IP-MPLS de diferentes paises se considera que el **rd** de cada cliente sea asignado por la Empresa que realizará la gestión de la red VPN del cliente y que sea esta la que se utilice en su red IP-MPLS Local.

```
ip vrf UNI
description VPN INTERNACIONAL UNI PERU
rd 10429:25800
export map exportar_12956_VPNINT
route-target export 10429:25800
route-target import 10429:25800
route-target import 12956:1000
maximum routes 1000 75
```

5.2.3 Configuracion de routing en el PE

La configuración de routing que se utiliza para el cargar en los PEs de la Red IP-MPLS pueden ser de dos tipos:

a. Routing con RIP

Esta configuración se realiza en el PE donse se conecta físicamente el Router CE del cliente y solo se ejecuta una sola vez por cada configuración de un nuevo cliente. De este modo se activará las sgts acciones:

- Activar la tabla de routing específica de la VPN en el router PE.
- Activar el BGP asociado a la tabla de routing . entendiendo que en el PE ya estan dadas de alta todas las conexiones BGP con el resto de PE´s peretenecientes a la Red IP-MPLS Local.
- Se redistribuye el RIP en el BGP, de modo que se propagen las rutas de la sede en toda la VPN.

```
router rip
 version 2

 address-family ipv4 vrf UNI
 redistribute bgp 6147 metric 2
 network 10.0.0.0
 no auto-summary
 version 2
 exit-address-family

router bgp AS (Sistema Autonomo de la red Local)

Address-family ipv4 vrf vpn <AS> UNI
redistribute rip metric 200
redistribute connected
```

default-information originate
no auto-summary
no synchronization
exit-address-family

- **Routing con BGP**

Principalmente se utiliza con la configuración de dos enlaces uno principal y el otro como backup , ambos cargados en dos PE´s diferentes a fin de poder establecer la redundancia completa.

Configuración Principal en el ROUTER PE1:

router bgp 6147

!
address-family ipv4 vrf UNI
redistribute rip metric 200
neighbor 10.128.223.166 remote-as 65513
neighbor 10.128.223.166 description -- CD=42791 PRINCIPAL ---
neighbor 10.128.223.166 update-source Serial0/1/2:0
neighbor 10.128.223.166 activate
neighbor 10.128.223.166 send-community both
neighbor 10.128.223.166 soft-reconfiguration inbound
neighbor 10.128.223.166 route-map set_CUSTOMER_LP in
no auto-summary
no synchronization
table-map MIPO
exit-address-family

Configuración Backup en el ROUTER PE2:

```
router bgp 6147
!
 address-family ipv4 vrf UNI
 redistribute rip metric 200
 neighbor 10.128.223.162 remote-as 65513
 neighbor 10.128.223.162 description -- CD=42792 BACKUP ---
 neighbor 10.128.223.162 activate
 neighbor 10.128.223.162 soft-reconfiguration inbound
 neighbor 10.128.223.162 route-map set_CUSTOMER_LP in
 no auto-summary
 no synchronization
 table-map MIPO
 exit-address-family
!
```

5.3 Configuracion en el punto de interconexion PoI

Se configura en los dos PEs designados para Interconectar con la Red IP-MPLS Internacional, considerandose a uno de ellos como el de la salida principal y al otro como el de la salida secundaria.

Se tendrá que realizar las sgts configuraciones:

Se configurará los parámetros necesarios para dar de alta a los circuitos VPNs, esto es activar la tabla de routing, activar el protocolo de routing para la VRF y activación del BGP para esa VRF.

Alta de conexión física de cliente, Para este caso además de las interfaces que se utilizan para el acceso de los clientes, se va a tener que usar las interfaces POS y FastEhternet.

5.3.1 Configuracion de conexión fisica en el router PoI principal.

```
!
ip vrf UNI
 description VPN INTERNACIONAL UNI PERU
 rd 10429:25800
 export map exportar_12956_VPNINT
 route-target export 10429:25800
 route-target import 10429:25800
 route-target import 12956:1000
 maximum routes 1000 75

!
interface POS4/0.102 point-to-point
 ip vrf forwarding UNI
 ip address 172.20.31.46 255.255.255.252
 frame-relay interface-dlci 102
```

5.3.2. Configuracion de conexión fisica en el router PoI backup

```
!
ip vrf UNI
 description VPN INTERNACIONAL UNI PERU
 rd 10429:25800
 export map exportar_12956_VPNINT
 route-target export 10429:25800
 route-target import 10429:25800
 route-target import 12956:1000
 route-target import 700:1
 maximum routes 500 75
!
```

```
!
interface FastEthernet12/0/0.4
 encapsulation dot1Q 102
 ip vrf forwarding UNI
 ip address 172.20.31.50 255.255.255.252
 no snmp trap link-status
!
```

5.3.3 Configuracion de routing en el PE principal hacia un PoI

El protocolo de routing es BGP y se consideraran los sgt casos:

Normal : Donde se considerara que en una red IP-MPLS Local existe un mismo sistema autonomo ,donde todos los PEs se intercambian las redes mediante el Protocolo iBGP.
AS-Override: Se considera a aquellos

```
!
router bgp 6147
!
 address-family ipv4 vrf UNI
 redistribute connected
 redistribute rip metric 200
 neighbor 172.20.31.45 remote-as 12956
 neighbor 172.20.31.45 update-source POS4/0.102
 neighbor 172.20.31.45 activate
 neighbor 172.20.31.45 send-community both
 neighbor 172.20.31.45 remove-private-AS
 neighbor 172.20.31.45 advertisement-interval 10
 neighbor 172.20.31.45 soft-reconfiguration inbound
 neighbor 172.20.31.45 distribute-list NO_WAN_EDC_VPNINT out
 neighbor 172.20.31.45 route-map in_default_PoI in
 neighbor 172.20.31.45 route-map out_MED_PPAL out
```

neighbor 172.20.31.45 maximum-prefix 1500
no auto-summary
no synchronization
table-map MIPO
exit-address-family

5.3.4. Configuración de routing en el PE backup hacia un POI

!
router bgp 6147

!
address-family ipv4 vrf UNI
redistribute connected
redistribute rip metric 200
neighbor 172.20.31.49 remote-as 12956
neighbor 172.20.31.49 update-source FastEthernet12/0/0.4
neighbor 172.20.31.49 activate
neighbor 172.20.31.49 send-community both
neighbor 172.20.31.49 remove-private-AS
neighbor 172.20.31.49 advertisement-interval 10
neighbor 172.20.31.49 soft-reconfiguration inbound
neighbor 172.20.31.49 distribute-list NO_WAN_EDC_VPNINT out
neighbor 172.20.31.49 route-map in_default_PoI in
neighbor 172.20.31.49 route-map out_MED_PPAL out
neighbor 172.20.31.49 maximum-prefix 1500
default-information originate
no auto-summary
no synchronization
table-map MIPO
exit-address-family

CAPITULO VI
SOLUCION DE PROBLEMAS OCURRIDOS EN LOS ENLACES VPN

En este capitulo, se presentará los comandos necesarios para solucionar los problemas que ocurren con las comunicaciones de los clientes con el servicio VPN Internacional. Para poder determinar las fallas se aplican las sgts acciones:

Verificación del Nivel Físico Local
Comprobación del Routing en el PoI
Pruebas de Conectividad

6.1.- Verificación del Nivel Físico Local

Ante el reclamo por una averìa en un circuito VPN Internacional se procede a verificar localmente el Estado de Nivel 2 y Nivel 1, ambas verificaciones se logran con el siguiente comando ejecutado desde la posición del operador del Centro de Gestion:

```
WASPE6#sh int s0/1/2:0

Serial0/1/2:0 is up, line protocol is up
  Hardware is Multichannel E1
  Description: IPVPN|IPVPN|CD=42791|UNI|UNI PERU|1M|0,768,256,0|PPP|Av Tupac
Amaruc:Circuito Principal
  Internet address is 10.128.223.165/30
  MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec,
     reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, crc 16, Data non-inverted
```

```
  Keepalive set (10 sec)
  Last input 00:00:00, output 00:00:01, output hang never
  Last clearing of "show interface" counters 1w3d
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 116
  Queueing strategy: VIP-based fair queuing
  Output queue: 0/40 (size/max)
  5 minute input rate 1000 bits/sec, 1 packets/sec
  5 minute output rate 12000 bits/sec, 2 packets/sec
     7311968 packets input, 1284481624 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     7 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 7 abort
     9574488 packets output, 1650213950 bytes, 0 underruns
     116 packets late drop, 168553 bytes late drop
     0 output errors, 0 collisions, 8 interface resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions no alarm present
  Timeslot(s) Used:1-16, subrate: 64Kb/s, transmit delay is 0 flags


WASPE1#sh int s5/0/0/16:0
Serial5/0/0/16:0 is up, line protocol is up
  Hardware is cyBus E3
  Description: IPVPN|CD=42792|UNI|UNI PERU|512|0,384,128,0|FR CIRCUITO
RESPALDO
  Internet address is 10.128.223.161/30
  MTU 1500 bytes, BW 512 Kbit, DLY 20000 usec,
     reliability 255/255, txload 4/255, rxload 1/255
  Encapsulation FRAME-RELAY IETF, crc 16, loopback not set
  Keepalive set (10 sec)
  LMI enq sent  0, LMI stat recvd 0, LMI upd recvd 0
  LMI enq recvd 87990, LMI stat sent  87990, LMI upd sent  0, DCE LMI up
  LMI DLCI 0  LMI type is ANSI Annex D  frame relay DCE
  FR SVC disabled, LAPF state down
```

Broadcast queue 0/64, broadcasts sent/dropped 1001962/0, interface broadcasts 1000754
Last input 00:00:00, output 00:00:00, output hang never
Last clearing of "show interface" counters 1w3d
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: Class-based queueing
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 10000 bits/sec, 3 packets/sec
263267 packets input, 10632950 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 1 giants, 0 throttles
1078 input errors, 94 CRC, 0 frame, 0 overrun, 0 ignored, 983 abort
1274724 packets output, 541864166 bytes, 0 underruns
0 output errors, 0 collisions, 2 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions no alarm present
Timeslot(s) Used:1-8, Transmitter delay is 0 flags

6.2.- Comprobación del Routing en el PoI

Verificado el nivel fisico, se procederà a realizar los comandos de comprobación en el PoI verificando los anuncios de rutas referidas a la VPN del cliente. Para lograr este objetivo se ejecuta el sgt. Comando:

6.2.1.-Comandos de verificacion en el routing en el PoI principal

LURPE1#sh ip bgp vpnv4 vrf UNI su

BGP router identifier 200.48.175.186, local AS number 6147
BGP table version is 4769362, main routing table version 4769362
738 network entries using 90036 bytes of memory
758 path entries using 48512 bytes of memory
2393 BGP path attribute entries using 143580 bytes of memory

85 BGP rrinfo entries using 2040 bytes of memory
156 BGP AS-PATH entries using 3952 bytes of memory
37 BGP community entries using 888 bytes of memory
450 BGP extended community entries using 12448 bytes of memory
995 BGP route-map cache entries using 19900 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 321356 total bytes of memory
13 received paths for inbound soft reconfiguration
BGP activity 1024719/998542 prefixes, 3014405/2968997 paths, scan interval 15 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
172.20.31.45	4	12956	1041638	1014998	4769362	0	0	12:58:10	732

LURPE1#

6.2.2.- Comandos de verificacion del routing en el PoI respaldo

LINPE1#LINPE1#sh ip bgp vpnv4 vrf UNI su
BGP router identifier 200.48.175.141, local AS number 6147
BGP table version is 236827, main routing table version 236827
741 network entries using 91143 bytes of memory
1478 path entries using 94592 bytes of memory
1375 BGP path attribute entries using 82800 bytes of memory
81 BGP rrinfo entries using 1944 bytes of memory
650 BGP AS-PATH entries using 17120 bytes of memory
102 BGP community entries using 3592 bytes of memory
123 BGP extended community entries using 4046 bytes of memory
460 BGP route-map cache entries using 9200 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 304437 total bytes of memory
BGP activity 35233/23564 prefixes, 129297/106363 paths, scan interval 15 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
172.20.31.49	4	12956	47624	48054	0	0	0	2d21h	Idle (PfxCt)

LINPE1#

Aquí se observa que existe un problema con la sesiòn BGP en la salida de respaldo dado que se encuentra en el estado de Idle. Para poder determinar las causas de este problema se revisa el System Logs del router de red, donde se determina que el problema se ha debido a un exceso de anuncios de rutas por esta salida, por lo cual se deberà normalizar esta situación , variando el parámetro que define la cantidad maxima de rutas permitidas de la sgt. forma:

Antes de efectuar el cambio:

```
LINPE1#
!
ip vrf UNI
 description VPN INTERNACIONAL UNI_PERU
 rd 10429:25800
 export map exportar_12956_VPNINT
 route-target export 10429:25800
 route-target import 10429:25800
 route-target import 12956:1000
 route-target import 700:1
 maximum routes 500 75
```

Despues de la modificaciòn :

```
LINPE1#
!
ip vrf UNI_PERU
 description VPN INTERNACIONAL UNI_PERU
 rd 10429:25800
 export map exportar_12956_VPNINT
 route-target export 10429:25800
 route-target import 10429:25800
 route-target import 12956:1000
 route-target import 700:1
 maximum routes 1000 75
```

Como se observa ,se ha variado el parámetro de maximo numero de rutas permitidas de 500 a 1000 . En este momento es que se procede a ejecutar el comando de CLEAR para poder normalizar el estado del BGP

LINPE1#clear ip bgp 172.20.31.49 vrf UNI_PERU

Despues de ejecutar el commando de CLEAR , se verificarà el anuncio de las rutas por este acceso:

LINPE1#sh ip bgp vpnv4 vrf UNI_PERU su
BGP router identifier 200.48.175.141, local AS number 6147
BGP table version is 237104, main routing table version 237104
741 network entries using 91143 bytes of memory
1478 path entries using 94592 bytes of memory
1375 BGP path attribute entries using 82500 bytes of memory
81 BGP rrinfo entries using 1944 bytes of memory
650 BGP AS-PATH entries using 17120 bytes of memory
102 BGP community entries using 3592 bytes of memory
120 BGP extended community entries using 3974 bytes of memory
727 BGP route-map cache entries using 14540 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 309405 total bytes of memory
BGP activity 35234/23564 prefixes, 129311/106375 paths, scan interval 15 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
172.20.31.49	4	12956	47624	48054	0	0	0	2d21h	Active

Después se unos instantes se vuelve a repetir el comando, encontrándose el cambio del estado a UP , y donde se observa el incrementos de los prefijos recepcionados

LINPE1#sh ip bgp vpnv4 vrf UNI_PERU su

BGP router identifier 200.48.175.141, local AS number 6147

BGP table version is 237109, main routing table version 237109
741 network entries using 91143 bytes of memory
2220 path entries using 142080 bytes of memory
1395 BGP path attribute entries using 83760 bytes of memory
81 BGP rrinfo entries using 1944 bytes of memory
650 BGP AS-PATH entries using 17120 bytes of memory
102 BGP community entries using 3592 bytes of memory
122 BGP extended community entries using 4038 bytes of memory
763 BGP route-map cache entries using 15260 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 358937 total bytes of memory
11 received paths for inbound soft reconfiguration
BGP activity 35234/23564 prefixes, 130054/106376 paths, scan interval 15 secs

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
172.20.31.49	4	12956	47684	48090	237109	0	0	00:01:00	731

6.3.- Pruebas de conectividad

Es necesario realizar las pruebas de PING , desde el Router del Cliente , comenzando por la red Local , extendiendose hasta el Router remoto conectado en la red IP-MPLS remota , pasando por la Plataforma Internacional.

6.3.1.-Pruebas de ping hacia el PE local

Se accesa al router del cliente , desde donde se generarà los paquetes ICMP , hacia el la Interface en el PE local a donde se conecta el circuito del cliente:
WASPE6#telnet 10.128.223.166 /vrf UNI
Trying 10.128.223.166 ... Open

CC

```
**********************************************************
*                UNI PERU                                *
*           Av. Tupac Amaruc S/N                         *
*                                                        *
*            CD 42791      CD 42792                      *
*           IP VPN A 1 M.  IP VPN A 512K                 *
*                                                        *
* ********************************************************

User Access Verification

Username: XXXXXX
Password: YYYYYY

UNI_PERU#ping 10.128.223.166

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.128.223.166, timeout is 2 seconds:
!!!!!
```

6.3.2 Pruebas de continuidad hacia los PoIs

Se realiza pruebas de ping , direccionandolo hacia las interfaces PoI:

```
UNI_PERU#ping 172.20.31.46

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.20.31.46, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms
UNI_PERU#
```

6.3.3 Pruebas de continuidad hacia los routers de la Plataforma Internacional.

Tambien se envian los paquetes ICMP al router de la Plataforma Internacional:
UNI_PERU#ping 172.20.31.45

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.20.31.45, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/7/8 ms
UNI PERU#

6.3.4 Pruebas de continuidad con el router del cliente remoto

Finalmente, se realizarà pruebas con el extremo remoto, con el router del cliente que se encuentra conectado a la Red IP-MPLS remota:

UNI_PERU#ping 201.28.26.218
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 201.28.26.218, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/123/125 ms
UNI PERU#

6.3.5 Pruebas con el trace hacia la direccion del router remoto

Tambien se verifica la conectividad con el router remoto, realizando un TRACE y accesando al router remoto:
UNI PERU#traceroute 201.28.26.218

Type escape sequence to abort.

Tracing the route to 201.28.26.218

1 10.128.223.165 [AS 6147] 8 msec 8 msec 4 msec
2 172.20.31.46 [AS 6147] 8 msec 8 msec 8 msec
3 172.20.31.45 [AS 6147] 4 msec 8 msec 8 msec
4 * * *
5 * * *
6 * * *
7 * * *
8 201.28.26.218 [AS 10429] 116 msec * 113 msec
UNI_PERU#

UNI_PERU#telnet 201.28.26.218
Trying 201.28.26.218 ... Open

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
+          ACESSO PERMITIDO SOMENTE A PESSOAS AUTORIZADAS                     +
+       TODAS AS CONEXOES ESTAO SENDO MONITORADAS E AUDITADAS
+
+              ATTENTION: AUTHORIZED PERSONAL ONLY.                           +
+                   DISCONNECT IMMEDIATELY.                                   +
+        DNS TE 200.153.0.68 Primario / 200.153.0.196 Secundario              +
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
```

User Access Verification

Username: XXXXXX

CAPITULO VII
IMPLEMENTACION DE ENLACES DE RESPALDO

7.1 Descripcion de los accesos IPSec

Como medio alternativo para otorgar una conexión de respaldo ante una eventualidad que afecte los enlaces VPNs configurados en una Plataforma IP-MPLS, surge los acceso IPsec(IP Security Protocol) a traves de Internet, terminado los tùneles en un equipo de red.
Siendo una ventaja de IPSec sobre los diferentes mecanismo de "tunneling" para implementar VPNs, la de encriptar los paquetes.
IPSec es un estandar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP y UDP).
Dentro del IPSec se distingen los siguientes componentes:

- Dos protocolos de seguridad: IP Authentication Header (AH) e IP Encapsulating security Payload(ESP).
    - Un protocolo de gestión de claves Internet Key Exchange (IKE) que permite dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

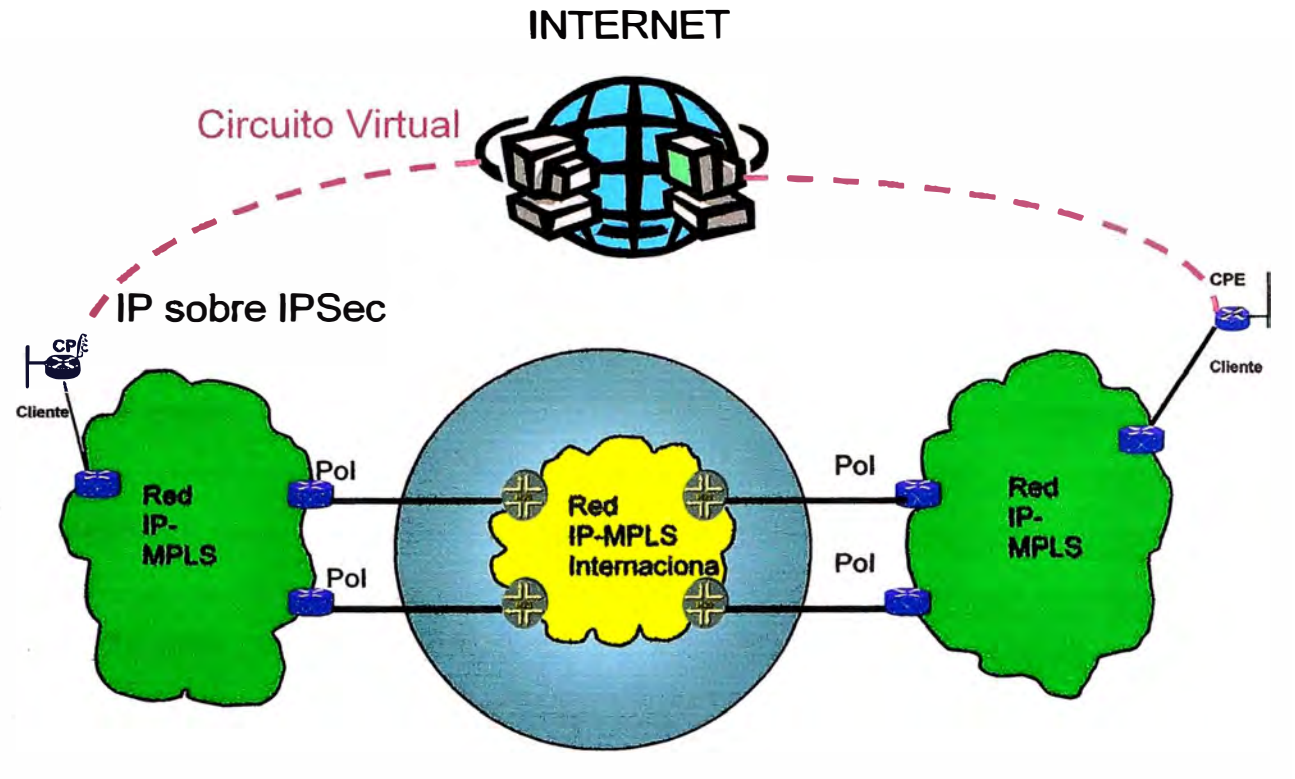

Fig 7.1 Enlace de respaldo

7.2 Plantilla de configuracion IPsec en los routers CE

UNI CD42488#sh run
Building configuration...

Current configuration : 3234 bytes

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption

hostname UNI CD42488

boot-start-marker

```
boot system flash:c2600-ik9s-mz.122-15.T16.bin
boot system flash :
boot-end-marker
!
logging buffered 4096 debugging
enable password 7 046B392939751E1A5141
!
no aaa new-model
!
resource policy
!
no network-clock-participate slot 1
no network-clock-participate wic 0
ip subnet-zero
!
!
ip cef
no ip domain lookup
ip name-server 200.48.0.51
no ip dhcp use vrf connected
!
!
crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
 lifetime 28800
crypto isakmp key tunelajegr0up@tempresas address 209.124.105.115
crypto isakmp key tunelajegr0up@tempresas address 201.134.169.254
crypto isakmp key tunelajegr0up@tempresas address 200.12.231.162
crypto isakmp key tunelajegr0up@tempresas address 200.91.88.90
crypto isakmp ccm
```

```
!
!
crypto ipsec transform-set MEXICO esp-3des esp-md5-hmac
crypto ipsec transform-set GUATEMALA esp-3des esp-md5-hmac
crypto ipsec transform-set COSTA_RICA esp-3des esp-md5-hmac
crypto ipsec transform-set NICARAGUA esp-3des esp-md5-hmac
!
!
crypto map REDVPN 1 ipsec-isakmp
 description ***TUNEL IPSEC CON NICARAGUA ISA SERVER***
 set peer 209.124.105.115
 set security-association lifetime kilobytes 100000
 set transform-set NICARAGUA
 set pfs group2
 match address 130
crypto map REDVPN 2 ipsec-isakmp
 description ***TUNEL IPSEC CON MEXICO CISCO SOHO 91***
 set peer 201.134.169.254
 set transform-set MEXICO
 set pfs group2
 match address 100
crypto map REDVPN 3 ipsec-isakmp
 description ***TUNEL IPSEC CON GUATEMALA ISA SERVER***
 set peer 200.12.231.162
 set security-association lifetime kilobytes 100000
 set transform-set GUATEMALA
 set pfs group2
 match address 110
crypto map REDVPN 4 ipsec-isakmp
 description ***TUNEL IPSEC CON COSTA_RICA ISA SERVER***
 set peer 200.91.88.90
 set security-association lifetime kilobytes 100000
 set transform-set COSTA  RICA
```

```
 set pfs group2
 match address 120
!
interface FastEthernet0/0
 description ****Conexion a MONLA****
 ip address 200.4.216.68 255.255.255.248
 duplex auto
 speed auto
 crypto map REDVPN
!
interface FastEthernet0/1
 description ****Conexion a Firewall****
 ip address 20.20.20.1 255.255.255.0 secondary
 ip address 200.4.216.75 255.255.255.248
 duplex auto
 speed auto
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 200.4.216.65
ip route 172.16.0.132 255.255.255.255 200.4.216.78
ip route 200.48.16.160 255.255.255.224 200.4.216.78
!
no ip http server
no ip http secure-server
!
!
access-list 100 permit ip 172.16.0.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 110 permit ip 172.16.0.0 0.0.0.63 172.17.200.0 0.0.0.255
access-list 110 permit ip 172.16.0.0 0.0.0.63 host 200.12.231.162
access-list 120 permit ip 172.16.0.0 0.0.0.63 172.17.100.0 0.0.0.255
access-list 120 permit ip 172.16.0.0 0.0.0.63 host 200.91.88.90
access-list 130 permit ip host 172.16.0.132 172.18.0.0 0.0.0.255
```

```
access-list 130 permit ip host 172.16.0.132 host 209.124.105.115
!
!
!
control-plane
!
dial-peer cor custom
!
line con 0
line aux 0
line vty 0 4
 password 7 01074B01561B140A326C5D
 login
!
!
end

UNI  CD42488#
```

CONCLUSIONES

1. El servicio VPN MPLS Internacional està basado en el estàndar de IETF RFC 2547 bis. Es por tanto un servicio de VPN basado en el protocolo IP. La red IP-MPLS mantiene entornos de routing separados e independiente para cada VPN, de mod que asegura la separaciòn completa de cada entorno de cliente, pudiendo ofrecer servicios de VPN sin ningún tipo de restricción sobre el direccionamiento utilizado por el cliente sobre una red IP/MPLS.
2. Una de las más importantes características del estandar RFC2547bis se definen los mecanismos bàsicos para proporcionar clases difenciadas de servicio sobre enlaces compartidos enter distintas aplicaciones. Los paquetes IP de cada una de las aplicaciones son marcados con una clase de servicio en el punto màs cercano a su origen, preferiblemente el mismo equipo originante del tràfico o, en su defecto, el equipo de conmutación que proporciona la comunicación con la red privada , manteniendose las mismas polìticas a lo largo de toda la red , de forma de asegurar una calidad de servicio especìfica para cada calidad, y, por ende, para cada aplicación.
3. El Servicio VPN MPLS es una alternativa màs econòmica para el cliente el cual necesita disponer de una red de “todos con todos”. Este servicio presenta una gran capacidad multiservicio IP para converger el transporte de datos ,voz e imàgenes ,sobre una ùnica conexión IP que garantiza los requerimientos especìficos de cada tipo de tràfico.
4. Este servicio permitirà la creación de extranets facilitando la integración plena de las empresas con nuevos entronos de trabajo como son sus clientes, proveedores, socios,etc

5 La aparicion de Internet posibilita nuevos mètodos de acceso màs econòmicos e universales y posibilita fácilmente la creación de VPNs IP .Esto ha producido .Esto a producido una fueret tendencia por parte de los proveedores de equipamiento e ISPs a ofertar este tipo de servicios , sin embargo las prestaciones que aportan las soluciones VPN IP basadsa en Internet no alcanzan los niveles de calidad exigidos por los clientes , por lo que los operadores han desarrollado redes MPLS de ùltima generaciòn que combinan la versatilidad del mundo IP con la fiabilidad de las redes privadas tradicionales.

6 En un futuro cercano aparecerán nuevas Tecnologías de acceso Universal (accesos IPsec a través de Internet) con una alta seguridad en la información, logrando una cobertura del servicio a nivel mundial.

BIBLIOGRAFÍA

1. Layer 3 VPN Service 1.0 Design and Implementation,
   Cisco, 2004.

2. CISCO MPLS Solution User Guide:Chapter 6, Administering Customer Edge Routers, 2003.

3. Interconnecting Cisco Network Devices 2003.

4. Los servicios de telecomunicaciones (redes, Aplicaciones y costes)
   Josè A. Carballar Falcòn RA-MA

5. Alta velocidad y calidad de servicio en redes IP,
   GA TOMAS, J-RAYA, RODRIGO, V RA-MA Editorial Febrero 2002.

6. BUILDING VPNs WITH IPSec and MPLS.
   Tan McGraw-Hill 2004.

7. Building MPLS-Based Broadband acces VPNs,
   Kumar Reddy Cisco Press, 2004

8. Building and Managing Virtual private Network,
   Dave Kosiur, Editorial Wiley, 1996