UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERIA ELECTRICA Y ELECTRONICA

DISEÑO DE UNA RED DE ALTA SEGURIDAD SOBRE LA ACTUAL RED DE LA ASOCIACION DE BANCOS DEL PERU

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO EN TELECOMUNICACIONES

PRESENTADO POR:
JORGE LUIS LEONARDO TORRES

PROMOCIÓN
2009 - II

LIMA – PERÚ
2013

DISEÑO DE UNA RED DE ALTA SEGURIDAD SOBRE LA ACTUAL RED DE LA ASOCIACION DE BANCOS DEL PERU

Dedicado a:

Dios, por brindarme salud;

A mis padres por guiarme siempre;

A mi hermana, por mostrarme que no hay límites cuando te propones mejorar y a mi hermano, por enseñarme a ser lo que soy y que nunca se debe parar de luchar;

A mi querida Universidad;

Y a mí angelito Mariela, que con su vida nos enseñó una lección para toda la vida.

SUMARIO

En este trabajo se presenta un estudio para mejorar la seguridad en las redes de los clientes cuyo negocio se encuentre involucrado con confidencialidad de la información que transporta.

En específico el trabajo se basa en la Red de Bancos del Perú, entre sus asociados y afiliados, detallando así el estado actual de la Red de Bancos.

Para lograr la confidencialidad de la información en toda la Red de Bancos se propone el uso del protocolo GET VPN, describiendo cómo se logra encriptar la información antes de entrar a la Red del Proveedor de servicios.

Finalmente se expondrá el diseño y propuesta para la actual red de Bancos, mejorando así la seguridad de la información.

INDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCION

Las redes en la actualidad se han convertido en socios estratégicos para las grandes empresas así como una fuente de desarrollo para el estado y la educación. Redes sobre las que actualmente no solo se cuenta con aplicaciones y datos críticos para el crecimiento de las empresas o entidades, sino que también soportan infraestructura de voz y video sobre IP, y que requieren a su vez una gran capacidad de la red capaces de poder brindar una comunicación directa entre las sedes remotas de las empresas involucradas, "punto a punto" (*branch to branch*).

Debido a estos requisitos la tradicional topología "punto a multipunto" (*Hub-and-spoke*) de las redes empresariales ya no es suficiente pues es una limitante al tener la necesidad de crear túneles y enlaces dedicados punto a punto, los cuales a su vez requieren de un equipamiento dedicado y de un procesamiento alto, pues al tener que mantener enlaces dedicados hacia una elevada cantidad de sedes se debe considerar dispositivos que soporten todos los enlaces y aumentan la dificultad al administrar esta red de equipos.

Así mismo, las redes actuales necesitan satisfacer la gestión de riesgos relacionados con la seguridad y el cumplimiento de las políticas de seguridad de las empresas para salvaguardar los datos, es decir implementar sistemas de seguridad capaces de soportar los ataques cada vez más comunes de intrusos con la intención de robar la información, conocer información clasificada e incluso simplemente molestar a las entidades por el simple hecho de que era fácil para ellos acceder a estos datos.

Para conseguir ambos propósitos es necesario contar con una tecnología capaz de proteger las infraestructuras tecnológicas pues conforme las redes se convierten en plataformas para un número cada vez mayor de dispositivos, aplicaciones y contenidos, la protección es una cuestión fundamental.

La tecnología a considerar es Group Encrypted Transport Virtual Private Network (GET VPN, Red Privada Virtual de Transporte Encriptado de Grupo).

Cisco (2008) afirma que: "GET VPN aporta mejoras de hasta 300% en el rendimiento. GET VPN representa una nueva categoría de VPNs diseñadas para encriptar datos transmitidos en redes de área extendida WAN. La solución ayuda a eliminar la necesidad de túneles punto a punto, lo que permite que las redes distribuidas de sucursales amplíen las VPN empresariales en varios miles de sitios al mismo tiempo soportando simultáneamente las necesidades de inteligencia de red que son esenciales para garantizar tanto la calidad de la voz y el vídeo, como la calidad de servicio, el enrutamiento y las opciones multicast. Debido a que la aplicación principal de GET VPN se ejecuta en redes basadas en conmutación multiprotocolo, la flexibilidad inherente de GET VPN permite a las empresas reforzar su seguridad gestionando su propia protección de red sobre el servicio WAN del proveedor de servicios".

Para cumplir con todo lo expuesto, este informe se divide en cuatro capítulos, los cuales son descritos a continuación:

El capítulo I, plantea aspectos fundamentales del trabajo, como son: Planteamiento de la necesidad o problema, objetivos generales y específicos, evaluación del problema, alcances del trabajo.

El Capítulo II, muestra un conjunto de definiciones que nos permitirán conocer el estado actual de la Red de Bancos y las consideraciones actuales en su diseño, tales como la topología y la estructura de los tipos de clientes con los que cuenta, tales como son los afiliados y los asociados. Se presenta un resumen de las tecnologías de seguridad y transporte con los que cuenta la Red de Bancos, explicando paso a paso como es que ocurre la comunicación entre cada una de sus sedes a través de la red del actual proveedor de servicios y de cómo se aprovecha de la tecnología MPLS que brinda para transportar la información con calidad de servicio, brindando cierta seguridad así como la alta redundancia con la que cuenta la Red de Bancos.

Se detalla los componentes de la tecnología MPLS, la estructura del paquete IP, la asignación de etiquetas y la conmutación de los paquetes.

En el Capítulo III, se expone con mayor detalle el protocolo GET VPN, los componentes en la red para realizar el encriptamiento. Se explica la arquitectura a nivel de paquetes y cabeceras y la arquitectura del protocolo GET- VPN utilizando en conjunto todo lo descrito anteriormente. Se detalla el SEC, que es el método de encriptación aprovechando así los beneficios de la tecnología IPSec y por último se menciona los beneficios de GET VPN.

En el Capítulo IV, se expone el proceso de diseño de la implementación del protocolo GET VPN en la Red de Bancos, se menciona la capacidad de los Routers CISCO que soportan el protocolo GET VPN, el software necesario y luego se diseña el cambio de Routers acorde a las necesidades de la Red de Bancos y todo en una Topología final.

CAPITULO I
PLANTEAMIENTO DE LA NECESIDAD

Este capítulo se desarrolla con la finalidad de presentar una manera clara y concisa el escenario bajo el cual nace la motivación de este informe y a qué necesidad responde. Se define cuáles son los alcances y aportes del mismo. Finalmente se dedica un punto a la síntesis de este informe enfocado en mejorar la seguridad en las comunicaciones, encriptando los mensajes, de la Red de Bancos y en general de cualquier cliente que maneje información confidencial y que desee ampliar el nivel de seguridad entre su Nodo Principal y sus nodos remotos, asegurándose que nadie dentro de la Red del Proveedor de servicios, algún intruso por ejemplo, podrá revisar o escanear la información pues esta se encuentra encriptada.

1.1 **Descripción del Problema:**

En los tiempos modernos todos, desde una persona común en su casa hasta las empresas más importantes del planeta, necesitan conectividad a las grandes redes de comunicaciones, como se muestra en la Figura 1.

Pero a su vez las redes son primariamente importantes para las empresas porque permite la comunicación y transacción de grandes cantidades de información.

Son justamente las grandes empresas, entre ellas los bancos que requieren realizar transacciones de alta velocidad, es decir tener las conexiones dedicadas entre sus sedes para garantizar que la información crítica (cuentas bancarias, claves de cuentas, transacciones financieras entre otros, que en algunos casos involucra millones de dólares), tenga la prioridad suficiente sobre otros aplicativos y es así que debido a la criticidad de la conectividad se plantea el esquema de las redes redundantes.

Lo expuesto anteriormente nos plantea un nuevo inconveniente pues al requerir anchos de banda dedicados para transacciones importantes nos damos cuenta que esta información queda expuesta si no prevemos la forma de brindar la seguridad y confiabilidad a nuestros enlaces no solo hacia el exterior sino en la misma Red del Proveedor de servicios.

El presente informe se en centra en la actual topología de la Red de Bancos del Perú, la cual cuenta con enlaces dedicados sobre una red MPLS y cuya topología es altamente redundante pues cuenta con dos enlaces de contingencia atendidos todos con última milla fibra óptica y atendidos desde Puntos de Presencia (POP) de la red MPLS ubicados geográficamente en lugares distintos.

De igual forma para garantizar la seguridad de la información y las transacciones de la Red de Bancos, se utiliza actualmente conexiones VPN sobre MPLS (MPLS – VPN) utilizando VRF, creando así lo que se denomina una Red Privada Virtual brindando 3 calidades de servicio al aprovechar los beneficios de la tecnología MPLS, creando sesiones activas con las sede remotas.

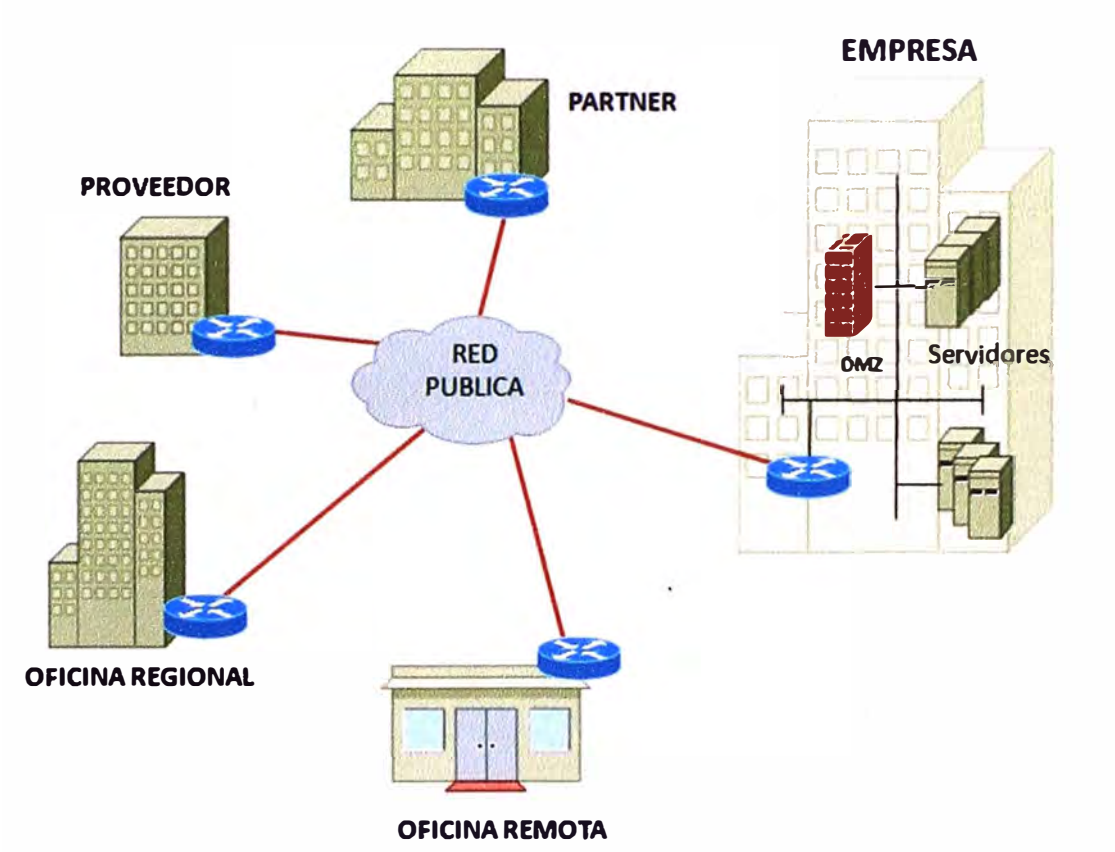

Figura 1. Esquema actual de las grandes empresas, distribuida en una Red Pública.
Fuente: Cisco Systems, 2004.

Como objetivo del presente informe se plantea el diseño de mejora de la Red de Bancos, con el uso protocolo GET VPN, el cual permite brindar seguridad sobre las redes dedicadas pero sin disminuir el performance de las Red al no necesitar sesiones activas dedicadas entre las sedes remotas (Cisco Systems, 2013).

1.2 Objetivos Generales:

- Analizar las ventajas del protocolo GET VPN sobre la actual Red de Bancos del Perú
- Plantear el uso del protocolo GET VPN para mejoras de seguridad sobre redes importantes tales como Fuerzas Armadas, Retails, entre otros clientes que deseen ampliar las posibilidades de mejorar la seguridad en sus comunicaciones.

1.3 Objetivos Específicos:

- Conocer los actuales esquemas de alta redundancia y de seguridad del estado actual de la Red de Bancos del Perú.
- Detallar el uso de MPLS – VPN y las modalidades que tiene para brindar seguridad en los enlaces.
- Analizar los beneficios del protocolo GET VPN a implementar sobre la actual topología de la Red de bancos del Perú.
- Fomentar el uso del protocolo GET VPN en el Perú mejorando el rendimiento de las Redes y la seguridad de estas.

1.4 Evaluación del Problema:

Actualmente en el Perú se tiene un "boom" de la Economía, se podría decir hasta sin precedentes debido a que mientras el mundo se encuentra en crisis el Perú mantiene un crecimiento económico casi constante durante los últimos 10 años, teniendo un crecimiento anual del PBI que se ha mantenido en el tiempo. (Álvarez, 2013)

Este denominado Boom es debido a la extracción de metales preciosos, es decir del sector minero, así como del sector de construcción entre muchos otros más, que actualmente no sólo centran sus operaciones en Lima, sino que han migrado sus centros de operaciones a los diferentes departamentos del Perú generándose así la descentralización de la economía. (Álvarez, 2013)

Es así que debido al crecimiento demográfico de la economía, las empresas del rubro construcción, mineras, así como bancos, cuentan con una mayor presencia en locales remotos y para poder cubrir las necesidades de comunicación y tráfico de datos críticos (hasta confidenciales) se requiere contar con una red de gran capacidad y altamente segura a la vez.

Actualmente contamos con redes que cumplen con ambos requerimientos pero que, o solo reducen su capacidad para brindar seguridad o en su defecto aumentan su capacidad pero sin brindar un mayor grado de seguridad en sus redes.

El presente informe busca contribuir a la mejora de las redes de las empresas o instituciones, centrándome en la mejora de la Red de Bancos del Perú, planteándose el uso del protocolo GET VPN.

1.5 Alcances del trabajo

El presente trabajo está orientado a ser una guía para aquellas personas que deseen mejorar el rendimiento de la red que administra o que deseen una guía para el uso del protocolo GET VPN. El aporte de este informe se encuentra en la manera cómo se ha recopilado la información y cómo está siendo presentada. El análisis presentado para la seguridad y redundancia es acerca del protocolo GET VPN y de cómo sirve de fundamento para el desarrollo de redes seguras y confiables.

1.6 Síntesis del trabajo

Se presenta un análisis de la actual red de Bancos del Perú indicando la topología para los asociados y los afiliados.

Se exponen los conceptos teóricos que permitan comprender el actual funcionamiento de la red de Bancos del Perú.

Se expone un análisis, así como lineamientos y recomendaciones para el uso del protocolo GET VPN.

Finalmente, se propone la implementación del protocolo GET VPN sobre la actual Red de Bancos del Perú.

CAPÍTULO II
ASPECTOS TEÓRICOS DE LA ACTUAL RED DE ASBANC

Para entender mejor esta investigación es necesario conocer aspectos teóricos relacionados a la conectividad, contingencia así como la seguridad y encriptación.

En este capítulo se desarrollan todos estos conceptos, comenzando por dar una idea de manera general acerca de los recursos con los que cuenta actualmente la Red de Bancos del Perú, para luego avocarnos en la arquitectura completa con la que cuenta para brindar la conectividad entre todos sus afiliados y asociados.

2.1 La Red de Bancos del Perú

La actual Red de Bancos del Perú es una asociación gremial que agrupa a los bancos e instituciones financieras privadas de nuestro país y cuyo principal objetivo es promover el fortalecimiento del sistema financiero privado, proporcionando a sus asociados servicios de información, asesoría y consulta, de esta manera es prioritario contar con enlaces altamente confiables pues las transacciones entre los bancos se vuelven críticas al estar involucrados grandes cantidades de dinero y no sólo en temas monetarios, pues también mantienen actualizados a todos los bancos acerca del estado financiero e historial crediticio de los usuarios, entre otra información relevante para los bancos.

De esta forma, entendiendo lo importante que es tener una red altamente confiable y segura para interconectar todos los bancos, la Red de Bancos del Perú cuenta con enlaces redundantes en cada uno de sus integrantes, los cuales están divididos en 2 grupos, el primer grupo son los Asociados (Los bancos más importantes del mercado) que forman un grupo de 16, mientras que también tenemos el grupo de Afiliados que está conformado por 50 entidades financieras y no financieras.

La diferencia entre ambos grupos es el nivel de redundancia pues los Asociados cuentan con una alta redundancia al contar con 3 enlaces mientras que los Afiliados solo con 2 enlaces, lo cual se pasará a detallar más adelante y se observa en las Figura 2, 3 y 4.

De esta manera, para conocer cómo se brinda actualmente la seguridad en la Red de Bancos del Perú, se explicará el uso de conexiones MPLS – VPN.

2.2 Diagramas Topológicos

2.2.1 Topología del Nodo Central:

En el Nodo Central o Nodo Principal se cuenta con los equipos que se encargan de definir las rutas y el direccionamiento a todas las sedes, es el equipamiento por el cual funciona toda la inteligencia de la Red de Bancos.

Los equipos se encuentran coubicados en el DataCenter de un conocido proveedor de Servicios, quien le brinda redundancia al tener el equipamiento distribuido en 2 lugares geográficamente separados para poder brindar una alta disponibilidad.

A continuación en la Figura 2, se muestra la topología del Nodo Central.

TOPOLOGIA – NODO CENTRAL

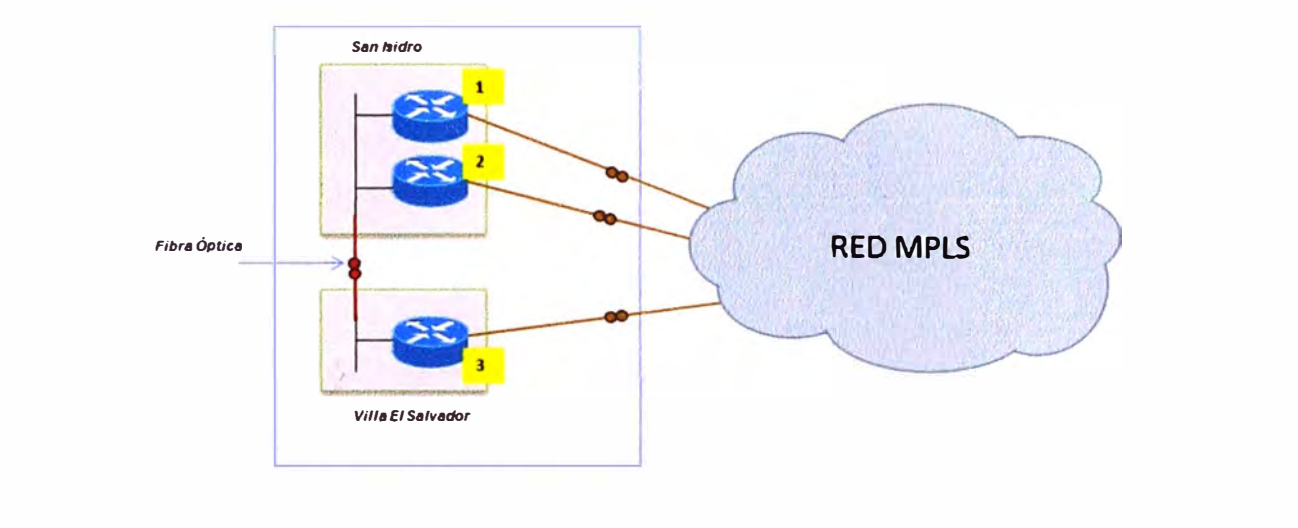

Figura 2. Topología del Nodo Central de la Red de Bancos

De la misma forma, en la Tabla 1 se describe el equipamiento en cada una de las sedes y en que direcciones se encuentran distribuidas.

Tabla 1. Equipamiento en el Nodo Central.

Descripción	Distrito	Tipo	Equipo	Cantidad
Principal	San Isidro	Principal	Cisco 2821	1
Principal	San Isidro	Secundario	Cisco 2821	1
Alterno	Villa el Salvador	Alterno	Cisco 2821	1

2.2.2 Topología Asociados:

La topología para un Asociado es una topología altamente redundante (muy parecida a la topología del Nodo Central), cuenta con 2 enlaces conectados a un Nodo Principal, el cual se encuentra conectado con un enlace dedicado de fibra óptica (Fibra oscura) hacia un Nodo Alterno.

El Nodo alterno se encuentra ubicado geográficamente en una ubicación distinta al Nodo Principal y este a su vez replica la base de datos ubicada en el Nodo Principal.

Los 3 enlaces se encuentran atendidos con medio de transmisión de fibra óptica y son atendidos desde Puntos de Presencia (Point of Presence – POP) distintos de la RED MPLS, revisar la Figura 3.

Tomando en cuenta la numeración se les denomina de la siguiente forma:

1 → Principal

2 → Secundario

3 → Alterno

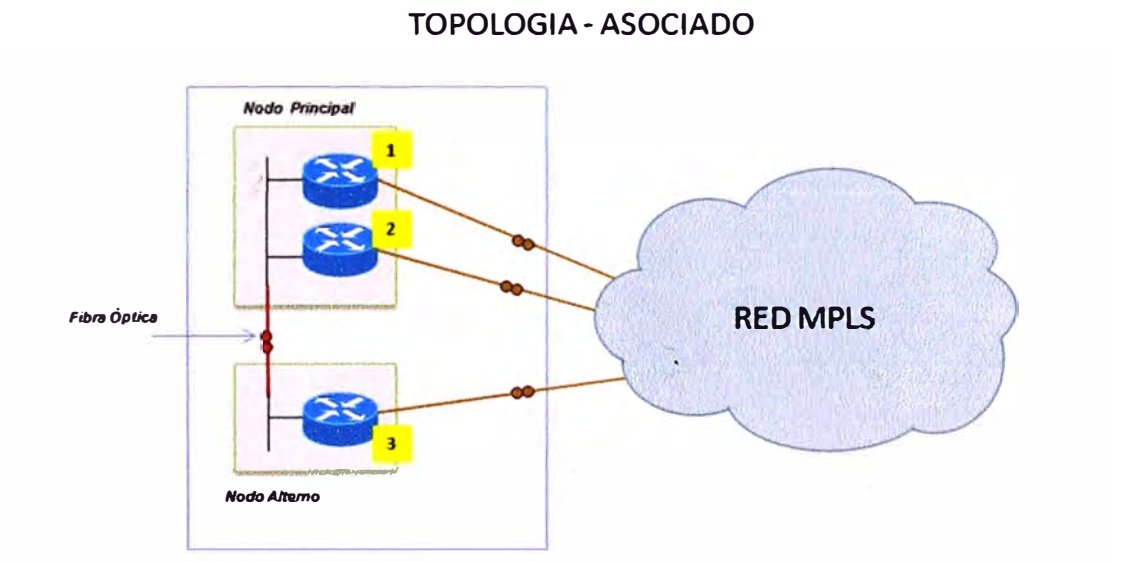

Figura 3. Topología de un Asociado de la Red de Bancos, Nodo Principal y Alterno.

De la misma forma, se describe el equipamiento de los Asociados en la Tabla 2.

Tabla 2. Equipamiento de los Asociados

Descripción	Tipo	Equipo	Cantidad
Principal	Principal	Cisco 2801	1
Principal	Secundario	Cisco 2601	1
Alterno	Alterno	Cisco 2801	1

2.2.3 Topología Afiliados:

Se podría considerar que la Red de Bancos cuenta con 2 tipos de afiliados, los cuales llamares Tipo I y T ipo II.

Afiliado Tipo I:

La topología para un Afiliado Tipo I es redundante, cuenta con 2 únicos enlaces conectados a un Nodo Principal donde cada uno de los enlaces es atendido con medio de transmisión de fibra óptica desde POP distintos, revisar la Figura 4 para ver la topología y la Tabla 3 donde se detalla el equipamiento.

1 → Principal

2 → Secundario

TOPOLOGIA – AFILIADO TIPO I

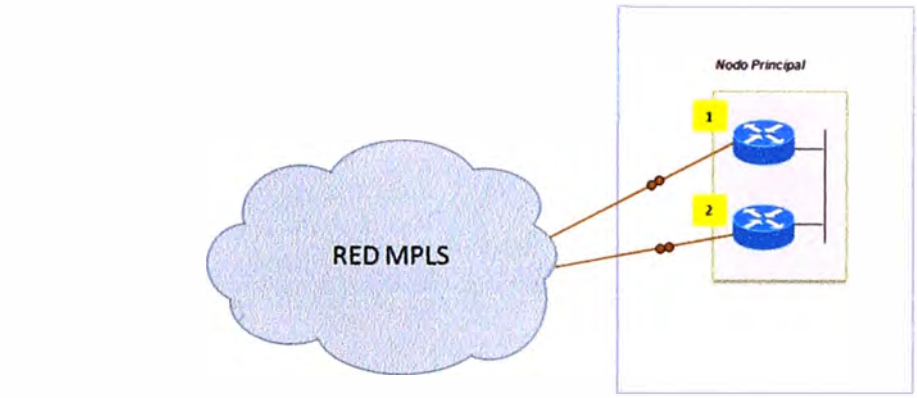

Figura 4. Topología de un Afiliado Tipo I de la Red de Bancos, Nodo Principal.

Tabla 3. Equipamiento de los Afiliados Tipo I

Descripción	Tipo	Equipo	Cantidad
Principal	Principal	Cisco 2801	1
Principal	Secundario	Cisco 2611	1

Afiliado Tipo II:

La topología para un Afiliado no es redundante, cuenta con un único enlace el cual se brinda con medio de transmisión fibra óptica, revisar la Figura 5. donde se explica la topología y la Tabla 4 donde se detalla el equipamiento.

1 → Principal

TOPOLOGIA – AFILIADO TIPO II

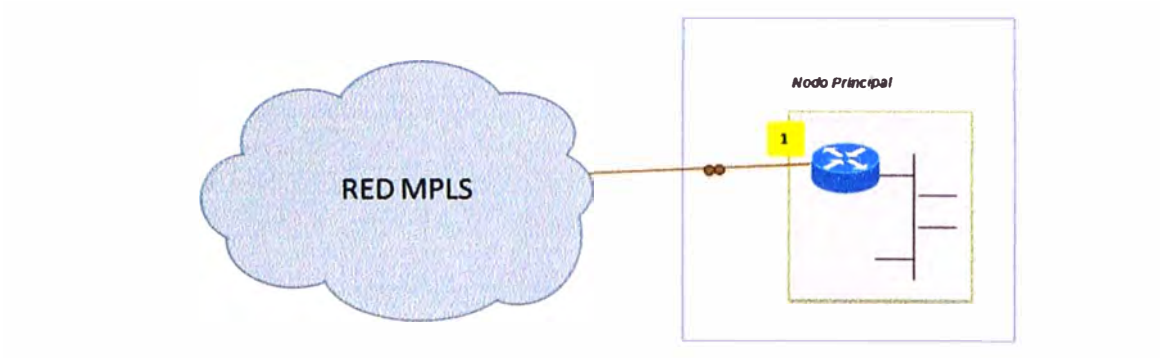

Figura 5. Topología de un Afiliado Tipo II de la Red de Bancos, Nodo Principal.

Tabla 4. Equipamiento de los Afiliados Tipo II

Descripción	Tipo	Equipo	Cant.
Principal	Principal	Cisco 2801	1

2.2.4 Resumen de la Topología:

La Red se encuentra conformada por los 3 tipos de topologías de acuerdo a lo expuesto anteriormente, como se explica el Nodo Principal cuenta con Routers ubicados de manera redundante denominados Nodo Central y Nodo Alterno, los cuales son encargados de entregar la ruta por defecto a toda la Red de Bancos.

Estos se encuentran ubicados San Isidro (Nodo Central) y en Villa el Salvador (Nodo Alterno) como se observa en la Figura 5.

La Red de Bancos cuenta con la siguiente cantidad de sedes:

- **Asociados** → 16 sucursales
- **Afiliados tipos I** → 9 sucursales
- **Afiliados tipo II** → 41 sucursales

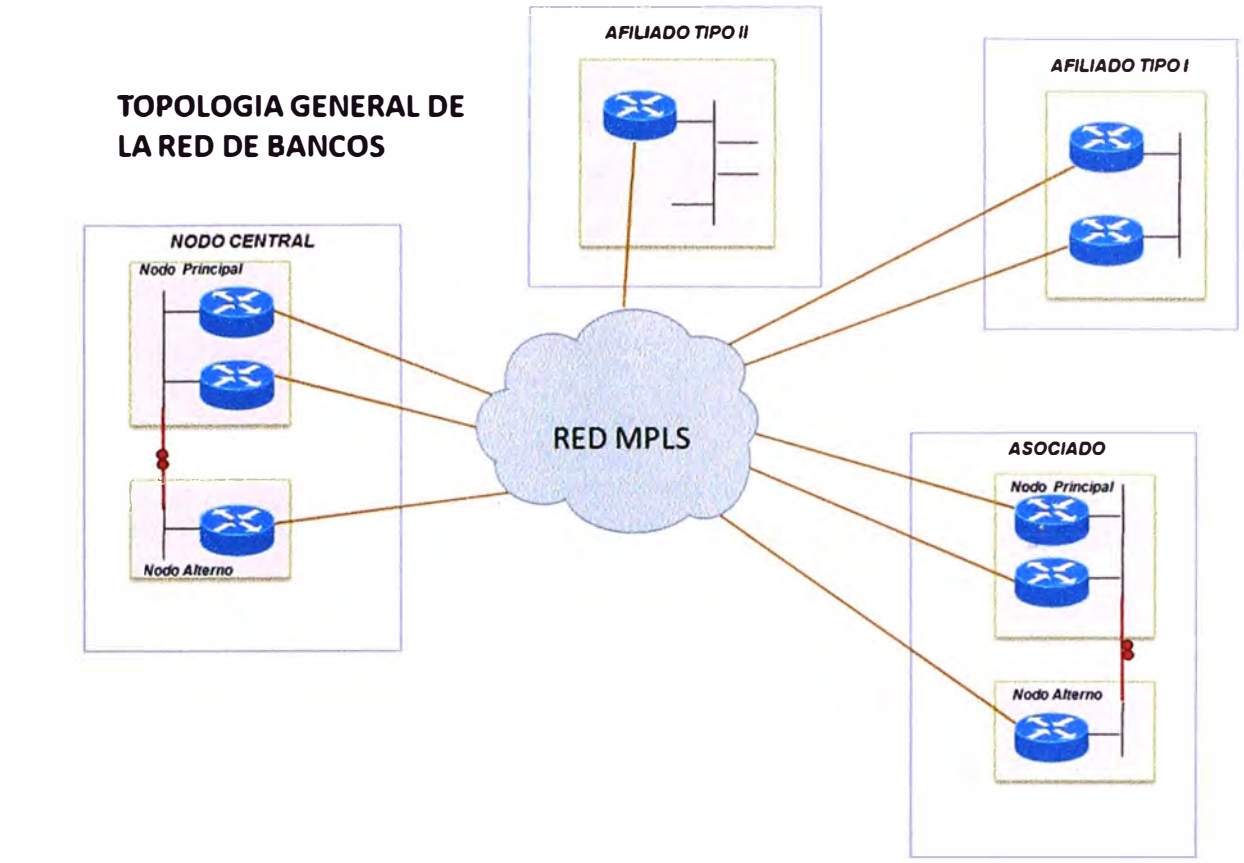

Figura 6. Topología general de la Red de Bancos.

2.3 Distribución de Anchos de Banda

Actualmente la Red de Bancos cuenta con los anchos de banda indicado en la siguiente Tabla 5 y distribuidos en 3 tipos de Calidades (A explicarse más adelante la descripción de CoS).

Tabla 5. Distribución de Anchos de Banda.

	CoS 3	CoS 2	CoS 1
Tipos de Datos	Voz y Video sobre IP	Datos críticos IP	Datos IP No Críticos
Prioridad	Máxima	Media	Normal
Ancho de Banda de Acceso	Mínimo la sumatoria del Ancho de Banda de cada CoS		
Aplicaciones	Apps en tiempo real como VoIP, Video, Multimedia, etc.	Apps de datos sensibles al retardo y/o criticas como ERP, SNA, etc.	Apps de base de datos, transaccionale y trasferencia de correo, entre otros.

El ancho de banda por tipo de sede actualmente es como se menciona en las Tabla 6, Tabla 7, Tabla 8 y Tabla 9 para cada tipo de sede.

Nodo Central:

Tabla 6. Distribución de Ancho de Banda en el Nodo Central.

Descripción	Tipo	BW Total	Distribución de Ancho de Banda		
			CoS1	CoS2	CoS3
Principal	Principal	7Mbps	768Kbps	6Mbps	64Kbps
Principal	Secundario	7Mbps	768Kbps	6Mbps	64Kbps
Alterno	Alterno	7Mbps	768Kbps	6Mbps	64Kbps

Asociados:

Tabla 7. Distribución de Ancho de Banda en los Asociados.

Descripción	Tipo	BW Total	Distribución de Ancho de Banda		
			CoS1	CoS2	CoS3
Principal	Principal	4Mbps	384Kbps	3Mbps	128Kbps
Principal	Secundario	1Mbps	192Kbps	768Kbps	64Kbps
Alterno	Alterno	4Mbps	384Kbps	3Mbps	128Kbps

Afiliados Tipo I:

Tabla 8. Distribución de Ancho de Banda en los Afiliados Tipo I.

Descripción	Tipo	BW Total	Distribución de Ancho de Banda		
			CoS1	CoS2	CoS3
Principal	Principal	2Mbps	384Kbps	1.5Mbps	128Kbps
Principal	Secundario	512Kbps	128Kbps	256Kbps	32Kbps

Afiliados Tipo I:

Tabla 9. Distribución de Ancho de Banda en los Afiliados Tipo II.

Descripción	Tipo	BW Total	Distribución de Ancho de Banda		
			CoS1	CoS2	CoS3
Principal	Principal	256Kbps	32Kbps	192Kbps	64Kbps

2.4 Seguridad con conectividad VPN

La actual Red de Bancos utiliza como medida de seguridad conexiones VPN sobre MPLS (MPLS – VPN) entre todas las sedes principales, lo cual se pasa a detallar a continuación para así poder diferenciarlo con el protocolo GET VPN, que es el tema del presente informe.

2.5 MPLS – Virtual Private Networks.

Para comprender el uso de MPLS – VPN, tenemos que entender el concepto de la red MPLS.

2.5.1 MPLS (Multi-Protocol Label Switching)

"Es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI" (Wikipedia, 2013).

> *MPLS es una red privada IP que combina la flexibilidad de las comunicaciones punto a punto o Internet así como la fiabilidad y calidad de los servicios Prívate Line, Frame Relay o ATM.*
>
> *Ofrece niveles de rendimiento diferenciados y priorización del tráfico, así como aplicaciones de voz y multimedia. Y todo ello en una única red.*
>
> *MPLS (Multi-Protocol Label Switching) intenta conseguir las ventajas de ATM, pero sin sus inconvenientes*
>
> *Asigna a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los routers intermedios (solo se mira la etiqueta, no la dirección de destino)* (Hernandez, 2005).

Las principales aplicaciones de MPLS son:

- Funciones de ingeniería de tráfico (a los flujos de cada usuario se les asocia una etiqueta diferente)
- Servicios de VPN o MPLS – VPN
- Servicios que requieren QoS

2.5.2 ¿Cómo funcionan las etiquetas en MPLS?

"MPLS se basa en el etiquetado de los paquetes en base a criterios de prioridad y/o calidad (QoS). La idea de MPLS es realizar la conmutación de los paquetes o datagramas en función de las etiquetas añadidas entre la capa 2 y la capa 3. Por tanto MPLS es una tecnología que permite ofrecer QoS, independientemente de la red sobre la que se implemente" (Hernandez, 2005).

El etiquetado en capa 2, delante de la capa 3 es la base de la conmutación, ver Figura 7.

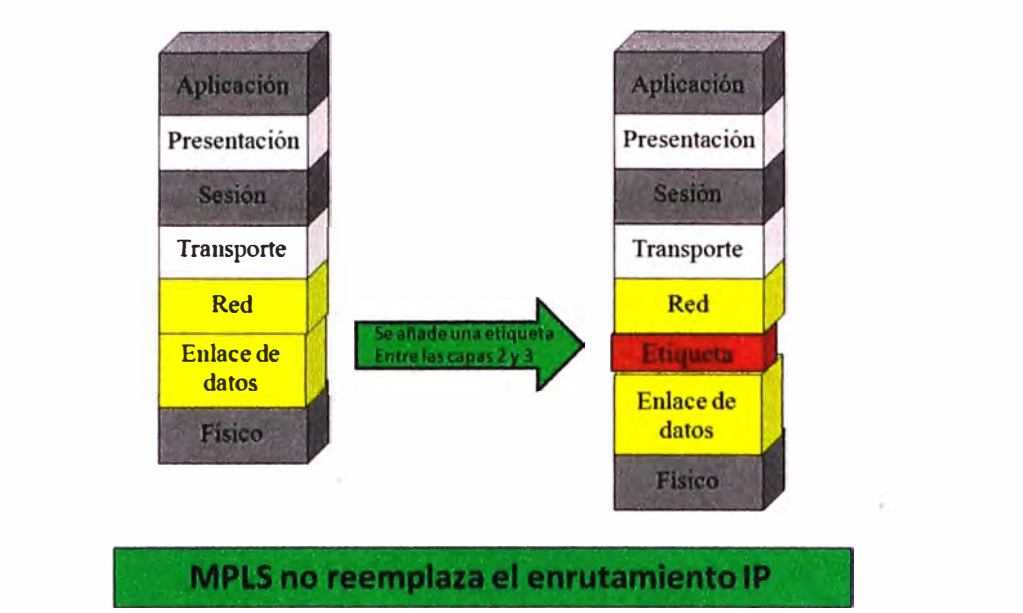

Figura 7. Se añade una etiqueta o "label" al paquete IP.

Esta etiqueta o "label" consta de 32 bits (4 campos) entre las cabeceras de las capas 2 y 3. A continuación se describe el formato de la etiqueta o cabecera MPLS, como muestra la Figura 7. Pero esta vez indicando la descripción de cada campo que forma parte de la etiqueta, ver Figura 8 y Figura 9.

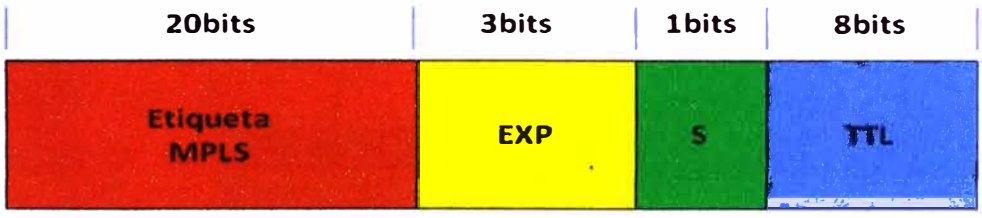

Figura 8. Formato de la etiqueta o cabecera MPLS

Campo Label ó Etiqueta.

- Campo de 20 bits. En este campo se coloca las etiquetas que serán conmutadas al momento de la transmisión de paquetes.
- Valores del 0 al 15 son reservados.

Campo EXP ó experimental.

- Campo de 3 bits. Indica CoS o Clase de servicio, para poder diferenciar el tráfico y dar prioridades.

Campo S ó Stack

- Campo de 1 bit. Indica un grupo ó stack de etiquetas.

Campo TTL ó Time-To-Live

- Campo de 8 bits. Elimina bucles en la región MPLS.

Figura 9. Descripción de los campos de la etiqueta MPLS

A continuación, se detalla como las etiquetas o "label" se colocan luego del paquete IP de capa 3, se muestra para cuando sea un paquete en IPv4 (Figura 10. Etiquetas MPLS sobre el paquete IPv4) e IPv6 (Figura 11. Etiquetas MPLS sobre el paquete IPv6).

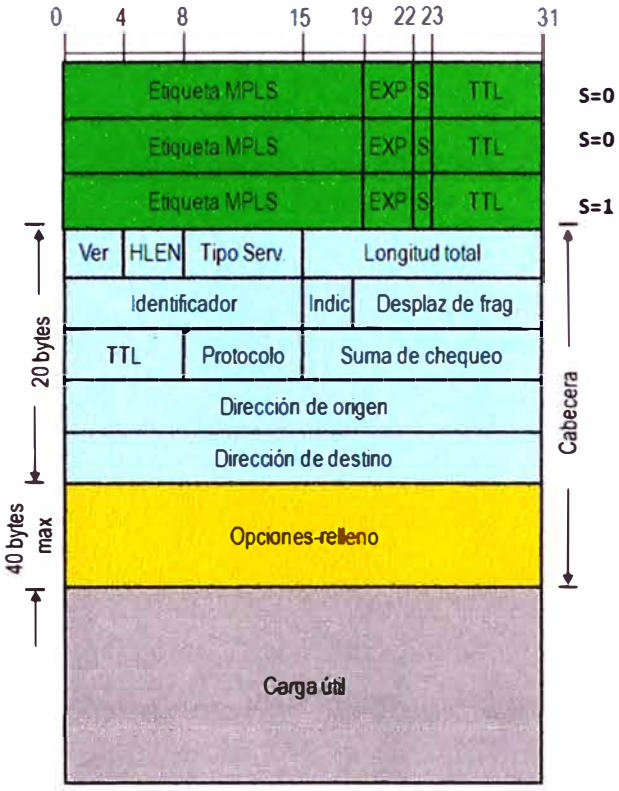

Figura 10. Etiquetas MPLS sobre el paquete IPv4.

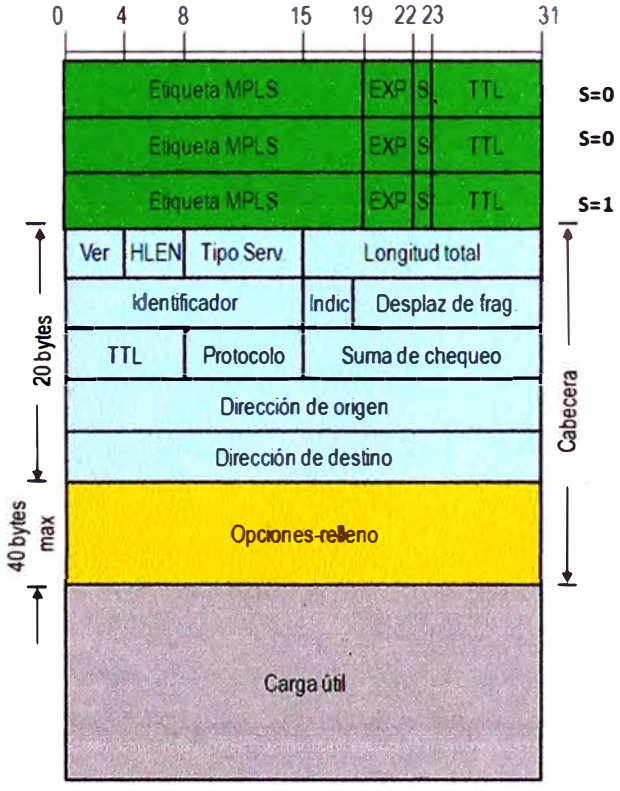

Figura 11. Etiquetas MPLS sobre el paquete IPv6.

2.6 ¿Y cómo se usa MPLS para el transporte de Información? Hablemos de MPLS – VPN.

"Para entender el funcionamiento de una red MPLS – VPN, es necesario conocer los términos P (router interno del proveedor), PE (router frontera del proveedor) y CE (router frontera de cliente que solicita el servicio). Se entiende como sitio a las intranets de los clientes que están separados físicamente pero lógicamente unidos vía una VPN, a través de un LSP" (Morales Dibildox, 2006, p.68).

A continuación la descripción completa del servicio en la Figura 12. Componente de una red MPLS – VPN.

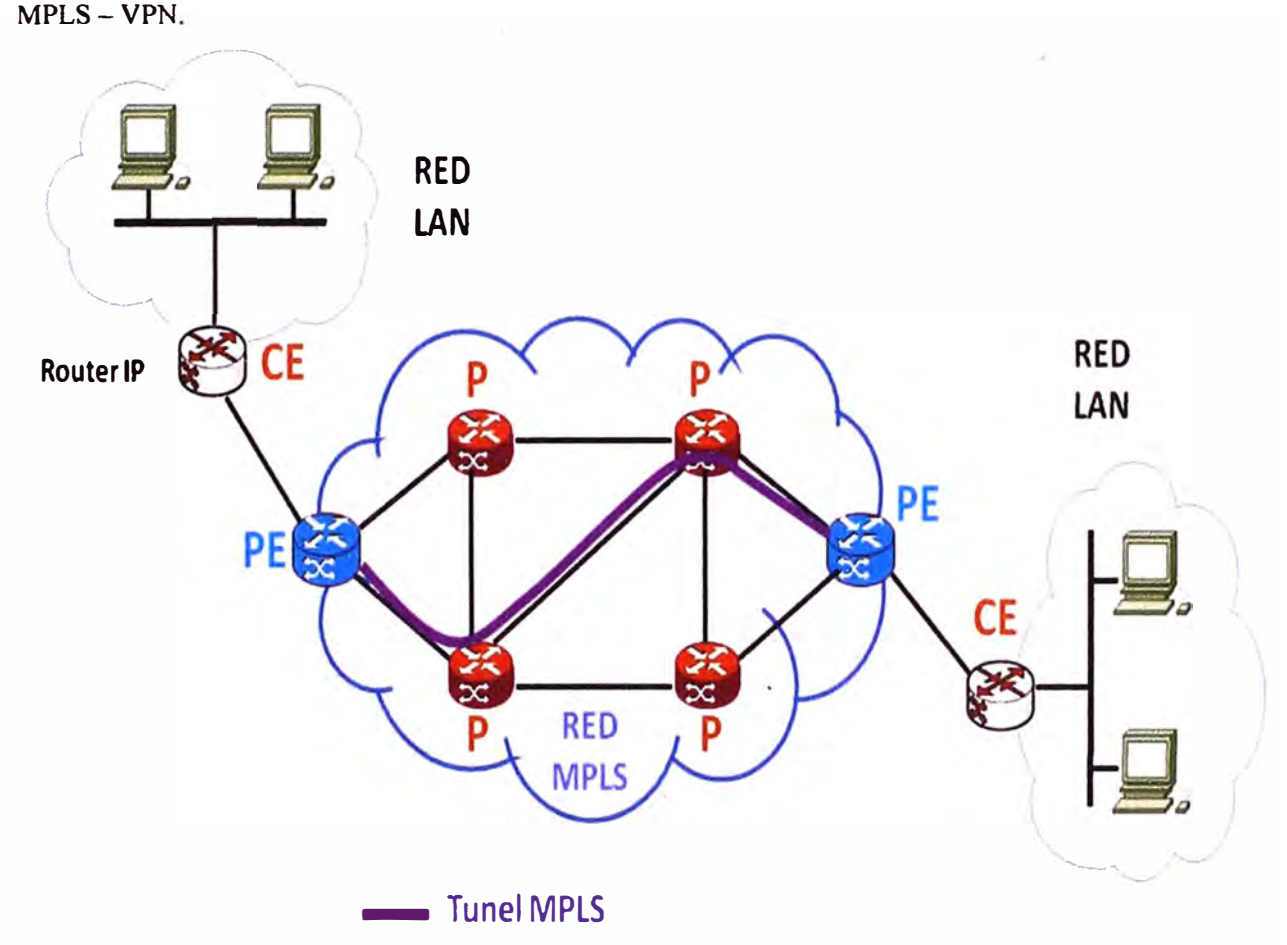

Figura 12. Componente de una red MPLS – VPN.

El reenvío de paquetes en una red VPN con tecnología MPLS se basa en la información de ruteo almacenada en las tablas de ruteo (incluyendo puertos).

Cada VPN está asociada con una o más instancias de Ruteo/Reenvío Virtual llamadas *VRF* (Virtual Routing and Forwarding). Una VRF determina la membresía que tiene el cliente conectado al router PE de la compañía proveedora de la Red MPLS.

Las VRF contienen las rutas disponibles en la VPN que pueden ser accesadas por los sitios de los clientes, cada sitio puede estar suscrito a varias VPN, pero solo a una VRF. Para

prevenir que no salga ni entre tráfico fuera de la VPN, cada VRF tiene guardada información de reenvío de paquetes, como se muestra en la siguiente Figura 13 (Morales Dibildox, 2006).

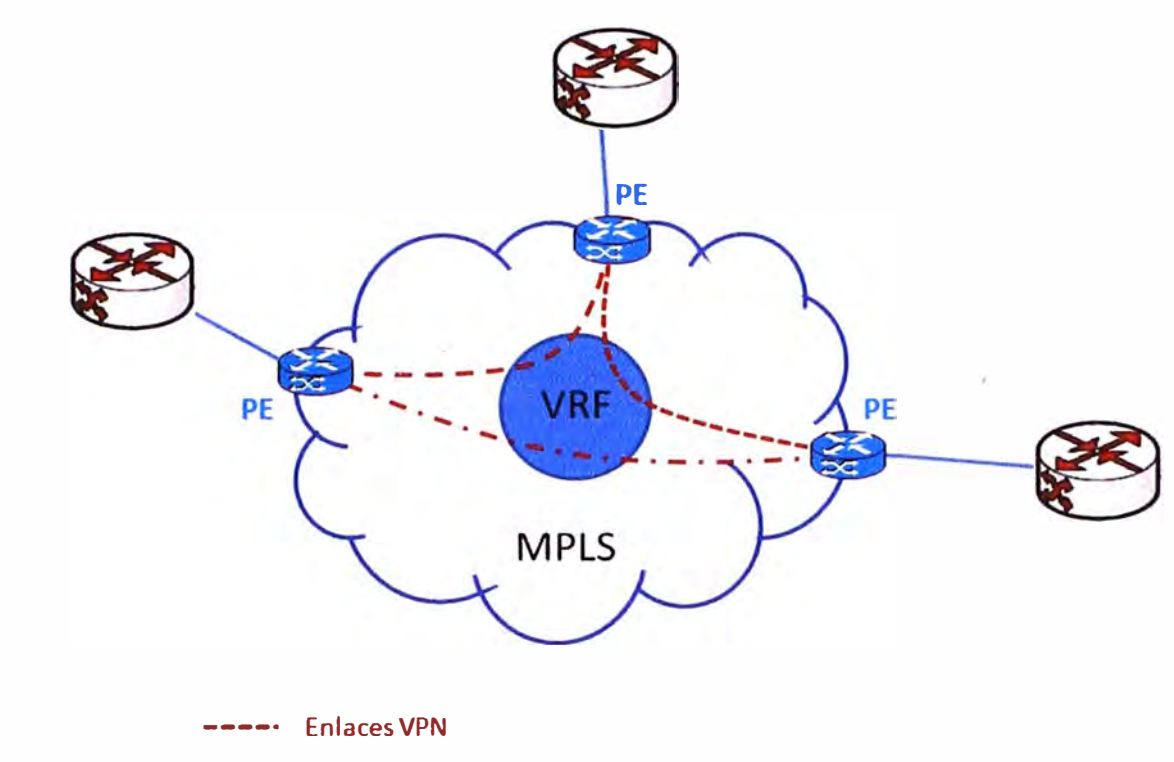

Figura 13. Diagrama de las rutas creadas en una VRF.

Gracias a esta arquitectura existen enlaces en malla (full-mesh) en cada sitio, a pesar de que cada sitio tiene un solo enlace a la nube del proveedor del servicio.

2.7 ¿Y cómo se realiza la conmutación de etiquetas?

Dibildox (2006) menciona que:

> *Los routers PE añaden una etiqueta a cada prefijo que obtienen de los routers CE, el prefijo incluye información de capacidad de alcance de los demás routers PE, es decir es un proceso de etiquetado.*
>
> 1. *Entra el paquete que proviene de un router CE al router PE, este le añade una etiqueta y lo envía.*
> 2. *Cuando el mensaje etiquetado llega al PE destino, este lee y quita la etiqueta para mandar el paquete al CE descrito en la etiqueta.*
>
> *El reenvío de etiquetas a través del eje troncal del proveedor se puede basar en conmutación dinámica de etiquetas o en Caminos de Ingeniería de Tráfico.*

En todo momento los paquetes que viajan por el backbone llevan dos etiquetas, la primera tiene la dirección del router PE (Que identifica a la VPN) y la segunda indica cómo el router PE debe de reenviar el paquete al router CE (Indica cual será el LSP a tomar). Cuando el router PE recibe el paquete, lo que hace es leer la etiqueta, quitarla y reenviarla al destino marcado en la segunda etiqueta. (p. 71)

Lo indicado anteriormente se explica gráficamente en la siguiente Figura 14:

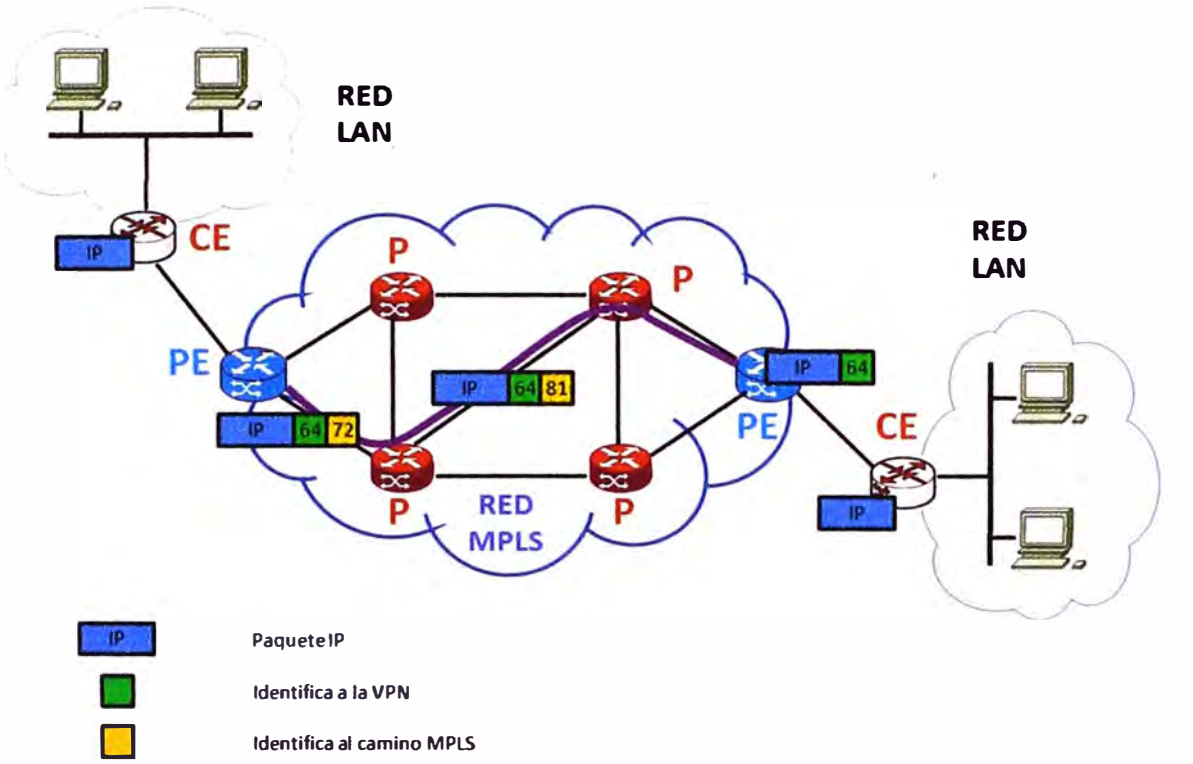

Figura 14. La conmutación de paquetes en la red MPLS – VPN.

Es de esta manera cómo se logra el envío de paquetes IP a través de la Red MPLS logrando una mayor flexibilidad con el uso de etiquetas, pues no se realiza el análisis de toda la cabecera del paquete IP.

Nuevamente, Dibildox (2006) nos refiere que:

> *Una de las principales ventajas técnicas de la MPLS – VPN es que no necesita conexión previa para establecer comunicación entre equipos, lo que facilita enormemente el tráfico entre dispositivos de red.*
>
> *"(...)"Gracias a que las MPLS – VPN residen entre la Capa 2 y la Capa 3 del modelo OSI (Nivel de Red) se pueden proveer servicios diferentes a distintos grupos de usuarios dentro de una VPN. Una VPN debe de proveer mecanismos*

efectivos para que los ISP puedan garantizar a sus clientes conexiones privadas a los servicios de sus intranets, ver Figura 15 (p. 73).

Consideraciones de una red MPLS:

Multiprotocolo Border Gateway Protocol (BGP - MP) lleva la información de enrutamiento CE entre los PE.

Para la MPLS – VPN no se puede garantizar la seguridad cuando el ataque sea lógico o físico desde la red del cliente o desde la misma red del proveedor, es decir desde los equipos backbone.

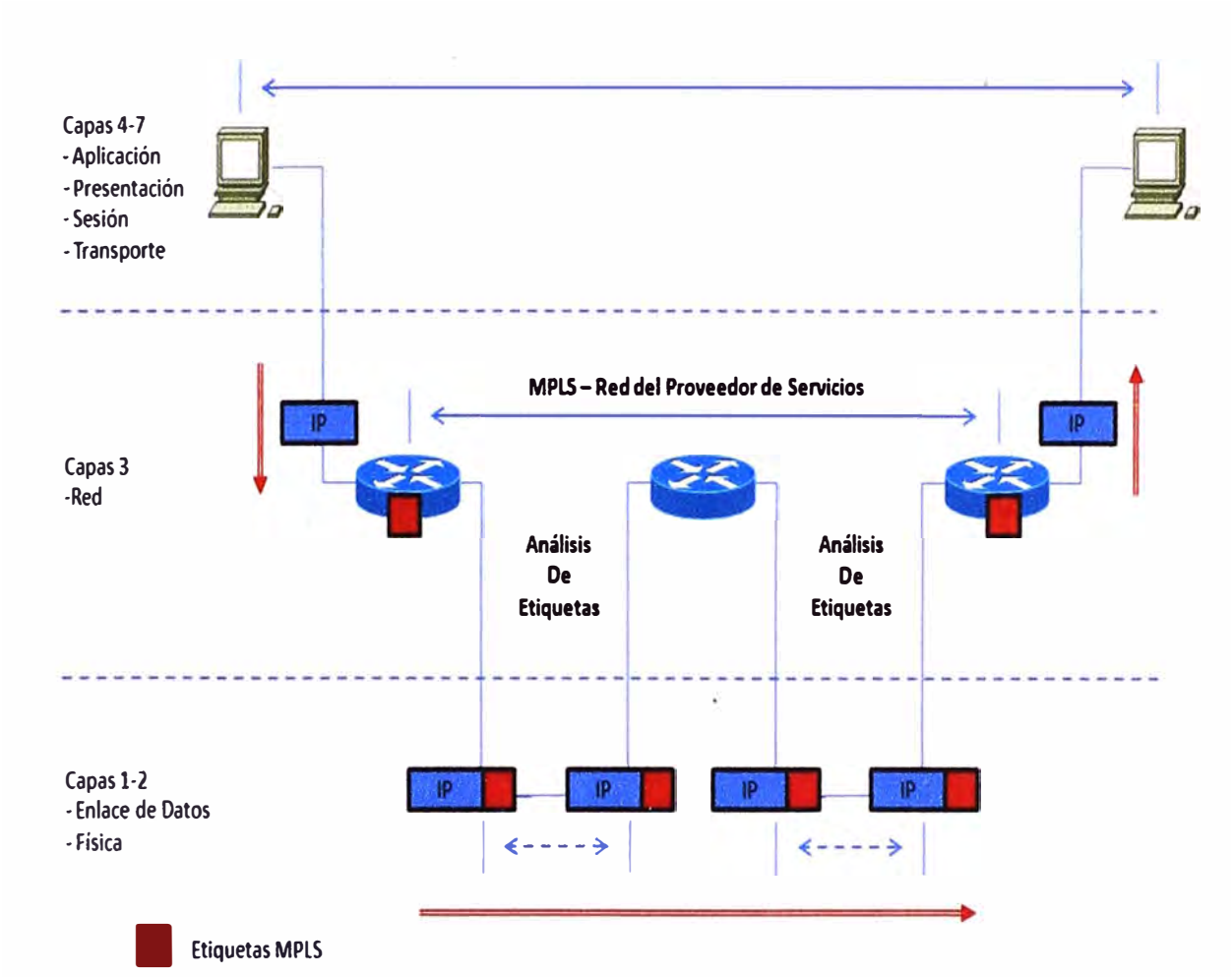

Figura 15. Las etiquetas MPLS residen entre la capa 2 y 3 del modelo OSI.
Fuente: Cisco Systems, 2004.

2.8 Seguridad en la red MPLS – VPN

Como menciona Dibildox (2006):

La MPLS – VPN ofrece la misma seguridad que las VPN orientadas a conexión, se garantiza la seguridad de que ningún paquete saldrá o entrará de las rutas permitidas. Es decir, sí existen varias VPN's que comparten los mismos medios

físicos o lógicos pero no llevan el mismo tipo de tráfico y/o son de diferentes clientes y nunca se invadirán.

Se garantiza que los paquetes del cliente recibidos en la frontera de la red del proveedor siempre serán enviados a la VPN correspondiente y que en el backbone el tráfico de cada VPN viaja aislado de los demás.

Si un intruso tratara de entrar ilegalmente (suplantación de identidad) a un router PE para ver los paquetes de información que envían los clientes, no podría realizarlo ya que los paquetes IP van dirigidos a interfaces o sub-interfaces en los PE que a su vez están asignados a diferentes VPN por lo que es casi imposible que tenga éxito (p. 75).

2.9 Alta disponibilidad o Redundancia en MPLS

"La alta disponibilidad en MPLS se brinda con el uso del protocolo BGP en la WAN, es decir se realiza el cambio de la tabla de ruteo usando el protocolo BGP" (Wikipedia, 2013). BGP intercambia información de encaminamiento entre sistemas autónomos a la vez que garantiza una elección de rutas libres de bucles. Es el protocolo principal de publicación de rutas utilizado por las compañías más importantes de ISP en Internet.

Un **Sistema Autónomo** (en inglés, *Autonomous System*: **AS)** se define como "un grupo de redes IP que poseen una política de rutas propia e independiente".

La ingeniería de tráfico en BGP es el modo en que se gestiona la red a partir de los atributos con los que cuenta dicho protocolo para satisfacer determinadas características o imposiciones de un escenario BGP.

Se definen características para el tráfico saliente y para el entrante, siendo este último algo más difícil de controlar. De modo que esta gestión de la red se hace a partir de la selección de las rutas que cualquier router va a propagar en una red y de las rutas que va a escoger como preferentes y alternativas.

Para ello se cuenta con un conjunto de atributos que dan información para la toma de decisión para filtrar o seleccionar rutas (Wikipedia, 2013).

Para el caso de configurar los enlaces en la Red de Bancos, se aprovecha el atributo llamado LOCAL-PREFERENCE y de esta manera poder dar prioridad a uno de los enlaces que llegan a la sede del cliente (Activo – Back up).

2.9.1 LOCAL-PREF

> *Este atributo es útil en un escenario en el que un sistema autónomo tiene conectividad con múltiples sistemas autónomos, de manera que pueda haber múltiples rutas hacia un mismo destino.*
>
> *Este atributo dará preferencia al envío de tráfico por un enlace en concreto, por tanto solo tendrá sentido dentro de un mismo sistema autónomo, luego solo se transmite por IBGP. Se escogerá el envío de datos por el enlace que tenga un LOCAL-PREF más alto, siendo el LOCAL-PREF por defecto de valor 100* (Wikipedia, 2013).

En este caso se podría, por ejemplo, colocar al enlace de contingencia un LOCAL-PREF de 50 (Back up), ver Figura 16.

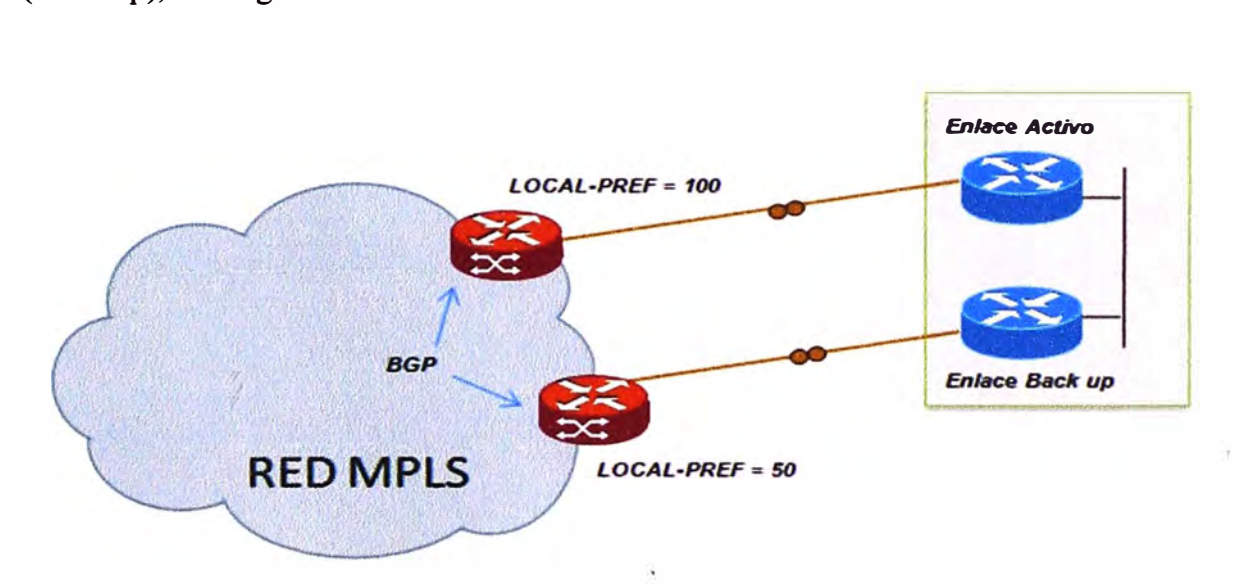

Figura 16. Ejemplo del LOCAL-PREF con el protocolo BGP (Activo – Back Up).

2.10 Soporte de CoS o Clase de Servicio en la red MPLS – VPN

Dibildox (2006), en su Tesis, nos menciona que:

> *Todo tráfico que va a entrar por las fronteras de la MPLS – VPN es clasificado y etiquetado dependiendo de las políticas definidas por los suscriptores que fueron puestas en ejecución por el proveedor. Posteriormente el tráfico ya etiquetado es transportado a través del núcleo del proveedor, es así como el tráfico que viene entrando y el que está dentro del núcleo del proveedor puede ser clasificado en diversas clases* (p. 78).

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP (Véase Figura 17) para poder propagar la clase de servicio CoS en el correspondiente

LSP. De este modo, una red MPLS puede transportar distintas clases de tráfico. (Explicada la diferenciación de CoS en el capítulo II, Distribución de Ancho de Banda)

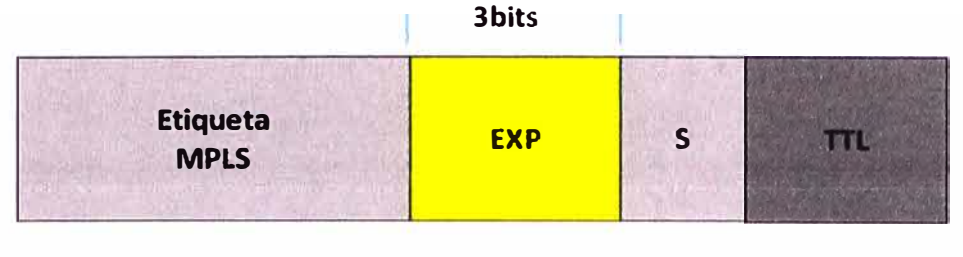

Figura 17. Uso del campo EXP para priorizar el tráfico en Clases de Servicio (CoS).

2.11 **Beneficios:**

Dibildox(2006), en su tesis menciona que:

> *Las cabeceras de la red MPLS – VPN están creadas en la capa 3 del modelo OSI por lo que no requieren de conexión, lo que las hace más fáciles de crear, manipular y son más escalables. Algunas de las características que ofrecen son:*
>
> - *Privacidad y seguridad, limitan la distribución de rutas VPN únicamente a los routers miembros a dicha comunidad VPN.*
> - *Integración transparente a las intranets de los clientes.*
> - *Escalabilidad mayor, miles de sitios por VPN y cientos de miles e inclusive millones de VPNs por cada proveedor de servicios.*
> - *CoS, que soportan diversas clases de servicios y prioridades dentro de la VPN y entre otras VPNs.*
> - *Escalabilidad de conexión a extranets e intranets extendidas que abarcan negocios múltiples* (p. 79).

Así mismo, todos los routers que soportan MPLS – VPN cuentan con los siguientes atributos:

- Interfaces dedicadas (lógicas o físicas)
- Tablas de ruteo dedicadas
- Reglas para la distribución de rutas VPN a lo enrutadores de puertos.

CAPÍTULO III
DISEÑO E INGENIERIA DEL PROTOCOLO GET VPN

En este capítulo se detallará el concepto del protocolo Group Encrypted Transport VPN (GET VPN) que es una un nuevo concepto de tecnología de encriptación WAN, que permite eliminar el divorcio actual entre la inteligencia de red y la privacidad de los datos.
Con la introducción de GET VPN, Cisco ofrece ahora una nueva categoría de Red Privada Virtual (VPN) que elimina la necesidad de túneles. Al eliminar la necesidad de crear VPN de punto a punto, una configuración de red WAN con muchas sedes remotas se mantiene altamente escalable y conserva la inteligencia de red que es crítica para la calidad de voz y video, enrutamiento y tráfico multicast. GET VPN, ofrece un nuevo estándar basado en modelo de seguridad IP (IPsec) que se basa en el concepto de los miembros de grupo "de confianza". Los miembros del grupo utilizan una metodología común de seguridad independiente de cualquier relación de VPN punto a punto IPSec.
GET VPN pueden utilizarse en una variedad de entornos WAN, incluyendo IP y Multiprotocol Label Switching. (Cisco Systems, 2013)
Las MPLS – VPN que utilizan esta tecnología de codificación son altamente escalables, administrables, rentables y cumplen con los requisitos reglamentarios exigidos por la encriptación. La naturaleza flexible de GET VPN permite a las empresas conscientes de su seguridad gestionar la seguridad a través de un proveedor de servicios WAN o manejar directamente la seguridad de la red WAN (Cisco Systems, 2013)
GET VPN simplifica el esquema para brindar seguridad a redes grandes de capa 2 o redes MPLS que requieren conectividad de malla completa o de malla parcial.

En el presente capítulo III se describirá las características del protocolo GET VPN, se explicara como al encriptar un paquete IP en una Red MPLS se logra asegurar que la información que pasa a través de los CE, se convierta en información ilegible ante cualquier intrusión.
Grupo Encrypted Transport VPN de Cisco (GET VPN) introduce el concepto de un grupo de confianza para eliminar los túneles punto a punto o los túneles en los enlaces VPN.

Todos los miembros del grupo (Group Member o GM) comparten una Asociación de Seguridad común (Security Association o SA), también conocido como un grupo SA. Esto permite a los GM's desencriptar el tráfico cifrado por cualquier otro GM. (Tenga en cuenta que en MPLS el CE actúa como un GM). En las redes GET VPN no hay necesidad de negociación de túneles entre los miembros de un grupo, porque GET VPN es un sistema sin túneles.

El estándar IETF RFC- 6407 Grupo Dominio de Interpretación (GDOI) es una parte integral de GET VPN (Cisco Systems, 2012)

3.1 GET VPN

Cisco Group Encrypted Transport Virtual Private Network (GET VPN) es un conjunto de características que son necesarias para proteger el tráfico de grupo multicast IP o el tráfico unicast sobre una WAN privada que se origina en o fluye a través de un dispositivo Cisco. GET VPN combina el protocolo de manipulación Group Domain of Interpretation (GDOI) con seguridad IP (IPsec) de encriptación para proporcionar a los usuarios un método eficaz para proteger el tráfico multicast IP o el tráfico unicast. GET VPN permite al router el poder aplicar el cifrado a no tunelizados (es decir, "nativo") multicast IP y paquetes unicast y elimina la necesidad de configurar túneles para proteger el tráfico multicast y unicast (Véase Figura 18) (Cisco Systems, 2013).

Figura 18. Asegurando la información Unicast y Multicast.

Fuente: Cisco Systems, 2013.

GET VPN es un modelo de seguridad basado en estándares que se basan en el concepto de los Group Members "de confianza". Los Routers miembros que son "de confianza" utilizan

una metodología de seguridad común, que es independiente de cualquier relación túnel IPsec de punto a punto. Además, redes cualquiera–cualquiera (any-any), mediante el uso de grupos de confianza en lugar de túneles punto a punto, se puede ampliar, manteniendo las características de la red de inteligencia más altos (como QoS, enrutamiento y multicast), que son fundamentales para la calidad de voz y video .

Redes basadas en GET VPN se pueden utilizar en una variedad de entornos WAN, incluyendo MPLS. Las redes MPLS – VPN que utilizan esta tecnología de cifrado son altamente escalables, manejables y rentables. La naturaleza flexible de GET VPN permite a las empresas preocupadas por la seguridad tanto para la gestión de su propia seguridad de red a través de un servicio WAN de servicios o de la red del Proveedor de Servicios.

3.2 **Descripción de la tecnología:**

La solución GET VPN se basa en estándares abiertos y tecnología innovadora de CISCO, así como patentada que ayuda a utilizar los beneficios de la red IP MPLS. Además de aprovechar la IKE (Internet Key Exchange) existente, IPsec y las tecnologías multicast, las soluciones GET VPN se basan en los siguientes conceptos básicos para proporcionar la funcionalidad requerida (Cisco Systems, 2012).

- GDOI (RFC 6407)
- Group Members (GM's)
- Key servers (KS's)
- Cooperative (COOP) KS's
- IP tunnel header preservation
- Group Security Association (SA)
- Rekey mechanism
- IPSec

3.3 **GDOI**

Domain Grupo de Interpretación o GDOI es un protocolo criptográfico para la gestión de claves de grupo. El protocolo GDOI se especifica en la Norma IETF RFC 3547 y se basa en la Asociación de Internet de Seguridad y Protocolo de administración de claves (ISAKMP), RFC 2408, e Internet Key Exchange versión 1 (IKE). Considerando que el IKE se ejecuta entre dos pares para establecer una "asociación de seguridad de pares", el protocolo de GDOI se ejecuta entre un miembro del grupo y un "grupo de controlador servidor de claves" (controlador) y establece una asociación de seguridad entre dos o más miembros del grupo, La topología se muestra en la Figura 19.

El ISAKMP define dos fases de la negociación. GDOI está protegido por una asociación de seguridad ISAKMP Fase 1. El intercambio de fase 2 está definido en IETF RFC 3547.

GDOI introduce dos claves de cifrado diferentes. Una clave asegura el plano de control GET VPN, la otra clave cifra el tráfico de datos. La clave que se utiliza para fijar el plano de control se conoce comúnmente como la Key Encryption Key (KEK) y la clave utilizada para cifrar el tráfico de datos se conoce como Traffic Encryption Key (TEK) (Cisco Systems, 2012).

3.4 GROUP MEMBERS (GMs)

El miembro del grupo se registra con el servidor de claves para obtener el SA que es necesario para comunicarse con el grupo. El miembro del grupo proporciona el ID de grupo al servidor de claves (Key Server) para obtener las respectivas políticas y llaves para este grupo. Estas claves se actualizan periódicamente y antes de que el actual SA expire, por lo que no hay pérdida de tráfico (Cisco Systems, 2012).

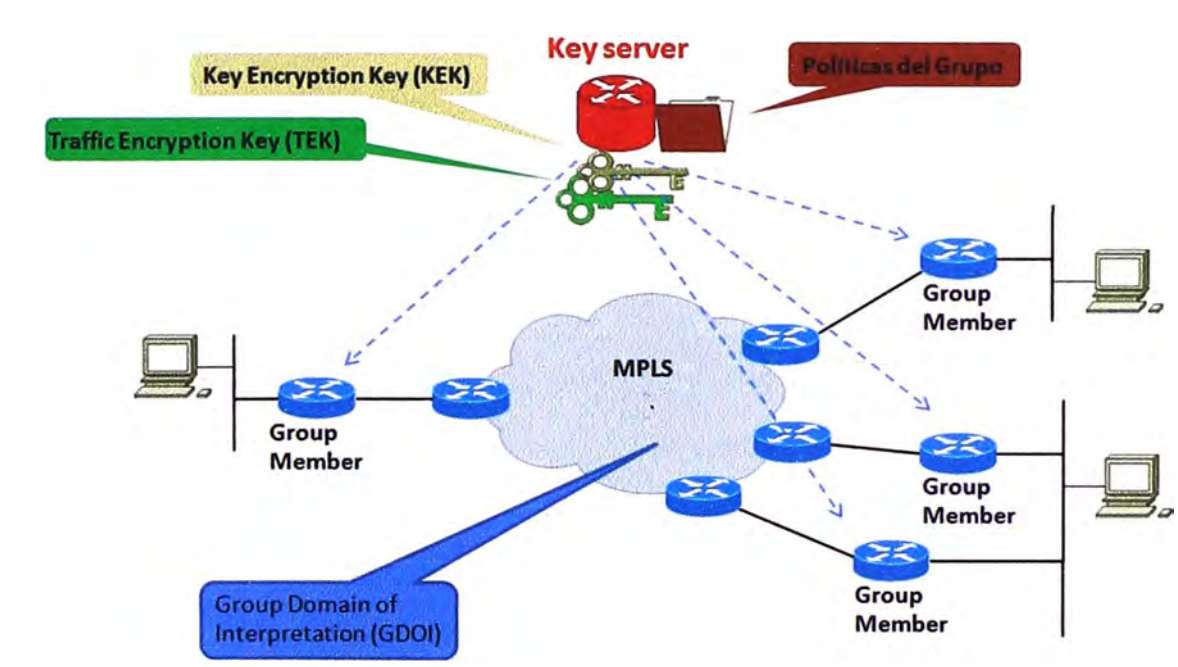

Figura 19. Algunos elementos del protocolo GET VPN.

Fuente: Cisco Systems, 2013.

3.5 KEY SERVER (KS's)

Las responsabilidades del Key Server (Servidor de Claves) incluyen el mantenimiento de las políticas, la creación y el mantenimiento de las claves para el grupo. Cuando un miembro del grupo se registra, el servidor de claves descarga esta política y las claves para

el miembro del grupo. El servidor de claves también regenera de claves del grupo antes de que las claves existentes expiren.

El servidor de claves tiene dos responsabilidades: las solicitudes de registro de nuevos usuarios y regeneración de claves. Un miembro del grupo puede registrarse en cualquier momento y recibir las políticas y las claves más actuales. Cuando un miembro del grupo se registra con el servidor de claves, el servidor de claves verifica el ID del grupo que el miembro del grupo está tratando de unirse. Si este ID es un identificador de grupo válido, el servidor envía la clave de la política de SA al miembro del grupo. Después de que el miembro del grupo reconoce que puede manejar la política descargada, el servidor de claves descarga las respectivas claves.

Hay dos tipos de claves que el Servidor de Claves se puede descargar: la clave de cifrado de clave (KEK) y la clave de cifrado del tráfico (TEK). La TEK se convierte en el SA con los que los miembros del grupo se comunican dentro del mismo grupo. La KEK encripta el mensaje de cambio de claves.

El servidor GDOI envía mensajes de cambio de claves si se produce una inminente expiración del SA o si la política ha cambiado en el servidor de claves (utilizando la interfaz de línea de comandos [CLI]). El cambio de claves también puede ocurrir si el temporizador KEK ha caducado, entonces el servidor envía una clave KEK para el cambio de claves. Los mensajes de cambio de claves también pueden ser retransmitidos periódicamente teniendo en cuenta que puede ocurrir una posible pérdida de paquetes. La pérdida de paquetes puede ocurrir porque los mensajes de cambio de claves se envían sin el uso de cualquier medio de transporte fiable. Si el mecanismo de cambio de claves es multicast, no hay ningún mecanismo de retroalimentación eficiente por el cual los receptores pueden indicar que no reciben un mensaje de cambio de claves, por lo cual se busca enviar actualizaciones permanentes a los receptores para tenerlos actualizados. Si el mecanismo de cambio de claves es unicast, los receptores enviarán un mensaje de confirmación (Cisco Systems, 2012).

La topología mostrada en la Figura 20 muestra el flujo de protocolos que son necesarios para que un Group Members pueda participar en un grupo, y son los siguientes:

1. Los miembros del grupo se registran con el servidor de claves. El servidor de claves autentica y autoriza a los miembros del grupo las descargas de la directiva IPsec y las claves necesarias para que puedan cifrar y descifrar los paquetes de multidifusión IP.

2. Según sea necesario, el servidor de claves "empuja" a un mensaje de cambio de claves de los miembros del grupo. El mensaje de cambio de claves contiene una nueva política y clave IPsec para utilizar cuando el viejo IPsec caduca. Los mensajes de cambio de claves se envían antes de la fecha de caducidad del SA para asegurar que las claves de grupo válido siempre están disponibles.
3. Los miembros del grupo son autenticados por el servidor de claves y se comunican con otros miembros del grupo autenticados que se encuentran en el mismo grupo con el SA que los miembros del grupo han recibido desde el servidor de claves.

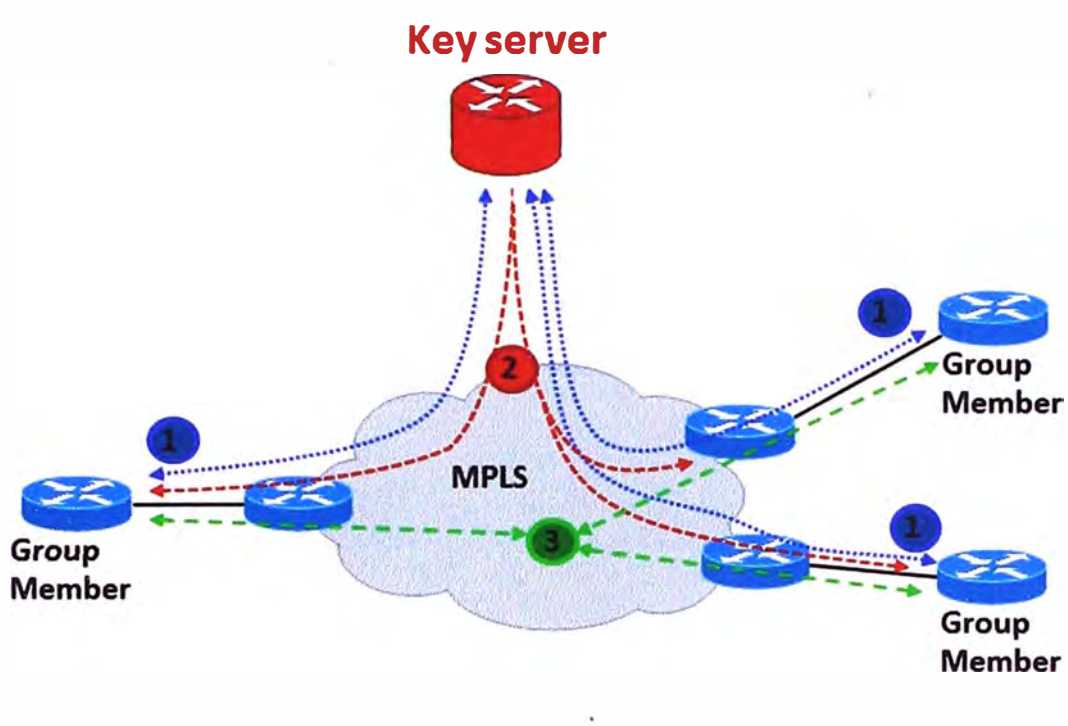

Figura 20. Flujo de protocolos para un Group Member.

Fuente: Cisco Systems, 2013.

3.6 Cooperative Key Servers (COOP KS's)

El KS es la entidad más importante en la red GET VPN porque el KS mantiene el plano de control. Por lo tanto, una sola KS es un único punto de error para toda una red GET VPN.

Debido a la redundancia es una consideración importante para KS's, GET VPN soporta múltiples KS's, esta funcionalidad se denomina Cooperative (COOP) KS's, para asegurar una recuperación sin problemas ni fallas si un KS falla o si se vuelve inaccesible.

Un GM se puede configurar para registrar a cualquier KS disponible de una lista de todos los COOP KS's. La configuración del GM determina el orden de registro. El KS definido como primario se pone en contacto primero, seguido por los KS definidos como secundarios, de acuerdo al orden que se haya asignado.

Cuando COOP KS's inicia, todo KS's asume un papel "secundario" y comienza un proceso de elección. Un KS, por lo general el que tiene la prioridad más alta, es elegido como KS "primario". Los otros KS's permanecen en el estado secundario. El KS primario es responsable de la creación de llaves y la distribución de configuraciones de políticas de grupos a todos los GM's, así como de sincronizar periódicamente el COOP KS'S (Cisco Systems, 2012).

3.6.1 *Proceso del KS Primario (véase* Figura 21)

- El Key Server genera una nueva "llave" en un periodo básico.
- El KS Primario revisa la consistencia de las Políticas y coordina a los Group Member con los KS Secundarios.
- El KS primario distribuye las "llaves" al KS Secundario y a los Group Members.
- El KS primario notifica a los secundarios la presencia de los KS Secundarios.

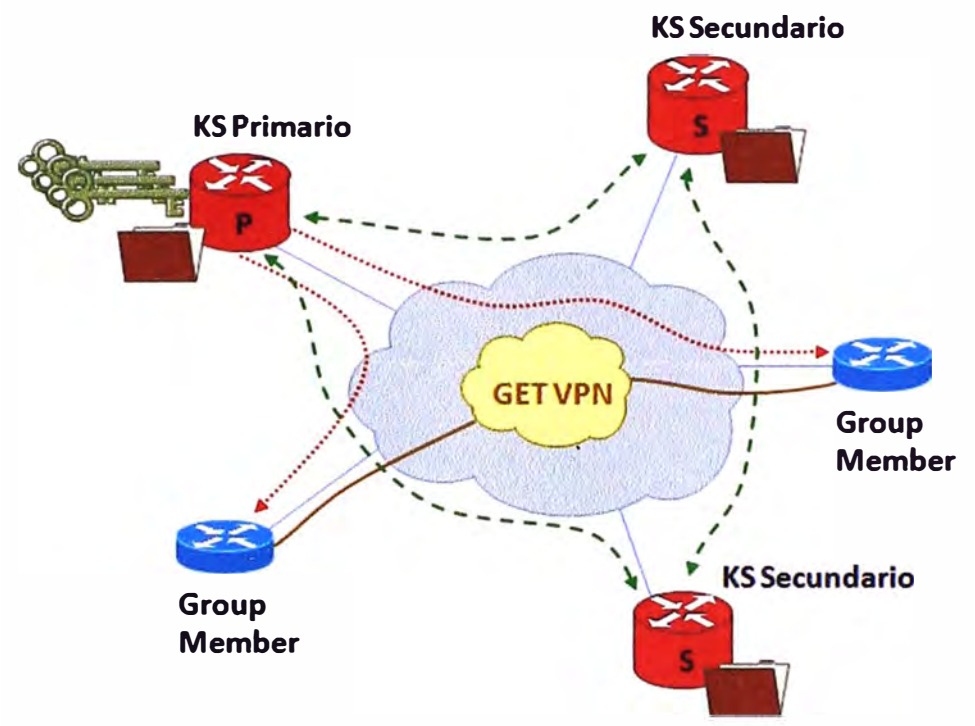

Figura 21. Procesos del KS Primario.

Fuente: Cisco Systems, 2013.

3.6.2 Proceso del KS secundario (véase Figura 22)

El Key Server Secundario revisa la consistencia de las políticas con el Key Server Primario.

El Key Server Secundario Autentica a los Group Members y actualiza la lista de Group Members con el KS primario.

El Key Server secundario provee las políticas y las llaves a los Group Members registrados.

El Key Server secundario monitorea la presencia del Key Server primario.

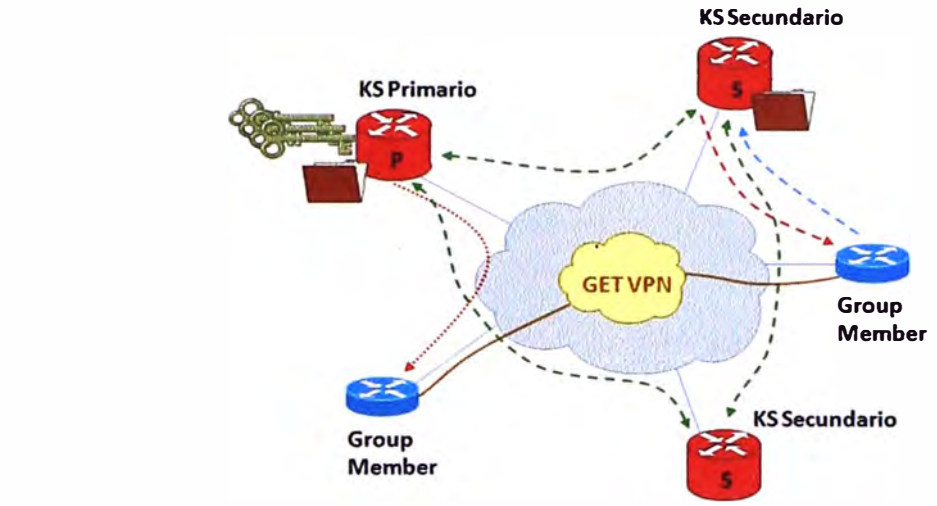

Figura 22. Procesos del KS Secundario.

Fuente: Cisco Systems, 2013.

3.6.3 Proceso de falla del Key Server primario (véase Figura 23*)*

Primer paso

- Perdida de la Base de Datos del Key Server primario
- Reinicio del Sistema
- Base de datos del GDOI borrada

Segundo paso

- Key Server secundario detecta la pérdida del Key Server primario.

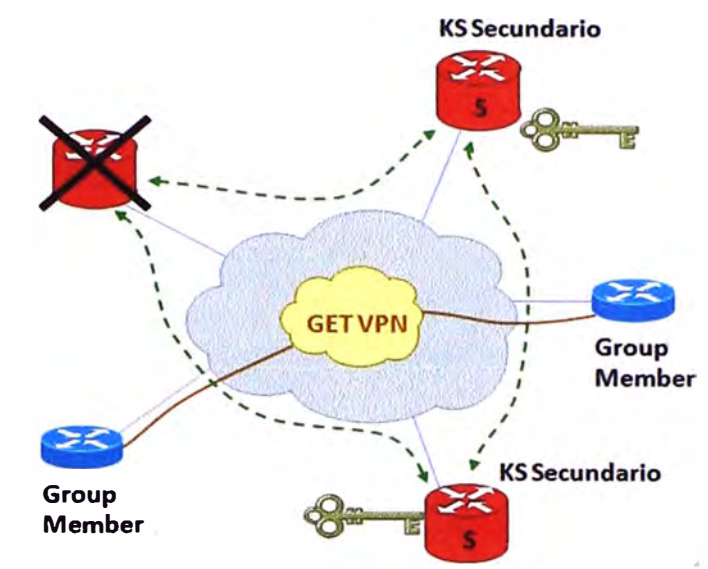

Figura 23. Escenarios de Falla del Key Server primario.

Fuente: Cisco Systems, 2013.

***Tercer paso (véase* Figura 24)**

Uno de los KS secundarios es elegido como KS primario.

El KS primario elegido gestionará las políticas, llaves y la lista del Group Member.

El KS primario elegido ahora será responsable de los mensajes de regeneración de llaves.

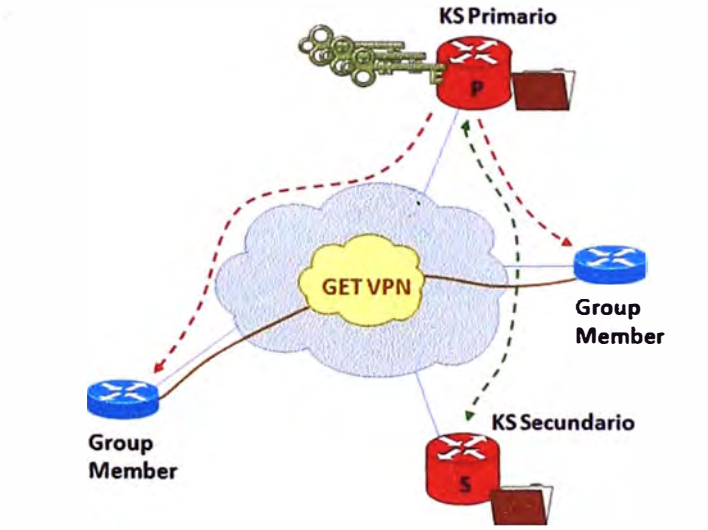

Figura 24. Elección de un nuevo Key Server primario.

Fuente: Cisco Systems, 2013.

3.7 IPSec (Internet Protocol Security)

Es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de

datos. IPSec crea túneles virtuales entre todas las sedes asociadas (Figura 25) e incluye también protocolos para el establecimiento de claves de cifrado (Figura 26).

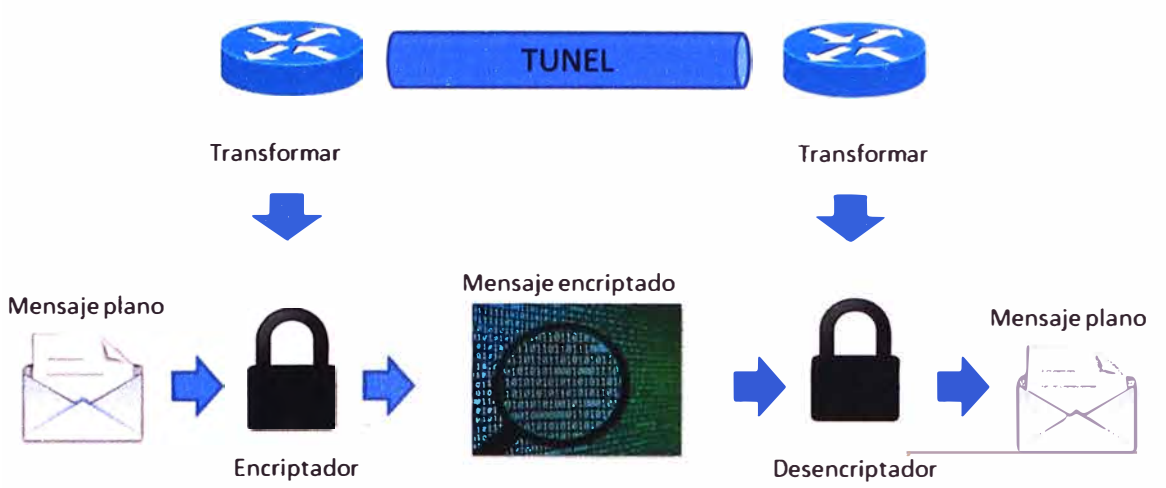

Figura 25. IPSec construye túneles virtuales, así como autentica y encripta la data útil.
Fuente: Cisco Systems, 2004.

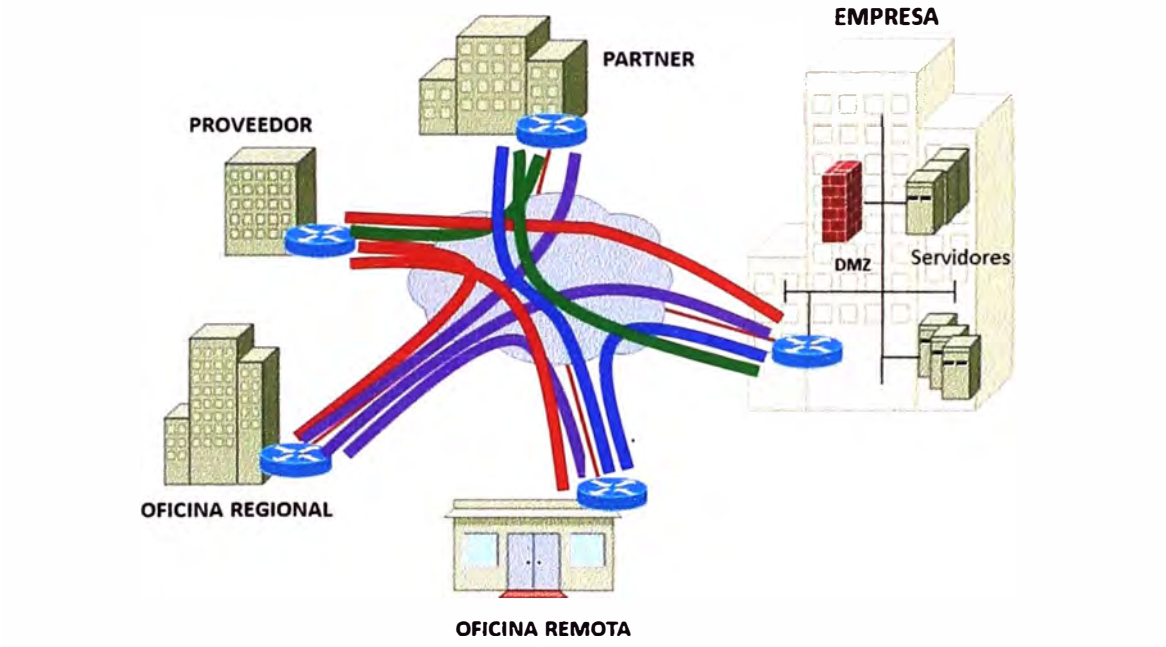

Figura 26. IPSec crea túneles virtuales por cada comunicación entre sedes.
Fuente: Cisco Systems, 2009.

IPsec consta de dos protocolos que han sido desarrollados para proporcionar seguridad a nivel de paquete, tanto para IPv4 como para IPv6:

3.7.1 Authentication Header (AH)

Proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados.

3.7.2 Encapsulating Security Payload (ESP)

Proporciona confidencialidad y la opción -altamente recomendable- de autenticación y protección de integridad. Este protocolo es reutilizado en GET VPN para poder encriptar la información útil, tal como se explicara más adelante.

3.8 IP tunnel header preservation

El modelo de seguridad de GET VPN usa la infraestructura de enrutamiento existente en vez de utilizar la tradicional superposición de IPSec. Los paquetes de datos mantienen las direcciones de red origen y destino preservando la cabecera de IP original en el paquete IP (Figura 27).

GET VPN permite confiar en la información existente de enrutamiento de capa 3, permitiendo así la capacidad de enfrentar las deficiencias de multicast y mejorar el rendimiento de red (Cisco Systems, 2012).

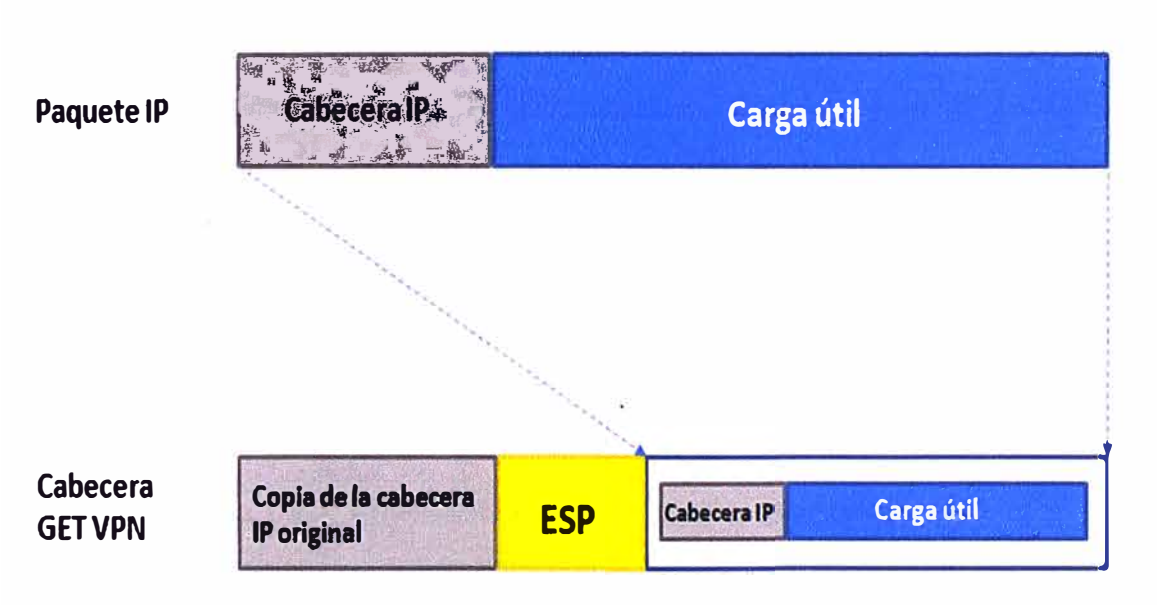

Figura 27. Conservación de la cabecera IP original en GET VPN.
Fuente: Cisco Systems, 2009.

3.9 Group Security Association (SA)

GET VPN utiliza el concepto de Group Security Assocation o agrupación de seguridad (SA). Todos los miembros del grupo de GET VPN pueden comunicarse entre sí usando una política de cifrado común y una SA compartida.

El concepto de asociación de seguridad (SA) como base para construir funciones de seguridad en IP. Una asociación de seguridad es simplemente el paquete de algoritmos y parámetros (tales como las claves) que se está usando para cifrar y autenticar un flujo

particular en una dirección. Por lo tanto, en el tráfico normal bidireccional, los flujos son asegurados por un par de asociaciones de seguridad. La decisión final de los algoritmos de cifrado y autenticación (de una lista definida) le corresponde al administrador Key Server (Cisco Systems, 2012).

Se resumen en lo siguiente:

- Todos los miembros del grupo comparten una SA.
- SA no es un miembro específico del grupo.
- SA es con un conjunto de los GM.

3.10 **Rekey Process**

Como se mencionó anteriormente, el KS no sólo es responsable de las políticas de encriptación y las llaves de cifrado, sino también para la regeneración de llaves y distribuirlos a los GM's. El proceso de envío de claves nuevas cuando las claves existentes están a punto de expirar, se conoce como el Rekey Process (proceso de regeneración de claves) (Cisco Systems, 2012).

3.11 **¿Y cómo se encripta usando el GET VPN?**

Al utilizar GET VPN, se logra encriptar la información considerando el IP Tunel Header Preservation, el cual con el uso de ESP se asocia a la información proveniente de los SA.

3.12 **ESP (Encapsulating Security Payload)**

Añadir encriptación al paquete IP con ESP hace que sea prácticamente imposible saber lo que dice, ya que la encapsulación sirve para dar soporte a la encriptación y a una autentificación de las cabeceras y campos.

Las RFCs de IPsec no insisten demasiado en un sistema particular de encriptación, pero normalmente se utiliza DES, triple-DES, AES o Blowfish para asegurar la carga útil de "ojos indiscretos". El algoritmo usado para una conexión en particular es definido por la Security Association (SA), y esta SA incluye no sólo el algoritmo, también la llave usada.

ESP rodea la carga útil con su protección. Los Security Parameters Index (SPI) y Sequence Number (SN), Payload Data, Padding (relleno), Pad Length y Next header son los campos del que conforman el encapsulamiento ESC, tal como se muestra en la Figura 28.

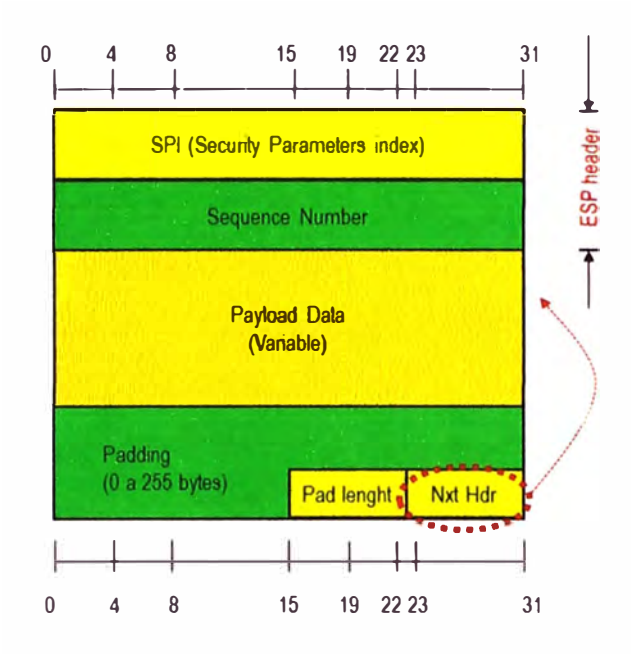

Figura 28. Estructura del encapsulamiento ESC.

Fuente: Friedl, 2004.

3.12.1 Security Parameters Index (SPI)

El SPI es un valor arbitrario de 32 bits que, en combinación con la dirección IP de destino y el protocolo de seguridad (ESP), identifica de forma exclusiva la Asociación de Seguridad para este datagrama. El conjunto de valores de SPI en el rango de 1 a 255 están reservados por la Internet Assigned Numbers Authority (IANA) para su uso futuro, un valor reservado SPI normalmente no será asignado por IANA a menos que se especifique el uso del valor de SPI asignado en un RFC. Esto normalmente es seleccionado por el sistema de destino al establecimiento de una SA. El campo SPI es obligatorio.

El valor de SPI de cero (0) se reserva para el uso local, específico de la implementación y NO DEBE ser enviada en la transmisión. Por ejemplo, una aplicación de gestión de claves puede usar el valor de SPI cero a significar "No existe asociación de seguridad" durante el período en que la implementación de ESP ha solicitado que su clave de entidad de gestión establezca una nueva SA, pero la SA aún no ha sido establecida (Friedl, 2004)

3.12.2 Sequence Number

Este campo de 32 bits contiene un valor de contador creciente (número de secuencia). Es obligatorio y siempre está presente, incluso si el receptor no opta por activar el servicio de anti-replay para una SA específica.

Este número es usado para prevenir ataques por repetición. El número está incluido en los datos encriptados, así que cualquier alteración será detectada (Friedl, 2004).

3.12.3 Payload Data o Carga útil

Los datos de "carga útil" es un campo de longitud variable que contiene los datos descritos por el campo "Next Header". El campo "carga útil" es obligatorio y es un número entero de bytes en longitud.

3.12.4 Padding (para Encriptación)

Varios factores requieren o motivan el uso de campo Padding o Relleno.

1. Si se emplea un algoritmo de encriptación que requiera el texto plano para ser un múltiplo de un número de bytes, por ejemplo, el tamaño de bloque de un sistema de cifrado de bloque, el campo de relleno se utiliza para llenar el texto plano (que consiste en los datos de los campos Payload Data, Pad Length y Next Header, así como el Padding) al tamaño requerido por el algoritmo.
2. El Padding también puede ser necesario, con independencia de los requisitos de algoritmo de cifrado, para asegurar que el texto cifrado resultante termine en un límite de 4 bytes. En concreto, los campos Pad Length y Next Header deben ser alineados a la derecha dentro de una palabra de 4 bytes, como se muestra en el formato de paquetes ESP figura anterior, para asegurar que el campo de datos de autenticación (si existe) está alineado en un límite de 4 bytes.
3. El Relleno, más allá de lo requerido por las razones del algoritmo o de alineación citados anteriormente, puede ser utilizado para ocultar la longitud real de la carga útil, en apoyo de la confidencialidad del flujo de tráfico. Sin embargo, la inclusión de dicho relleno adicional tiene implicaciones adversas de ancho de banda y por lo tanto su uso debe realizarse con cuidado.

El remitente puede agregar desde 0 a 255 bytes de relleno. La inclusión del campo Relleno en un paquete ESP es opcional, pero todas las implementaciones deben apoyar la generación y el uso de padding.

Con el fin de asegurar que los bits a cifrar son un múltiplo del tamaño de bloque del algoritmo (primer punto anterior), el cálculo de relleno se aplica al campo Payload Data e inclusive a los campos Pad Length y Next Header.

A los efectos de garantizar que los datos de autenticación está alineado en un límite de 4 bytes (segundo párrafo anterior), el cálculo de relleno se aplica al campo Payload Data e inclusive a los campos Pad Length y Next Header.

Si se necesitan bytes de relleno, pero el algoritmo de cifrado no especifica el contenido de relleno, se debe utilizar el siguiente proceso por defecto. Los bytes de relleno se inicializan

con una serie de valores enteros (sin signo, de 1 byte). El primer byte de relleno añadido al texto plano se numera 1, con posteriores bytes de relleno que componen una secuencia monótona creciente: 1, 2, 3, etc. Cuando se emplea este esquema de relleno, el receptor debe inspeccionar el campo Relleno. (Este esquema fue seleccionado debido a su relativa simplicidad, facilidad de implementación en hardware, y porque ofrece una protección limitada contra ciertas formas de ataques en ausencia de otras medidas de integridad) (Friedl, 2004).

3.12.5 Pad Length

El campo Pad Length indica el número de bytes inmediatamente anteriores a él. El intervalo de valores válidos es de 0-255, donde un valor de cero indica que no hay bytes de relleno presentes.

El campo Pad Length es obligatorio.

3.12.6 Next Header

El Next Header es un campo de 8 bits que identifica el tipo de datos contenidos en el campo de datos de carga útil, por ejemplo, una cabecera de extensión IPv6, TCP, UDP, etc., o un identificador de protocolo de capa superior. El valor de este campo es seleccionado entre el conjunto de Números de Protocolo IP definidos en la más reciente RFC de la Autoridad de Números Asignados de Internet (IANA). El campo Next Header de la cabecera es obligatoria.

Finalmente, una vez encriptado en IPSec el paquete IP quedara como se muestra en la Figura 29, que es justamente como ocurre en la encapsulación de GET VPN (Friedl, 2004).

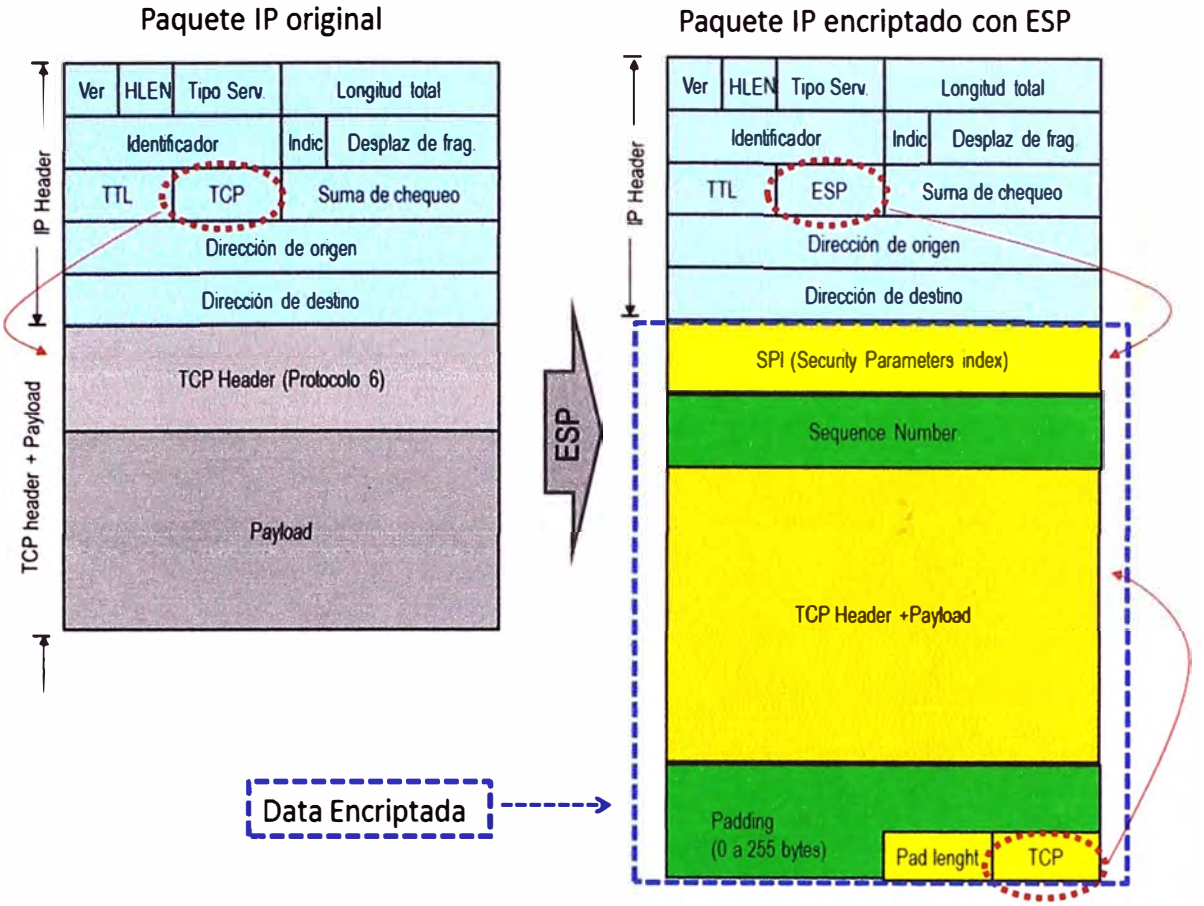

Figura 29. Paquete IP original vs Paquete IP encriptado con ESP tomando como ejemplo una cabecera TCP.

Fuente: Friedl, 2004

3.13 MPLS y GET VPN

Como se mencionó anteriormente, el protocolo GET VPN puede ser utilizado en una variedad de entornos WAN, de los cuales resalta MPLS, pues las redes MPLS – VPN que utilizan GET VPN permiten, además de contar con la encriptación, ser escalables, manejables y rentables.

GET VPN permite a las empresas que hacen de la seguridad su negocio, tener la confianza de la seguridad con la que cuenta su información a través del Proveedor de Servicios.

GET VPN utiliza la conmutación de etiquetas con las que realiza el transporte de la data, previamente encriptada por el Group Member, para así aprovechar la flexibilidad de MPLS al no tener que analizar toda la cabecera IP y manteniendo las clases de servicio (CoS) que nos brinda MPLS (Figura 30).

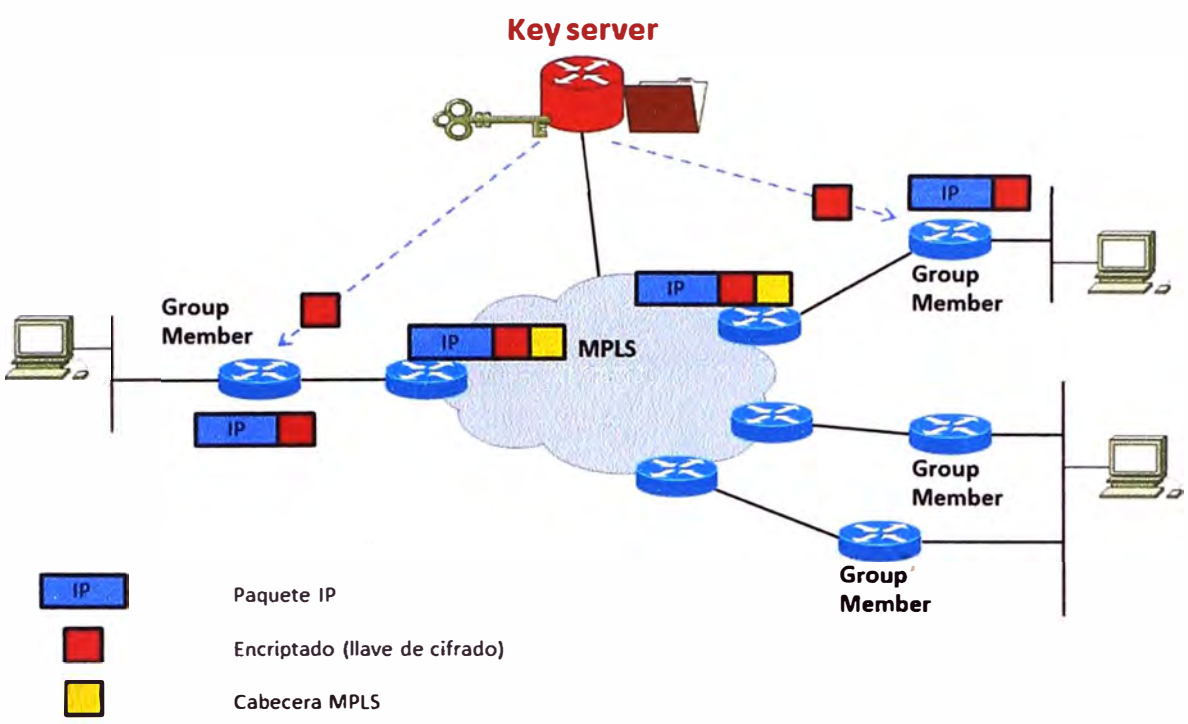

Figura 30. Escenario donde se utiliza GET VPN sobre MPLS.

3.14 Beneficios de GET VPN:

3.14.1 Encriptación de redes WAN privadas sobre MPLS

El incremento de los riesgos de seguridad y nuevas regulaciones han derivado en la necesidad de tener seguridad en el transporte WAN.

Las empresas que hoy en día manejan su propia infraestructura WAN o que utilizan el servicio de interconexión WAN de algún proveedor de servicios pueden emplear GET VPN para asegurar la privacidad de la data y al mismo tiempo mantener la conectividad de malla completa intrínseca de la red WAN.

De este modo, las organizaciones pueden alcanzar un equilibrio entre el control de la seguridad de sus negocios y los proveedores de servicios, manteniendo al mismo tiempo el cumplimiento de las normas de seguridad (Cisco Systems, 2009)

3.14.2 Seguridad de Cloud Computing

El cambio hacia un data center virtualizado y cloud-computing está creando requerimientos nuevos para brindar seguridad de la data en tránsito (Figura 31).

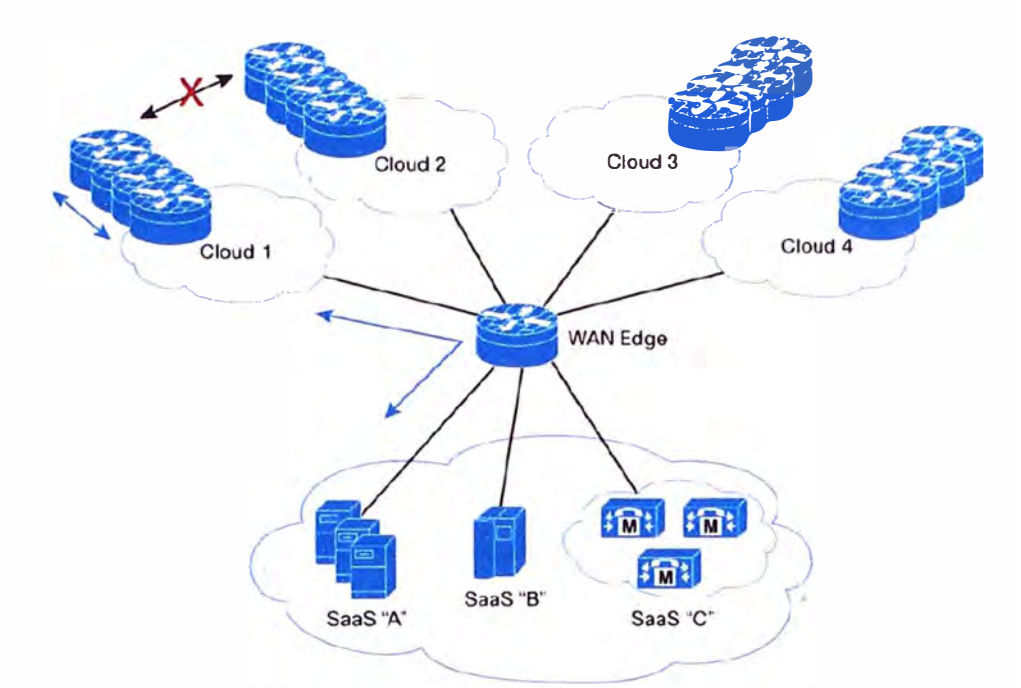

Figura 31. Ejemplos de seguridad en Cloud-Computing.
Fuente: Cisco Systems, 2009.

Por ejemplo, en la figura anterior:

- Cada Cloud representa un comunidad que debe t ener acceso selectivo a entornos "*software-as-a-service*" virtualizados en el data center. Los usuarios de Cloud 1 pueden acceder sólo a SaaS "A". los usuarios de Cloud 2 requieren acceso a SaaS A y C, etc.
- Todos los miembros en la nube están permitidos de comunicarse entre ellos.
- Cada Cloud representa a diferentes organizaciones y las comunicaciones inter-cloud deben ser denegadas. Por ejemplo cada Cloud puede representar a un departamento de una entidad de Gobierno accediendo a un data center compartido. O clientes empresariales - como un consorcio de bancos o clínica- accediendo a aplicaciones alojadas en el datacenter del proveedor de servicios.
- GET VPN puede ser utilizado para implementar estas aplicaciones. Las comunicaciones Inter-cloud pueden ser denegadas o permitidas según se necesite (Cisco Systems, 2009)

3.14.3 Administrando MPLS seguro.

GET VPN ha sido diseñando para añadir encriptación sin problemas en redes MPLS. Los proveedores de servicios están utilizando esto para ofrecer servicios de encriptación de

MPLS como valor agregado, manteniendo la inteligencia de red que es crítica para la voz, video, routing y multicast.

Las regulaciones de seguridad han sido quienes han impulsado estos servicios.

Los *Key Server* y la distribución de políticas de seguridad pueden permanecer bajo el control de la empresa o también ser administrados por el proveedor de servicios (Figura 32) (Cisco Systems, 2009).

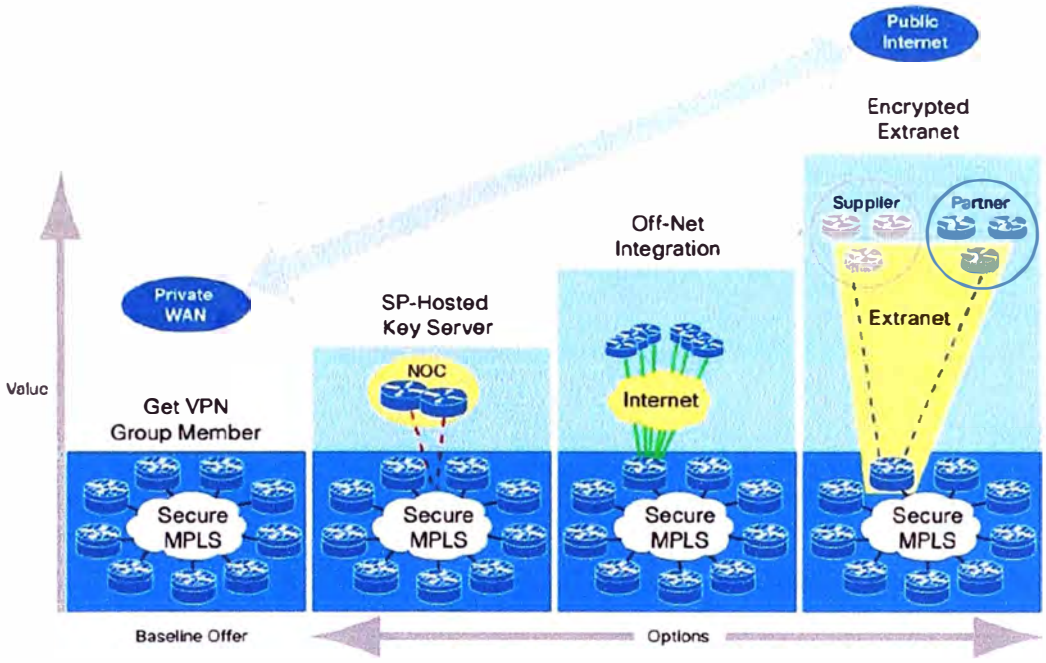

Figura 32. Administración de servicios de MPLS seguro.

Fuente: Cisco Systems, 2009.

CAPITULO IV
DISEÑO PROPUESTO

En el presente capitulo se detallará los modelos de router, con sus respectivos IOS, que soportan y nos permiten habilitar el protocolo GET VPN.

Se explicara el diseño a proponer en la Red de Bancos, incluyendo el cambio de equipos y se explicará la topología a brindar a la actual Red de Bancos y como funcionara el protocolo GET VPN una vez implementado sobre la red MPLS del proveedor de servicios.

4.1 Equipos que soportan GET VPN:

Como diseño se propone utilizar los equipos de la marca CISCO de la segunda generación y uno de la primera generación que soportan GET VPN, los cuales se pasa a detallar en la Tabla 10.

Tabla 10. Equipos que soportan GET VPN.

Función	Equipo
GET VPN Group Member	Cisco 870, 880, 890, 1900, 2900 y 3900 Series Integrated Series Routers
	Cisco ASR 1000 Series Router
GET VPN Key Server	Cisco 1900, 2900 y 3900 Series Integrated Series Routers

Fuente: Cisco Systems, 2009

4.2 Requerimientos de software para el protocolo GET VPN

Tabla 11. Requerimiento de Software.

Equipo	Licenciamiento	Versión recomendada
Cisco 1900, 2900 y 3900 Integrated Series Routers	Requiere "SEC Technology Package License"	Cisco IOS Software Release 15.0
Cisco ASR 1000 series Routers	Requeire "Advanced Enterprise Services or Advanced IP Services feature sets, along with VPN License".	Cisco IOS Software XE Release 2.3.2

Fuente: Cisco Systems, 2009

4.3 Anchos de banda recomendados:

Cisco nos brinda un valor de ancho de banda recomendable para cada tipo de equipo mencionado anteriormente, para obtener el máximo rendimiento, para los casos cuando sea un Group Member (Véase Tabla 12) o cuando sea un Key Server (Véase Tabla 13).

4.3.1 Group Member

Tabla 12. Equipos vs anchos de banda – Grupo Member.

Modelo	Ancho de Banda recomendado SEC – GET VPN
880	8 Mpbs o menor
890	10 Mpbs o menor
1921	15 Mpbs o menor
1941	25 Mpbs o menor
2901	25 Mpbs o menor
2911	35 Mpbs o menor
2921	45 Mpbs o menor
2951	55 Mpbs o menor
3925	75 Mpbs o menor
3925E	235 Mpbs o menor
3945E	335 Mpbs o menor
ASR 1001 Sin licencia	700 Mpbs o menor
ASR 1001 Con licencia	1.4 Gbps o menor

Fuente: Cisco Systems, 2009

4.3.2 Key Server

Tabla 13. Equipos vs Cantidad de Group Members – Key Server.

Modelo	Equipos Soportados
1921	Hasta 30
1941	Hasta 100
2921	Hasta 250
2951	Hasta 500
3925	Hasta 1000

Fuente: Cisco Systems, 2009

4.4 Propuesta a la Red de Bancos:

Se está proponiendo a la Red de Bancos del Perú colocar el equipamiento y anchos de banda, de acuerdo a la Tabla 14, Tabla 15 y Tabla 16, basándonos en las tablas recomendadas por Cisco para cada función que se cumpla dentro de la red GET VPN.

4.4.1 Equipamiento:

Nodo Central:

En el nodo Central se instalará los Key Server, los cuales, de acuerdo a la Tabla 13, en donde debemos tomar en cuenta la cantidad de routers con los que cuenta la Red de Bancos del Perú, que son en total 66 miembros (lo que significa 107 routers) por lo cual se recomienda el Cisco 2921 que soporta hasta 250 routers,

Tabla 14. Equipamiento propuesto en el Nodo Central.

Descripción	Distrito	Tipo	Equipo	Función	Cant.
Central	San Isidro	Principal	Cisco 2921	Key Server primario	1
Central	San Isidro	Secundario	Cisco 2921	Key Server Secundario	1
Alterno	Villa el Salvador	Alterno	Cisco 2921	Key Server Secundario	1

Asociados y Afiliados:

De acuerdo a la Tabla 12 y a la necesidad de contar con una red escalable en ancho de banda se considera equipamiento que soporten más del doble del actual ancho de banda, en este caso para todos los tipos de miembros se considerara routers CISCO 2901 que soportan hasta 25 Mbps.

Tabla 15. Equipamiento propuesto en los Asociados.

Descripción	Tipo	Equipo	Función	Cant.
Central	Principal	Cisco 2901	Group Member	1
Central	Secundario	Cisco 2901	Group Member	1
Alterno	Alterno	Cisco 2901	Group Member	1

Tabla 16. Equipamiento propuesto en los afiliados.

Descripción	Tipo	Equipo	Función	Cant.
Central	Principal	Cisco 2901	Group Member	1
Central	Secundario	Cisco 2901	Group Member	1

4.4.2 Anchos de Banda

El ancho de banda a considerar para la solución a brindar a la Red de Bancos del Perú, tal y como se encuentra actualmente constara de 3 Clases de Servicio y aclarando que el protocolo GET VPN es independiente del ancho de banda.

Nodo Central:

En el Nodo Central se encuentra los Key Server, encargados de la encriptación y de la llaves en la red GET VPN a implementar, por lo cual todos los routers de la Red de Bancos del Perú accederán a estos equipos, es así que como el CoS2 es dedicado para datos críticos y se considera brindarle un ancho de banda de 6Mbps dedicados, brindándole al CoS1 y CoS3 menores anchos de banda pues no los utiliza (véase Tabla 17), que en caso La Red de Bancos del Perú requiera modificarlos puede solicitarlo pues los equipos dimensionados (Tabla 14) fueron configurados para soportan mayores anchos de banda.

Tabla 17. Distribución de Anchos de Banda propuestos en el Nodo Central.

Descripción	Tipo	BW Total	Distribución de Ancho de Banda

			CoS1	CoS2	CoS3
Central	Principal	7Mbps	768Kbps	6Mbps	64Kbps
Central	Secundario	7Mbps	768Kbps	6Mbps	64Kbps
Alterno	Alterno	7Mbps	768Kbps	6Mbps	64Kbps

Asociados y Afiliados

Para los Asociados y Afiliados se deja la decisión a cada miembro de la Red de Bancos de acuerdo a su requerimiento de ancho de banda, el cual sin problema puede mantenerse de acuerdo a lo indicado anteriormente (véase Tabla 7, Tabla 8 y Tabla 9) y en caso el miembro requiera modificar el ancho de banda puede solicitarlo pues el equipamiento dimensionado (véase Tabla 15 y Tabla 16) soportaría anchos de banda mucho mayores.

4.5 Topología final a brindar en la sede del cliente:

Se mostrara en la Figura 33 el diseño final como se propone quedará la Red de Bancos y funcionará el GET VPN una vez implementado

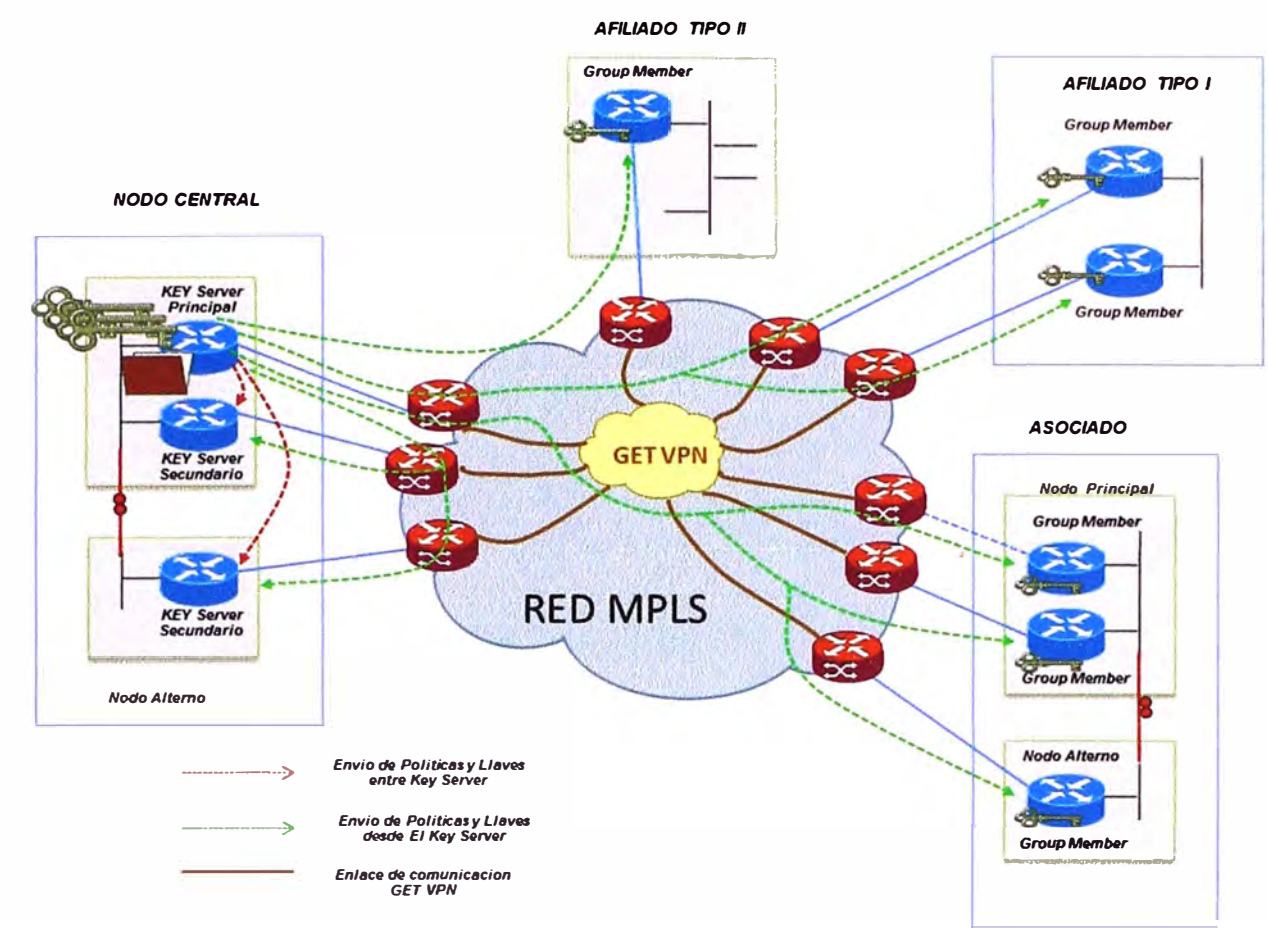

Figura 33. Topología final en el cliente Red de Bancos.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Se lograr encriptar la información usando el protocolo GET VPN y no se está modificando el funcionamiento de la red MPLS, se mantiene la configuración de Alta Disponibilidad de la red, por lo que no se ve afectada y seguirá siendo redundante (dos o una contingencia según sea el caso) tal y como se encuentra actualmente.
- Para conseguir la Alta disponibilidad con el protocolo GET VPN se continúa usando el protocolo BGP dando prioridad a quien tenga el LOCAL-PREF más alto.
- Al tener la cabecera GET VPN que mantiene la cabecera del paquete IP intacta, para la Red MPLS es como si no se estuviera utilizando el protocolo GET VPN, es decir es transparente para la red MPLS el uso del protocolo GET VPN, por lo cual no se tiene una "sobrecarga" del paquete IP al pasar por la red MPLS y cuando el paquete IP alcanza el CE este lo analiza como si se tratase de un paquete de una VPN estandar. En conclusión, el uso de GET VPN no produce una mayor "sobrecarga" al momento de analizar el paquete IP.
- Al mantener la cabecera IP, no se pierde las clases de servicio, es decir aún mantenemos las clases de servicio para diferenciar el tráfico en la red MPLS.
- Con GET VPN, al no necesitar túneles dedicados para la comunicación ya no es necesario el esquema Hub-and-Spoke y también nos permite tener una red any-to-any o full mesh sin un esquema punto a punto.
- GET VPN optimiza el proceso de replicación y encriptación de tal manera que se produce una vez por paquete en lugar de varias veces para cada destino como es común en tradicional túnel IPsec.
- Así mismo, permite escalabilidad en la red al permitirnos incluir sedes nuevas y la configuración sólo tendrá que hacerse en la Sede Principal, mas no en el resto de sedes pues el Key Manager será el encargado en enviar.

RECOMENDACIONES

- Como se menciona en la presente investigación, la Red MPLS cuenta con seguridad

que es inherente a la tecnología, pues al crear VRF's nos aseguramos que la información fluya punto a punto entre las sedes en los extremos, asignando hasta el puerto por el cual debe influir, por lo cual no es posible que alguien fuera de la Red del proveedor acceda a esta información.

- Pero, qué pasa si un intruso desde entro de la Red del proveedor, que tenga acceso al PE o al P, intente vulnerar la seguridad y robar información, podría lograrlo si tiene los permisos necesarios, es así que con GET VPN logramos encriptar este tráfico dentro de la Red del Proveedor de servicios y se vuelve ininteligible hacia el intruso.
- Antes de la instalación se debe tener en cuenta que la plataforma completa de routing quedara con la marca CISCO, pues es una marca reconocida a nivel mundial y especializado en Networking.
- Para mantener la alta disponibilidad, tal y como se encuentra en la **Figura 3.14** (Topología final en el cliente Red de Bancos), se recomienda el instalar 1 Key Server Principal y 2 Key Server Secundario.
- Se recomienda mantener, para cada tipo de integrante los tipos de Topología mencionados en la presente investigación, así se puede realizar un troubleshooting (revisión de problemas) con mayor facilidad.
- Se recomienda altamente el implementar GET VPN en todos los clientes, no solo de Banca o de Gobierno, sino también del sector privado como Universidades, Mineras, Petroleras, etc. Pues no solo brinda mayor escalabilidad, sino que se enfoca en lo más importante del presente informe, brindar una mayor seguridad a la información del cliente, además que se encuentra regulado por la NTP.

ANEXO A

GLOSARIO DE TERMINOS

Branch to branch—Usado en Telecomunicaciones para referirse a comunicaciones de extremo a extremo.

Hub-and-spoke—Referido a cuando un concentrador envia información a sedes remotas.

GET VPN—Cisco Group Encrypted Transport VPN, el cual define una nueva categoría de VPN, la cual no utiliza túneles.

VRF—La tecnología VRF (*Virtual Routing and Forwarding*) permite múltiples tablas de rutas separadas las cuales pueden coexistir en el mismo router y al mismo tiempo

MPLS— Multi Protocol Label Switching, Su capacidad para dar prioridad a los paquetes que transportan tráfico de voz hace que sea la solución perfecta para llevar las llamadas VoIP

QoS—*Quality of Service* O Calidad de Servicio, son las tecnologías que permiten aplicar un tratamiento específico a un determinado tipo de tráfico.

Full-mesh—Utilizado cuando se menciona que una red cuenta con una comunicación de todos contra todos, es decir, que no necesitan de un intermediario para poder comunicarse todas las sedes.

Backbone— La palabra *backbone* se refiere a las principales conexiones troncales de Internet o de la red del Proveedor

WAN—Son las siglas de **Wide Area Network**, red de área amplia, una red de ordenadores que abarca un área geográfica relativamente grande

GDOI—Group Domain of Interpretation, hace referencia a un medio de distribución y gestión de claves para los grupos de sistemas seguros.

Group Member—Dispositivo (Cisco IOS router) que se registra en un grupo que es controlado por el Key Server para los propósitos de la comunicación con otros miembros del grupo

Group Security Association—SA que es compartida por todos los Group Members en un grupo.

IPsec—IP security. Protocolo de cifrado de datos para los paquetes IP que se definen en la RFC (revisar IETF RFC 2401).

ISAKMP—Internet Security Association and Key Management Protocol. Protocolo que proporciona un marco para los protocolos de gestión de claves criptográficas.

KEK—key encryption key. Key usado para proteger la regeneración de Claves entre el Key Server y los Group Members.

Key server—Dispositivo (Cisco IOS router) que distribuye las claves y las políticas a un Group Members.

SA—Security Association. SA que es compartido a todos los Group Members in un grupo.

TEK—Traffic Encryption Key. Key que es usada para proteger la regeneración de claves entre los Group Members.

BIBLIOGRAFIA

Álvarez, J. C. (19 de Junio de 2013). Maximixe: La minería es el "motor" para desarrollar una economía diversificada. (D. GESTION, Entrevistador) Lima, Peru.

Cisco Systems, I. (2004). *CCNP Self-Study: Building Cisco Remote Access Networks (BCRAN), 2nd Edition.*

Cisco Systems, I. (2006). *Cisco Group Encrypted Transport VPN – Technical Overview.* Obtenido de http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/prod_presentation0900aecd8058203e.pdf

Cisco Systems, I. (2006). *Tunnel-less VPN with Cisco Group Encrypted Transport (GET).* Obtenido de http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/prod_presentation0900aecd80582031.pdf

Cisco Systems, I. (18 de Abril de 2008). *Cisco amplía su Red de Autodefensa con un sistema de seguridad integral.* Obtenido de http://www.cisco.com/web/ES/about/press/2008/cisco-noticias-08-04-17.html

Cisco Systems, I. (2009). *Cisco Group Encrypted Transport VPN: Tunnel-less VPN Delivering Encryption and Authentication for the WAN.* Obtenido de www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6635/ps7180/product_data_sheet0900aecd80582067.pdf

Cisco Systems, I. (Diciembre de 2012). *Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide.* Obtenido de http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6525/ps9370/ps7180/GETVPN_DIG_version_1_0_External.pdf

Cisco Systems, I. (2013). *Advanced IPSec with GET VPN.* Obtenido de http://www.menog.org/presentations/menog-2/nadhem-alfardan-get-vpn.pdf

Cisco Systems, I. (2013). *Cisco Group Encrypted Transport VPN*. Obtenido de http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_getvpn/configuration/xe-3s/sec-get-vpn.pdf

Cisco Systems, I. (2013). *Group Encrypted Transport VPN*. Obtenido de http://www.cisco.com/en/US/products/ps7180/index.html

Friedl, S. (24 de Agosto de 2004). *An Illustrated Guide to IPsec*. Obtenido de http://unixwiz.net/techtips/iguide-ipsec.html

Hernandez, J. (21 de Abril de 2005). *MPLS*. Obtenido de monografias.com: http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml

Morales Dibildox, L. (16 de mayo de 2006). Tesis profesional. *Investigación de Redes VPN con Tecnología MPLS*. Cholula, Puebla, Mexico.

S. Kent, & R. Atkinson. (Noviembre de 1998). *http://www.ietf.org/*. Obtenido de IP Encapsulating Security Payload (ESP): http://www.ietf.org/rfc/rfc2406.txt

Wikipedia. (31 de Octubre de 2013). Obtenido de "Multiprotocol Label Switching": http://es.wikipedia.org/wiki/Multiprotocol_Label_Switching

Wikipedia. (11 de Setiembre de 2013). Obtenido de Border Gateway Protocol: http://es.wikipedia.org/wiki/Border_Gateway_Protocol