UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO DE UNA RED IPVPN DEDICADA PARA UNA INSTITUCION GUBERNAMENTAL

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

VICTOR RAUL HUAYLLANI YLLATINCO

PROMOCIÓN
1999-I

LIMA – PERÚ
2013

DISEÑO DE UNA RED IPVPN DEDICADA PARA UNA INSTITUCION GUBERNAMENTAL

A mi familia
Por su apoyo incondicional para lograr
Alcanzar una meta más y seguir adelante.

SUMARIO

El presente trabajo está enfocado al diseño de una infraestructura de red para interconectar varias sedes a nivel nacional de una institución Gubernamental, todo dentro de una misma intranet.

El primer objetivo de este trabajo consiste en buscar el mejor diseño de infraestructura de red que permita garantizar la interconexión de las diversas sedes institucionales, de acuerdo a los requerimientos mínimos de la institución Gubernamental y que permita una transferencia segura y confiable.

El segundo objetivo es que el diseño de la infraestructura de red permita garantizar una velocidad de transmisión mínima para interconectar las sedes institucionales en una intranet, que permita compartir y/o consumir recursos entre cada sede, la transferencia de información institucional debe tener un nivel de seguridad y confiabilidad óptima.

En el análisis del diseño se observa que una infraestructura de red IPVPN-MPLS reúne las condiciones necesarias para interconectar las sedes institucionales a nivel nacional, posee un nivel de seguridad óptimo para la transferencia de información a través de la nube y da una conexión rápida entre la sedes.

ÍNDICE

INTRODUCCIÓN

En el presente informe presenta el diseño de una infraestructura de Red para interconectar las sedes de una institución Gubernamental, mejorar el rendimiento de la red y dar mayor seguridad a la información. Esto debido a que la actual infraestructura de red no cuenta con un medio de interconexión óptimo con las demás sedes, no brinda un rendimiento adecuado para los servicios web y cliente/servidor que van aumentando con el tiempo además de no garantizar un nivel de seguridad de la información transferida. Por lo que se plantea utilizar una infraestructura red robusta como IPVPN-MPLS, con el fin de crear una gran intranet entre las sedes institucionales y que una todas conexiones con un nivel de seguridad óptimo.

El informe se ha dividido en cuatro capítulos.

En el capítulo uno se plantea los objetivos, alcances y la problemática de ingeniería en donde se detalla la problemática de la infraestructura de red que posee la institución Gubernamental, una Infraestructura obsoleta que no brinda un rendimiento adecuado a los diversos servicios el mismo que genera incomodidad en los tiempos de respuesta al usuario final.

En el capítulo dos se expone los conceptos generales de tecnología de Redes Privadas Virtuales IPVPN MPLS, se presenta las tecnologías actuales que existen para transmisión de datos y finalmente se estudia los conceptos generales de calidad de servicio.

En el capítulo tres se presenta la metodología para la solución del problema, en esta parte se determinara cual es la tecnología más óptima que nos permita transmitir los diversos servicios en la institución Gubernamental.

En el capítulo cuatro se realiza un análisis de costos y presupuesto requeridos para la nueva infraestructura de red solicitado por la institución gubernamental y el tiempo de ejecución.

Finamente se presentan las conclusiones y recomendaciones del informe.

CAPITULO I
DEFINICION DEL PROBLEMA

La mayoría de instituciones públicas carecen de una infraestructura de red adecuada para los servicios que brinda, en los 90's se rediseño la infraestructura para las instituciones gubernamentales que fue óptimo para ese momento, en la actualidad incremento el número de servicios los servicios web y de aplicaciones cliente/servidor los niveles de servicios que eran locales pasaban a regional para luego convertirse a nivel nacional, y el incremente de nuevas sedes no planeadas son acopladas a la infraestructura de red y a esto implementar servicios de voz y datos en un mismo cable, esto género que el diseño de infraestructura de red de los 90's se degrade en su nivel de calidad de servicio, generando congestión, lentitud en los servicios y malestar con los usuarios finales. Se necesitaba un reordenamiento de la Infraestructura y buscar nuevas tecnologías para dar una óptima calidad servicio.

En este capítulo se expondrá los objetivos y alcance del presente informe, Finalmente se expone la problemática que presenta la actual Infraestructura de red dentro de la institución Gubernamental, el cual no garantiza la seguridad ni la calidad de los servicios.

1.1 Objetivo del trabajo

El objetivo del presente informe de suficiencia es formular una propuesta para implementar un medio de comunicación optimo, para lograr este objetivo se analizara los requerimientos para el transporte de información y las estadísticas de transferencia de voz y datos por sede (Tabla 1.1). Una vez definido estos requerimientos se procederá a analizar las diferentes tecnologías de comunicación que existen en la actualidad y finalmente escoger la tecnología que me mejor se adapte a los requerimientos.

Los objetivos específicos del presente informe se describen a continuación:

Definir el medio de comunicación óptimo que permita interconectar las sedes de una institución Gubernamental a nivel nacional.

Permitir a los usuarios finales tener una conectividad a la intranet y extranet por medio de la red de comunicaciones de voz y data para sus aplicaciones cliente/servidor y web con mejor rendimiento y un óptimo tiempo de respuesta.

Garantizar un mayor nivel de seguridad en la transferencia de información para los diversos servicios de voz y datos.

1.2 Alcance

Los alcances del presente informe se describen a continuación:

Primero: Análisis de por qué la infraestructura red actual no es la adecuada para cubrir los diversos servicios de voz y data en forma segura y rápida para las diversas aplicaciones en la intranet y extranet.

Segundo: Se determinara los requisitos exigidos de los servicios de intranet y extranet con el fin de evitar congestión o lentitud en los servicios prestados a los usuarios finales.

Tercero: La formulación de la propuesta para implementar servicios de comunicación óptima para la transferencia de voz y data; se refiere específicamente al análisis del porque las redes privadas virtuales son el medio de comunicación más óptimo que nos permita interconectar distintas sedes en forma regional y a nivel nacional.

Cuarto: La infraestructura de comunicación a implementarse para interconectar las diversas sedes institucionales tiene el objetivo de mejorar los servicios que consume el usuario final, el cual podrá acceder a toda información publicada en la intranet y realizar trámites y/o consultas sin problemas de lentitud o congestión.

1.3 Formulación del problema de ingeniería

La institución Gubernamental requiere una infraestructura de red que pueda unir sus sedes institucionales y cumpla como mínimo los siguientes requerimientos:

A. Las sedes deben estar interconectadas con un ancho de banda adecuado de acuerdo al nivel de información que maneje y la zona geográfica donde se ubique.

B. Las sedes podrán compartir recursos entre ellas, la información que comparte será de acuerdo al ancho de banda que se le asigne a la sede y cada sede deberá mantener su distribución de IPs y la estructura de su LAN de cada sede deberá mantenerse Intacta

C. Las sedes podrán consumir recursos de otras sedes por medio de web service o información pública que ellas requieran mostrar.

D. Todas las sedes deben estar en una misma Intranet, en el cual todas las sedes pueden comunicarse, como si fuera una gran nube gubernamental, esta Intranet debe estar aislada de otras redes externas y debe cumplir ciertas normas de seguridad.

E. Las sedes podrán consumir aplicaciones centralizadas de una sede hacia las otras, ya sea con aplicaciones cliente/servidor o por web service (servidor de aplicaciones) todas dentro una misma Intranet.

F. La Intranet debe permitir conexiones con otras redes externas, extranet y permitir la conexión a internet vía un tercer proveedor.

G. Las sedes deben acceder al Portal Corporativo vía la intranet para consumir

recursos de los servicios privado del Gobiemo que este brinde y este Portal Corporativos debe tener salida extema para sus servicios públicos, para que otras instituciones públicas o privadas requieran consumir por medio la extranet (ejemplo La Reniec, El Poder Judicial y El Banco Central de la Reserva, publican sus servicios públicos para que otras instituciones consuman sus recursos y ellos consumen servicios de otras instituciones).

H. Cada sede puede publicar servicios en la Intranet y también deberá poder consumir servicios de la misma intranet de otra sede.

I. La Infraestructura de las solución debe permitir crear grupos de trabajos entre las sedes, como sub redes dentro de la misma nube, donde los trabajos dentro de la sub nube sea comunes entre las sedes de la misma sub nube.

J. La infraestructura propuesta debe separar el empaquetado de información de voz y data, la voz debe tener mayor prioridad en la transferencia de paquetes, ambas deben considerarse como críticos, no debe existir pérdidas de paquetes en las transferencias.

K. En cada sede debe implementar conexión activa llamada principal y otra pasiva llamada backup, en caso que el principal tuviese problemas el backup tendría asumir la carga del principal sin problemas y así mantener la continuidad de los servicios.

L. Cada sede podría emitir videoconferencias hacia las demás sedes sin saturar o congestionar la nube propuesta.

M. La información Transferida debe tener niveles de seguridad en toda la nube propuesta, los paquetes no deben ser alterados a lo largo de la transferencia.

N. La rapidez de transferencia de información en la nube debe estar garantizado, desde una sede hacia otro.

O. En la implementación de red o nube, se debe considerar que los troncales principales de la red o nube deben ser de Fibra óptica en su mayoría, para tener una mayor eficiencia en la transferencia de información.

Estos son los requerimientos mínimos que el proveedor debe cumplir. Para poder brindar a la institución Gubemamental una calidad de servicio óptimo.

La propuesta de solución del proveedor debe cumplir como mínimo todos estos requerimientos emitido por parte del cliente, el cliente debe validar si la propuesta del postor cumple con sus requerimientos.

La propuesta debe incluir los equipos físicos (Routers, Switches, cableado, convertidores Fc a Utp, etc.) que son requeridos para implantación propuesta, así como la mano de obra y los software con sus licencias necesarios para poner en marcha su propuesta.

En la propuesta del proveedor solo se debe considerar la interconexión de todas las

sedes a nivel nacional, con un sistema de conexión óptimo para la institución Gubernamental.

1.4 La infraestructura actual en las diversas sedes.

La institucional gubernamental cuenta una infraestructura de red actual que data de los 90's el cual fue optimo en su momento, pero con el tiempo fue degradándose, debido al aumento de aplicaciones en la intranet y extranet, el aumento de sedes nuevas a nivel nacional esto incremento de tráfico en la red, ocasionando lentitud en los sistemas, en el anexo B se observas los diversos servicios que consume la institución.

La Infraestructura de red actual cuenta con switches (3com, Nortel, entre otros) a velocidades de transferencia de 10MB usando con cables de red categoría 5, con conexiones con algunas sedes mediante un sistema de radio enlace con antenas parabólicas a velocidades de 15MB en teoría, bajando la calidad de servicio en días de lluvia y con un alto costo en mantenimiento de las antenas parabólicas y el sistema de radio enlace.

La infraestructura de red actual solo posee conexiones radio enlace por antenas a algunas sedes principales, mientras la mayoría de sedes simplemente no tiene conexión, convirtiéndose en isla (sedes sin sistema) del sistema Gubernamental.

En cada sede ya se están implementando switches a un (1) GB y cambiando el sistema de cableado de red, faltaría un sistema de interconexión que pueda unir las sedes a nivel nacional en una intranet.

En el estado, las instituciones Gubernamentales manejan información delicada (expedientes, resoluciones, cedulas, escritos, demandas, juicios, entre otras) que deben ser manejadas con un nivel de seguridad confiable para evitar posibles filtraciones de información.

La institución Gubernamental, posee un amplio número de sedes a nivel nacional aprox. 32 sedes, que son las sedes más importantes de acuerdo al Tabla 1.1, en este Tabla mostramos una conexión activa o principal a la nube por sede y otra conexión pasiva o backup, ambos poseen la misma velocidad de transferencia, el circuito de backup solo se activara en caso que el principal tenga problemas.

En el Tabla 1.1. Observamos la segmentación del ancho de banda asignado a cada sede institucional, El segmento de voz (telefonía IP) tiene asignado como máximo 1 MB, debido a que la telefonía IP llega a cubrir alrededor de los 540 KB, 1MB es un valor aceptables para los requerimientos, En la parte de datos se le asignado el resto con la posibilidad a cubrir todo el ancho de banda si en caso nadie use el segmento de voz.

En el Tabla 1.1 muestra 32 sedes pero existe más sedes que están dentro de los departamentos o sedes principales, por ejemplo Arequipa posee 16 subsedes, La libertad

posee 12 subsedes entre otras, cada subsede debe tener el mismo accesos a la intranet por la nube propuesta, para acceder a la información de su sede principal y las demás sedes si lo requiera. En cada sede sus enlaces son independientes y cada sede puede tener sub sedes independientes.

Tabla 1.1 Ancho de banda de las sedes principales

		Ancho de Banda		Segmentación	
Ítem	**Sede**	Principal	backup	Voz	Data
1	San Martín	2 MB	2 MB	1 MB	1 MB
2	Lambayeque	4 MB	4 MB	1 MB	3 MB
3	Ancash	4 MB	4 MB	1 MB	3 MB
4	Tumbes	2 MB	2 MB	1 MB	1 MB
5	Madre de dios	2 MB	2 MB	1 MB	1 MB
6	Arequipa	8 MB	8 MB	1 MB	7 MB
7	Callao	8 MB	8 MB	1 MB	7 MB
8	Cañete	4 MB	4 MB	1 MB	3 MB
9	Huancavelica	2 MB	2 MB	1 MB	1 MB
10	Ica	4 MB	4 MB	1 MB	3 MB
11	Junín	8 MB	8 MB	1 MB	7 MB
12	La libertad	8 MB	8 MB	1 MB	7 MB
13	Lima	16 MB	16 MB	1 MB	15 MB
14	Pasco	2 MB	2 MB	1 MB	1 MB
15	Ucayali	2 MB	2 MB	1 MB	1 MB
16	Cajamarca	4 MB	4 MB	1 MB	3 MB
17	Piura	4 MB	4 MB	1 MB	3 MB
18	Loreto	2 MB	2 MB	1 MB	1 MB
19	Ilo	4 MB	4 MB	1 MB	3 MB
20	Huánuco	4 MB	4 MB	1 MB	3 MB
21	Apurímac	2 MB	2 MB	1 MB	1 MB
22	Amazonas	2 MB	2 MB	1 MB	1 MB
23	del Santa	4 MB	4 MB	1 MB	3 MB
24	Ayacucho	4 MB	4 MB	1 MB	3 MB
25	Huara	4 MB	4 MB	1 MB	3 MB
26	Lima Norte	8 MB	8 MB	1 MB	7 MB
27	Tacna	4 MB	4 MB	1 MB	3 MB
28	Moquegua	4 MB	4 MB	1 MB	3 MB
29	Puno	2 MB	2 MB	1 MB	1 MB
30	Cusco	4 MB	4 MB	1 MB	3 MB
31	Sullana	4 MB	4 MB	1 MB	3 MB
32	Lima Sur	4 MB	4 MB	1 MB	3 MB

Monitoreo de las sedes Institucionales a nivel nacional

En el Anexo F del presente informe se muestras los pantallazos de monitoreo de las

sedes institucionales a nivel nacional usando la herramienta IpSwitch que monitorea Ips de los Switches de cada sede.

En la Figura 1.2 del Anexo F se muestra caídas e intermitencias de algunas sedes, que consumen servicio Cliente/servidor y web de otras sedes y de la dese central Lima en color rojo indica cauda de conexión.

En las Figuras 1.3, 1.4, 1.5 y 1.6 del Anexo F muestran una alternativa de solución usando IPVPN a nivel nacional, cada punto sería una sede conectada a la intranet vía la nube IPVPN-MPLS.

En las Figuras 1.7 y 1.8 del Anexo F muestra la necesidad de conexión a redes Externas como la RENIEC y el Banco de la Nación, los cuales las sedes a nivel nacional consumen sus servicios expuestos vía los diversos sistemas implementados.

CAPÍTULO II
MARCO TEORICO CONCEPTUAL

2.1 FUNDAMENTOS DE MPLS

A partir de 1990 existió una gran explosión en el crecimiento del tráfico de red millones de usuarios corporativos y residenciales se unieron a la red pública de datos (Internet) provocando que existiese un incremento en el tamaño de las redes físicas y por ende, mayor consumo de ancho de banda. Con el pasar de los años las demandas de servicios son cada vez más múltiples; si anteriormente el Internet transportaba aplicaciones tolerantes en el tiempo tales como Ftp (file transfer protocol), Http (hipertext transfer protocol) ó correo electrónico, en la actualidad son aplicaciones en tiempo real como videoconferencia, voz sobre IP (VoIP), telecontrol, entre otras. Siendo así, se desarrollaron nuevas tecnologías y los servicios de capa 2 llegaron a ser una fuente de ingresos significativa para los proveedores de servicios.

En la actualidad la gran mayoría de proveedores manejan múltiples redes en un mismo núcleo o core que soportan tecnologías como FrameRelay, ATM lo cual conlleva algunas desventajas como:

- Gastos significativos en la adquisición de los equipos para las diferentes tecnologías.
- Incremento en los costos operacionales.
- Escalabilidad.
- Reducida fiabilidad.
- Deficiente uso de los recursos de la red.

MPLS (Multi protocol Label Switching) surge como una solución escalable cuya magnitud e importancia se resume en una "red multiservicio", es decir múltiples servicios que convergen en un único core MPLS.

2.1.1 PERSPECTIVA HISTÓRICA

El desarrollo de MPLS comienza en los años 90 con las empresas [3] Ipsilon y Toshiba como pioneras, quienes pusieron en el mercado los productos IP Switching y Cell Switch Route respectivamente. En respuesta a estas ofertas a partir de 1996, las

compañías Casca de Communications (IP Navigator), Cysco Systems (Tag Switching) e IBM (Aggregate Route-Based IP Switching) anunciaron sus propios productos. El trabajo realizado por cada una de estas firmas fue realizado con el objetivo común de resolver un conjunto de problemas existentes en las tradicionales redes IP tales como:

- El enrutamiento IP presentaba dificultades tanto en hardware como en software. En hardware por la implementación y en software por la limitación de la tasa de envío de paquetes en los routers IP.
- Existía congestión de red debido a que en el proceso de enrutamiento IP el envío de paquetes era sobrecargado (debido a que envía los paquetes en base a la dirección de destino) y por este mismo hecho, algunas de las líneas principales eran sobre utilizadas mientras otras no eran ocupadas.
- Finalmente, redes IP eran colocadas sobre redes ATM lo cual implica mayores costos.

Dados estos primeros pasos, en abril de 1997 [3] la **IETF** (Internet Engineering Task Force) establece el grupo de trabajo MPLS con el fin de desarrollar un estándar común; en su primera serie de estándares publicado en el año 2001. La tecnología MPLS consiste en la integración de "label swapping" con el enrutamiento de capa de red. Con esta tecnológica se esperaba [1,4]:

- Mayor flexibilidad en la entrega de nuevos servicios de ruteo. MPLS tiene la habilidad de identificar el flujo de un tráfico en particular, es decir distinguir entre diferentes tipos de servicio. Por ejemplo, si se requiere separar paquetes de email de paquetes de video, en los routers tradicionales y mediante el ruteo IP, se escoge un único camino para todos los paquetes; MPLS escoge diferentes caminos de acuerdo a la aplicación, los mismos que pueden estar basados en diferentes parámetros tales como ancho de banda requerido, QoS (Calidad de Servicio), dirección fuente, entre otros.
- Mejorar el desempeño, un ejemplo claro es a través de la Ingeniería de Tráfico. A diferencia del tradicional ruteo IP que siempre toma el camino más corto para el envío de información, usando por lo general las mismas rutas para destinos múltiples y por tanto creando congestión de tráfico; MPLS-TE (MPLS – Traffic Engineering) posibilita la creación de múltiples túneles al mismo destino y usar diferentes caminos para el envío dela información, proveyendo balance de carga a través de los diferentes enlaces, aliviándola congestión y asegurando la optimización del tráfico en cada router.
- Escalabilidad en el enrutamiento de capa de red, agregando información de envío a través de las etiquetas, mientras se trabaja en presencia de jerarquías de enrutamiento.

En la actualidad el trabajo y esfuerzos de la **IETF** continúan, creándose nuevos grupos de trabajo referidos a MPLS tales como Layer 3 VPN (l3vpn), Layer 2 VPN

(l2vpn), Common Control and Measurement Plan (ccamp) y Pseudo Wire Emulation Edge to Edge (pwe3).

2.1.2 DEFINICIÓN DE MPLS

Multi protocol Label Switching [7] es una tecnología de envío en la cual los paquetes son enviados basados en etiquetas1. Su arquitectura describe los mecanismos para ejecutar la conmutación de etiqueta ó label switching combinando los beneficios de IP switching de la capa 2 con el IP routing de la capa 3.

2.1.3 CARACTERÍSTICAS DE MPLS

Entre las características más importantes de MPLS se pueden mencionar [7]:

- En MPLS los paquetes son enviados basados en etiquetas.
- Las etiquetas pueden corresponder a redes de destino IP o también a otros parámetros tales como dirección fuente, QoS, entre otros.
- El mecanismo de envío a lo largo de la red se denomina label swapping.
- MPLS soporta el envío de otros protocolos.

2.1.4 ARQUITECTURA MPLS

Básicamente la arquitectura MPLS está conformada por dos componentes principales [1,7]: el componente de control (control plane) y de envío (data plane).

Adicionalmente existen nuevos términos introducidos los cuales permiten describir la funcionalidad y roles de cada uno de los equipos o dispositivos que en su conjunto forman la arquitectura. A continuación de manera breve se describen cada uno de ellos.

2.1.4.1 Red MPLS

Una red MPLS está conformada por una serie de nodos o puntos llamados LSR (Label Switching Routers), lo cuales son capaces de conmutar y enviar paquetes IP etiquetados [1].

.2.1.4.2 Componente de control (Control Plane)

La función del componente de control es intercambiar información de ruteo y etiquetas, esto lo realiza mediante complejos mecanismos definidos en estándares tales como BGP (Border Gateway Protocol), OSPF (Open Shortest Path First), EIGRP (Enhanced Interior Gateway Routing Protocol) y TDP (Tag Distribution Protocol), LDP (Label Distribution Protocol), RSVP (Resource Reservation Protocol) respectivamente [7].

2.1.4.3 Componente de envío (Data Plane)

La función de este componente es el envío de paquetes basados en etiquetas. En la se observa la arquitectura básica de un nodo MPLS realizando enrutamiento IP.

2.1.4.4 LSR (Label Switch Router)

Un LSR o router de conmutación de etiqueta es cualquier router o switch que cumple las siguientes funciones:

- Intercambiar información de ruteo.
- Intercambiar etiquetas.
- Enviar paquetes basados en etiquetas o celdas2.

En una red MPLS se pueden distinguir tres tipos de LSR [2]:

- **LSRs de Ingreso**, un LSR de ingreso es un router que está ubicado en la periferia de la red MPLS cuya función es recibir paquetes IP, imponer una etiqueta (ó pila de etiquetas) y finalmente enviarlos al dominio MPLS. La operación de imposición de etiqueta es conocida como **Push Action**.
- **LSRs de Salida**, un LSR de salida es un router que está ubicado en la periferia de la red MPLS y cuya función es recibir paquetes IP etiquetados, remover la etiqueta (ó pila de etiquetas) y finalmente enviarlos fuera del dominio MPLS. La operación de remover la etiqueta es conocida como **Pop Action**.

NOTA: los LSRs de entrada y salida son conocidos como **Edge-LSR** y realizan una conmutación basada en FECs (Forwarding Equivalance Class).

- **LSRs Intermedios**, un LSR intermedio es un router que está ubicado en el núcleo de la red MPLS cuya función es recibir paquetes IP etiquetados, cambiar la etiqueta existente por otra y enviarlos al siguiente LSR. Realizan conmutación directa.

La operación de cambiar la etiqueta existente por otra es conocida como **Swap Action**.

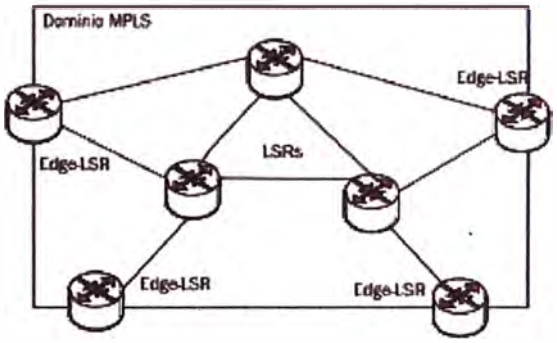


Figura 2.1.1 El LSR y Edge LSR en la red MPLS [2]

2.1.4.5 FEC (Forwarding Equivalence Class)

Una Clase Equivalente de Envío [3] se define como un conjunto de paquetes IP que comparten los mismos atributos, que son enviados de la misma manera, a través del mismo camino (Figura 2.1.1) y/o requieren el mismo servicio.

Cuando los paquetes entran al dominio MPLS a través del LSR de ingreso, éste determina a qué Clase Equivalente de Envío corresponden los mismos y por tanto todos los paquetes que pertenecen a la misma FEC tienen la misma etiqueta.

2.1.4.6 LSP (Label Switched Path)

Un LSP se puede definir como un camino lógico, unidireccional de origen a destino que se forma por la concatenación de varios LSRs. El primer LSR de un LSP es el LSR

de ingreso el último es el LSR de salida y entre los dos se encuentran los LSR intermedios (Figura 2.1.2).

Un LSP es el mismo para paquetes que pertenecen a la misma FEC.

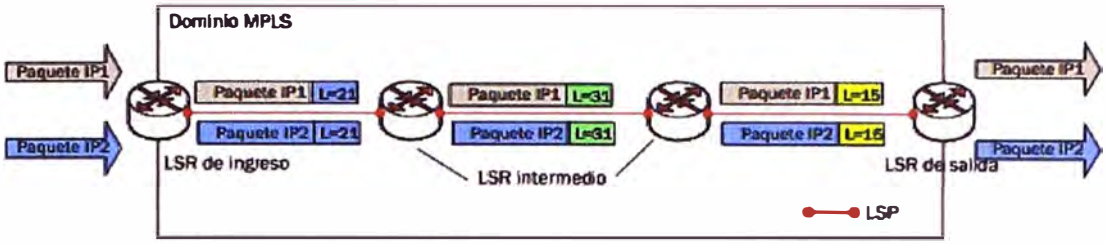


Figura 2.1.2 FEC y establecimiento de un LSP [3]

2.1.4.7 Etiqueta MPLS

Una etiqueta MPLS es un conjunto pequeño de 32 bits cuya estructura se puede observar en la Figura 2.1.3. Los campos contenidos en la cabecera MPLS contienen la siguiente información [3]:

Figura 2.1.3 Formato de la cabecera MPLS [3]

- **Etiqueta**, este campo está conformado por 20 bits y su valor representa a determinada FEC durante el envío de paquetes. Su valor es usado como un indicador dentro de la tabla de envío almacenada en un LSR.
- **EXP**, 3 bits experimentales los cuales son usados para identificar la Clase de Servicio a la que pertenece el paquete.
- **Bottom of Stack**, un bit que sirve como indicador en el caso de existir dos o más etiquetas MPLS insertadas en el paquete (label stack), el mismo que dice si la etiqueta es la última en la cola.
- **TTL**, campo llamado Time to Live constituido de 8 bits y que representa el número de saltos que un paquete IP da antes de llegar a su destino. Su valor va disminuyendo en cada salto, cuando este valor es cero el paquete es eliminado. De esta manera se evita lazos o que el paquete permanezca innecesariamente en la red debido a un enrutamiento erróneo o defectuoso.

2.1.4.8 Encapsulación MPLS

La etiqueta MPLS o pila de etiquetas es insertada entre las cabeceras de capa de enlace y capa de red por lo que es conocida como "*shim header*" o cabecera acuñada (ver Figura 2.1.4).

El uso de la *shim header* permite soportar conmutación de etiqueta sobre algunas tecnologías de capa 2 tales como Ethernet, FDDI, enlaces punto a punto, entre otras.

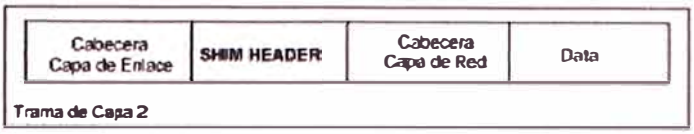


Figura 2.1.4 Cabecera acuñada "*shim header*" [3]

2.1.4.9 Pila de Etiquetas

Una de las opciones que ofrece MPLS es la agregación de dos o más etiquetas a un paquete lo cual se conoce como label stack. La primera etiqueta en la cola es conocida como top label, la última como bottom label y entre ellas se tienen cualquier número de etiquetas.

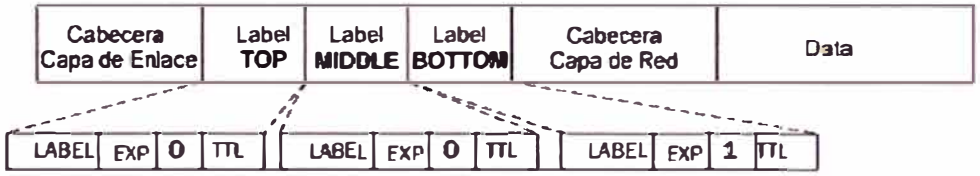


Figura 2.1.5 La pila de etiquetas [3]

Como se muestra en la Figura 2.1.5 el valor del bit perteneciente al campo BoS en el caso de la etiqueta bottom es 1 y para el resto es cero. Existen algunas aplicaciones que necesitan más de una etiqueta como por ejemplo MPLS VPNs (2 etiquetas) y MPLS Traffic Engineering (2 ó más etiquetas).

2.2 REDES PRIVADAS VIRTUALES

En la industria de las telecomunicaciones el término VPN (Virtual Private Network) o Red Privada Virtual es una de las palabras más conocida y usada por cada uno de los proveedores de servicios, los mismos que con el objetivo de brindar y satisfacer los requerimientos de sus clientes, han encontrado en la implementación de redes privadas virtuales una solución a través de la cual se logra extender las redes de sus clientes a nivel nacional, alrededor del mundo y a menores costos.

Una red privada virtual VPN reemplaza las redes tradicionales basadas en routers que conectan los sitios de los clientes a través de enlaces punto a puntos dedicados emulando enlaces punto a punto a través de una infraestructura compartida. Usa una red pública, usualmente el Internet para conectar sitios remotos.

Con el crecimiento del Internet las redes privadas virtuales se han convertido en el área de mayor crecimiento y su popularidad está acompañada del surgimiento de muchas técnicas a través de las cuales se puede proveer esta función. Asimismo cada una de éstas técnicas usa diferentes protocolos y por ende el uso de una en especial tiene sus propias ventajas y desventajas.

2.2.1 DEFINICIÓN DE UNA RED PRIVADA VIRTUAL

Una red privada virtual se puede definir de la siguiente manera:

Una red privada virtual se puede definir [6] como una red a través de la cual se interconectan sitios/puntos que se encuentran geográficamente dispersados, mediante enlaces punto a punto a través de una infraestructura compartida. Para ello las redes privadas virtuales hacen uso de técnicas avanzadas de encriptación y tunneling (enrutamiento punto a punto) permitiendo a las organizaciones seguridad extremo a extremo a través de una red pública como por ejemplo el Internet.

Cabe aclarar que la red es privada en el sentido de que el enrutamiento y direccionamiento utilizado en la red es totalmente independiente del enrutamiento y direccionamiento de otras redes. Y es virtual, ya que la infraestructura para operar la red de determinada compañía puede ser compartida con otras compañías que quieren contratar su propia VPN [3].

La empresa que presta las facilidades para establecer la red se denomina proveedor de servicios VPN y la empresa que contrata el servicio se conoce como cliente VPN.

2.2.2 TOPOLOGÍA BÁSICA DE UNA RED PRIVADA VIRTUAL

Se pueden diferenciar los siguientes componentes en la topología básica de una red privada virtual [3]:

- Una red existente con servidores y estaciones de trabajo.
- Conexiones a Internet.
- Puerta de enlaces VPNs, como por ejemplo firewalls, PIX, o concentradores VPNs.
- El software que crea y mantiene los túneles.

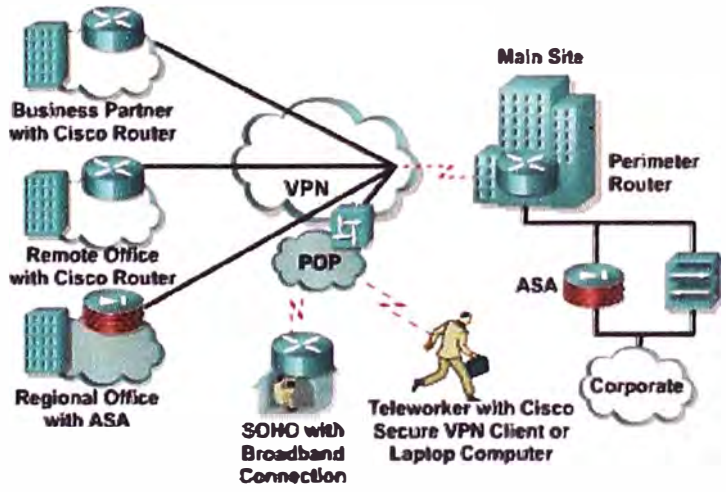


Figura 2.2.1 Elementos que conforman una VPN [1]

Cabe recalcar que la palabra clave al momento de referirse a una VPN es la seguridad (Figura 2.2.1). La seguridad de los datos en una red privada virtual puede hacerse de tres maneras:

- Encapsultamiento de los datos.
- Encriptación,

- Encapsulamiento y encriptación.

2.2.3 TIPOS DE REDES PRIVADAS VIRTUALES

Existen tres tipos comunes de VPNs [5,11]:

VPN de Acceso Remoto (Remote Access [RAS] VPN)

Una VPN de acceso remoto se conoce también con el nombre de Virtual Private Dial-upNetwork (VPDN), y consiste en una conexión usuario a LAN a través de la cual usuarios de determinada compañía necesitan conectar la red privada desde varios puntos remotos (VPN) y cuyo acceso es vía marcación (dialing mode). Es decir, es una red privada virtual donde el modo de acceso del usuario es a través de la marcación. El uso de una VPDN o VPN de acceso remoto permite a las empresas contar con conexiones seguras y cifradas entre su red privada y usuarios remotos a través de un tercero, es decir un proveedor de servicios.

Una empresa que crea y usa una VPN de acceso remoto, a través de un ISP (Internet Service Provider) proporciona una cuenta dial-up de Internet a cada uno de sus usuarios los mismos que al marcar un número 1800 determinado logra conectarse al Internet y mediante el uso de un software VPN de usuario/cliente acceder a la red corporativa.

Site-to-Site VPN

Este tipo de VPN consiste en la conexión de múltiples puntos geográficamente dispersados a través de una red pública como por ejemplo el Internet. Cada punto requiere únicamente de una conexión local hacia la misma red pública. Las Site-to-SiteVPNs pueden ser categorizadas en dos grupos:

- ***Site-to-Site Intranet VPN***: Es aquella VPN que se construye con puntos/oficinas que pertenecen a la misma compañía. Es decir, una empresa que tiene uno o más puntos remotos los cuales se comunican a través de únicamente una red privada virtual.
- ***Site-to-Site Extranet VPN***: VPN que se construye para conectar una empresa con sus socios o clientes. Es decir, una compañía que posee vínculos con otra, ya sea un cliente, socio, proveedor; éstas pueden implementar una Extranet VPN mediante la cual se una la red LAN de cada empresa permitiendo así trabajar en un mismo entorno.

VPN basadas en Firewall [5]

Una VPN basada en firewall está intrínsicamente incluida en una implementación Site-to-Site. Es una solución orientada a resolver los problemas de seguridad y es implementada cuando una compañía requiere mayores y avanzadas medidas de seguridad para sus VPNs.

El buen y correcto diseño de una VPN puede ser de gran beneficio para una empresa desde los siguientes puntos de vista:

- Ampliar la conectividad geográficamente.
- Reducir los costos operacionales.
- Reducir los tiempos de tránsito y costos de viaje para usuarios remotos.
- Mejorar la productividad.
- Se logra simplificar la topología de red y con ello se facilita la administración de la misma. Entre otras.

Ahora analizaremos el enfoque principal de red privada virtual

2.2.4 CARACTERISTICAS DE SEGURIDAD EN UNA VPN

Como se ha mencionado anteriormente el enfoque principal en la implementación de una red privada virtual es la seguridad para lo cual se hace uso de técnicas avanzadas de encriptación y tunneling. El fundamento de VPNs seguras está basado en la autenticación, la encapsulación y la encriptación [5,11].

2.2.4.1 Confidencialidad de los datos

Como característica de diseño de una VPN la confidencialidad de los datos tiene como objetivo proteger la interpretación del contenido de los mensajes desde fuentes no autenticadas o no autorizadas. Una VPN logra ofrecer confidencialidad a través de mecanismos encapsulación y encriptación.

Este es uno de los servicios más importantes que se pueden brindar a través de una implementación VPN.

Encapsulación

La encapsulación es uno de los principales componentes de la confidencialidad en una implementación VPN. Los túneles son una excelente aplicación del encapsulamiento.

Tunneling [6]

El enrutamiento punto a punto o tunneling, es el proceso de colocar un paquete dentro de otro paquete y al nuevo paquete compuesto enviarlo a través de la red. En la Figura 2.2.2 se puede diferenciar los siguientes elementos, los datos que se transfieren se denominan carga, el paquete que se envía se encapsula utilizando la cabecera de un protocolo de enrutamiento punto a punto el cual es enviado desde y hacia los extremos del túnel, definidos como extremos finales del túnel o del canal. A través de la cabecera del protocolo de enrutamiento los routers intermedios deciden por donde encaminar el paquete hacia el punto final del túnel.

En tunneling se usan tres protocolos diferentes:

- **Passenger protocol**, los datos originales (IPX, AppleTalk, IPv4, IPv6).
- **Protocolos de encapsulamiento**, protocolos que envuelven la información original (GRE,IPsec, L2F, PPTP, L2TP).

- **Carrier protocol**, el protocolo por el cual viaja la información (FrameRelay, ATM, MPLS).

Cabe mencionar que los protocolos (GRE,IPsec, L2F, PPTP, L2TP) ofrecen el mismo nivel de seguridad.

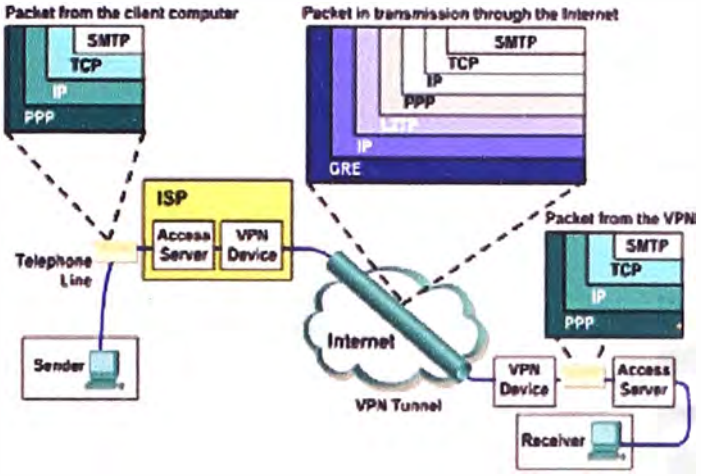


Figura 2.2.2 Encapsulamiento de información en la red VPN [1]

El paquete original es encapsulado dentro de un protocolo de encapsulamiento el mismo que es puesto dentro de la cabecera de un protocolo de transporte (usualmente IP) para la transmisión del paquete a través de la red pública (Ver Figura 2.2.2).

Criptografía

La criptografía es otra de las principales características de confidencialidad en una implementación VPN. El cifrado es el proceso de tomar todos los datos que un computador está enviando a otro computador y codificarlos de tal manera que sólo el otro computador sea capaz de decodificar y pon ende entender. Existen dos tipos de algoritmos de criptografía:

Criptografía Simétrica o Llaves privadas.

La criptografía simétrica o de llave privada (también conocida como criptografía convencional) está basada en una llave secreta que comparten ambas partes que se comunican (ver Figura 2.2.3).

La parte emisora utiliza la llave secreta como parte de la operación matemática para cifrar (o codificar) texto plano a texto cifrado. La parte receptora utiliza la misma llave secreta para desencriptar (o descifrar) el texto cifrado a texto plano.

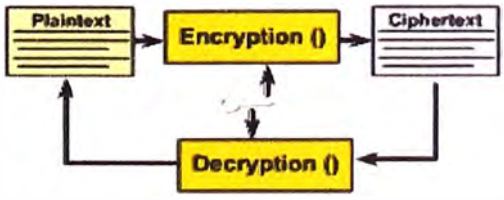


Figura 2.2.3 Bosquejo de criptografía de llave pública [5]

Algunos ejemplos de los esquemas de criptografía simétrica son los algoritmos DES, 3DES y AES.

Data Encryption Data (DES), fue desarrollado por IBM y publicado como estándar en el año 1997. Este algoritmo utiliza una llave para la transformación, de modo que el descifrado sólo pueda ser realizado por aquellos que conocen la clave concreta para cifrar. La llave o clave mide 64 bits de los cuales son utilizados 56 en el algoritmo, el resto se utiliza únicamente para comprobar la paridad y después son descartados.

En la actualidad, el algoritmo DES es considerado inseguro para muchas aplicaciones debido a que el tamaño de la clave (56 bits longitud efectiva) es demasiado pequeña. Se ha detectado que claves DES se han roto en menos de 24 horas y resultados de estudios demuestran que existen debilidades teóricas en su cifrado.

Triple Data Encryption Data (3DES), triple DES se puede definir como un algoritmo de cifrado de bloque que se formó a partir de DES. Fue desarrollado por Walter Tuchman8 en1978. Se puede resumir su funcionamiento observando la Figura 2.2.4.

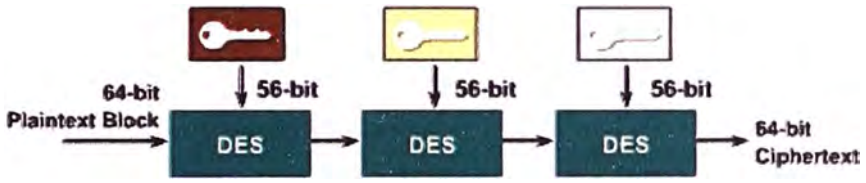


Figura 2.2.4 Bosquejo de 3 DES [5]

Advanced Encryption Standard (AES), algoritmo formalmente conocido como criptografía de Rijnda el, sucesor de DES y 3 DES y aprobado por el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology [NIST]) en diciembre del año 2001.

Este algoritmo está caracterizado por soportar llaves de 128, 192, y 256 bits siendo la llave de 128 segura es un algoritmo más seguro y rápido que 3 DES. El tamaño del bloque es de18 bits.

AES es un algoritmo que fue adoptado como estándar por el gobierno de los Estados Unidos y se espera que al igual que DES sea utilizado en todo el mundo.

Criptografía Asimétrica o Llaves públicas.

La criptografía asimétrica o de llave pública utiliza dos llaves diferentes para cada usuario: una es una llave privada conocida sólo por este usuario; la otra es una llave pública correspondiente, que es accesible para todos. Se utiliza una llave para encriptación y la otra para la desencriptación, dependiendo de la naturaleza del servicio de comunicación que se esté implementando. Estos algoritmos proporcionan no rechazo y autenticación. En la actualidad se usa el sistema de llave o clave pública: RSA diseñado por Rivest, Shamir y Adelman (ver Figura 2.2.5).

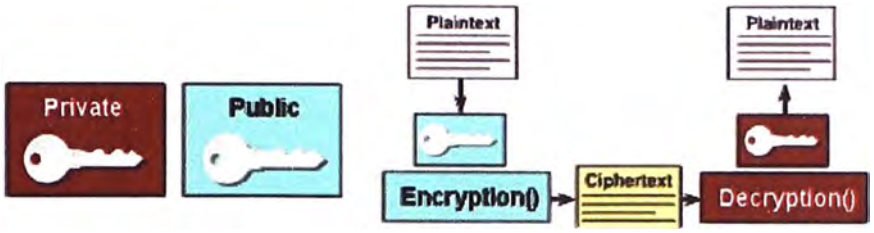


Figura 2.2.5 Bosquejo de criptografía de llave privada [5]

Algoritmo de llave pública RSA (Rivest, Shamir y Adelman), fue uno de los primeros grandes avances en la criptografía pública y el primero en desarrollarse. RSA utiliza los principios de intercambio de llave de Diffie-Hellman (IKE):

Una llave pública para encriptar los datos y verificar firmas digitales y,

Una llave privada para desencriptar los datos y para firmar con una firma digital.

2.2.4.2 Integridad de los datos

Existe la posibilidad que los datos sean modificados en el transcurso de su viaje a través del Internet. La integridad de los datos en VPNs garantiza que no se produzcan alteraciones y modificaciones mientras los datos viajan de origen a destino y para lograrlo VPNs suelen utilizar los siguientes métodos: one-way hash functions, message autentication codes (MAC) o firmas digitales.

Funciones Hash

Una función hash consiste en tomar un mensaje de longitud variable y generar una cadena de longitud fija, lo cual se conoce como valor hash. Las funciones hash son usadas para asegurar la integridad de los datos y ejemplos de algoritmos hash son MD5 (MessageDigest5), Secure Hash Algorith (SHA-1) y RIPE-MD-m 160.

Códigos de Autenticación de Mensajes

Los códigos de autenticación de mensajes MACs agregan una llave a las funciones hash. El emisor crea un archivo, calcula la MAC basado en la llave compartida con el destinatario y luego añade la MAC al archivo. Cuando el destinatario recibe el archivo calcula una nueva MAC y la compara con la MAC añadida.

Firmas Digitales

Una firma digital es una criptografía de llave pública pero en sentido inverso, es decir que funciona de manera inversa al proceso de cifrado normar. La firma digital utiliza la llave privada en algunos bloques de datos (sólo un individuo tiene acceso a la clave privada) y el receptor descifra esos datos con la clave pública que está disponible y que es conocida. En otras palabras un emisor firma digitalmente un documento con la llave privada del emisor y el receptor puede verificar la firma usando la misma llave pública del emisor.

2.2.4.3 Autenticación

Mediante la autenticación se asegura que el mensaje llegue desde una fuente válida hacia una fuente válida. Mediante la autenticación se protege a la VPN de ataques que dependen de la suplantación de la identidad del remitente y adicionalmente permite a cada usuario de la comunicación saber exactamente con quién está hablando. La autenticación incluye contraseñas, certificados digitales, tarjetas inteligentes.

- Nombre de usuario y contraseña: utiliza nombres de usuarios y contraseñas predefinidos para diferentes usuarios o sistemas.
- One Time Password (OTP) (Pin/Tan): es un método más fuerte que el método de nombre de usuario y contraseña en el cual se generan nuevas contraseñas por cada autenticación.
- Biométrica: por lo general la biometría se refiere a las tecnologías que se utilizan para medir y analizar características del cuerpo humano tales como huellas dactilares, patrones de voz faciales, etc., enfocados principalmente en fines de autenticación.
- Llaves pre-compartidas: este método de autenticación utiliza un valor de llave secreta que es manualmente introducido por cada uno de los compañeros y luego se utiliza para autentificar a los pares.
- Certificados digitales: usa el intercambio de certificados para autentificar los pares.

Un certificado es una estructura de datos que está firmada digitalmente por una autoridad certificadora (CA) en la que los usuarios del certificado pueden confiar. El certificado contiene varios valores, como el nombre y el uso del certificado, la información que identifica al propietario de la llave pública, la llave pública misma, una fecha de expiración y el nombre de la autoridad certificadora.

Los certificados de llaves públicas proporcionan un método conveniente y confiable para verificar la identidad de un remitente.

2.2.5 TERMINOLOGÍA USADA EN REDES PRIVADAS VIRTUALES

Una solución VPN tiene un cierto número de componentes los cuales se pueden diferenciar en la Figura 2.2.6 y cuyo papel se describe a continuación [1,5].

Proveedor de servicios (ServiceProvider), es la organización que con su propia infraestructura la cual incluye equipo y medio de transmisión proporciona a sus clientes líneas dedicadas emuladas. El proveedor de servicios ofrece a sus clientes un Servicio de Red Privada Virtual (Virtual Private Network Service).

Red de proveedor (Provider Network [P-Network]), es la infraestructura, equipo y medio de transmisión del proveedor de servicios usada para ofrecer servicios VPNs.

Red de cliente (Customer Network [C-Network]), corresponde a la parte de la red que está bajo el control del cliente.

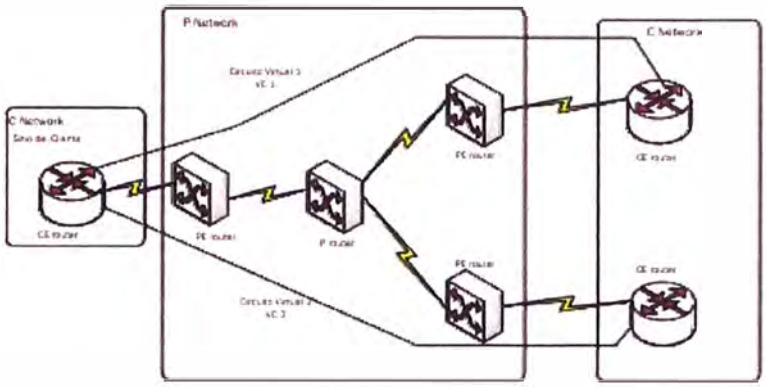


Figura 2.2.6 Dispositivos de una MPLS VPN [3]

Sitio del cliente (Customer Site), es una parte contigua a la C-Network que puede comprender muchas ubicaciones físicas.

Equipo de proveedor (Provider device [P-device]), es el equipo que está dentro de la P-Network que no tiene conectividad con el cliente y tampoco ningún conocimiento de la VPN. Este equipo usualmente es un router y es comúnmente conocido como un P-router.

Equipo de borde del proveedor (Provider Edgedevice [PE device]), el PE es un dispositivo que está en la P-Network al cual se conectan los CE. Usualmente es un router y es a menudo referido a un PE router.

Equipo de borde del cliente (Customer Edgedevice [CE device]), equipo en la C-Network es el dispositivo a través del cual el cliente/usuario final se conecta a la red del proveedor de servicios también es conocido como equipo local del cliente (Customer Premises Equipment [CPE]). Usualmente es un router y es a menudo referido a un CE router.

Circuito virtual (Virtual Circuit [VC]), es un enlace lógico punto a punto que se establece a través de una infraestructura compartida a nivel de capa 2. Un circuito virtual puede estar constantemente activo (Permanent Virtual Circuit [PVC]) ó establecido por demanda (Switched Virtual Circuit [SVC]).

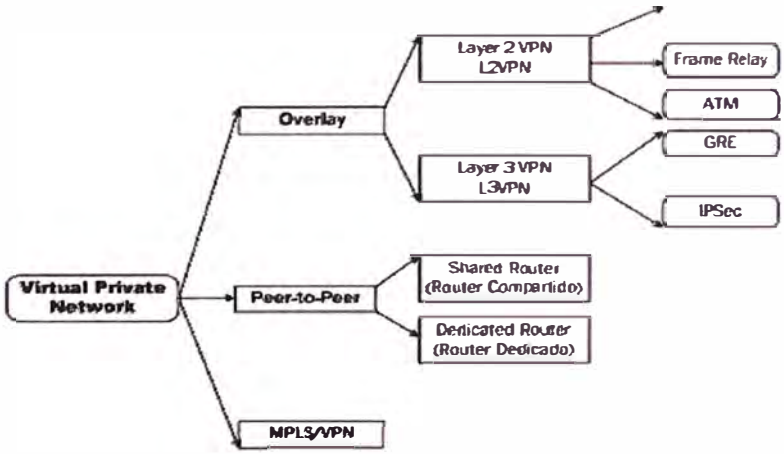


Figura 2.2.7 Clasificación de VPN [3]

2.2.6 MODELOS USADOS EN IMPLEMENTACIONES DE VPNs

Existen varios caminos a través de los cuales se puede clasificar las redes privadas virtuales (ver Figura 2.2.7) a pesar de ello y por la utilización se puede categorizar a las VPNs según los siguientes criterios:

2.2.6.1 MODELO OVERLAY

A través del modelo Overlay el proveedor de servicios provee la VPN al cliente a través de un conjunto de líneas arrendadas emuladas las cuales se conocen normalmente como circuitos virtuales (virtual circuits [VCs]) las cuales pueden estar constantemente disponibles PVC o ser establecidos por demanda SVC (Figura 2.2.8).

Adicionalmente el cliente establece la comunicación router a router entre los CE routers a través de los VC proporcionados por el proveedor de servicios. La información de enrutamiento siempre se intercambia entre los dispositivos del cliente y por ende el proveedor de servicios desconoce la estructura interna de la red del cliente.

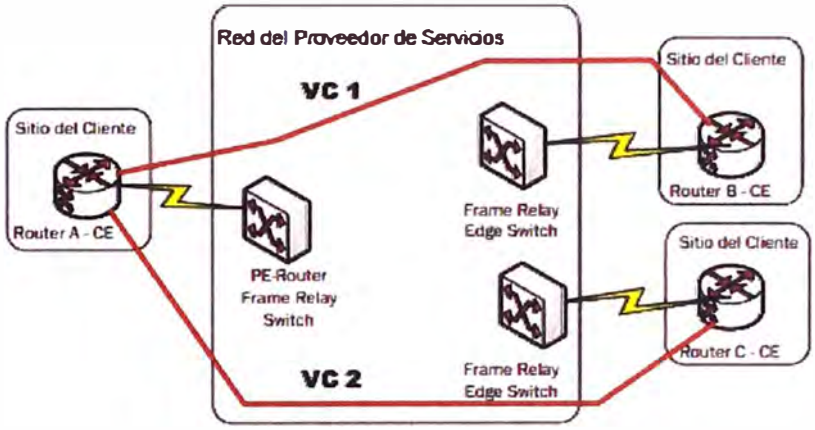


Figura 2.2.8 Modelo Overlay VPN [3]

Este tipo de VPNs puede ser implementada a nivel de capa 1 usando líneas arrendadas, a nivel de capa 2 usando por ejemplo X.25, FrameRelay circuitos virtuales ATM y finalmente a nivel de capa 3 usando túneles IP (GRE).

Modelo Overlay implementación a nivel de capa 1:

Adopta la solución tradicional de multiplexación por división en el tiempo TDM, en esta topología el proveedor de servicios establece la conectividad en la capa física entre los sitios del cliente y el cliente es responsable de las capas superiores (Figura 2.2.9).

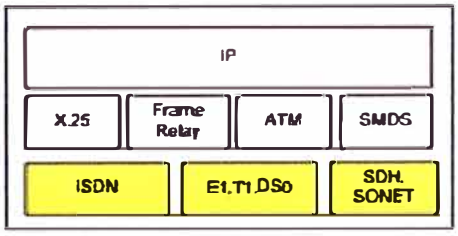


Figura 2.2.9 Overlay VPN a nivel de capa 1 [9].

Modelo Overlay implementación a nivel de capa 2:

La implementación a nivel de capa 2 (L2VPN) adopta la solución tradicional de WAN switcheada: el proveedor de servicios establece circuitos virtuales de capa 2 entre los sitios del cliente y el cliente es responsable de las capas superiores (Figura 2.2.10).

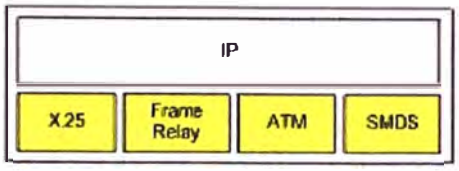


Figura 2.2.10 Overlay VPN a nivel de capa 2 [9]

Modelo Overlay implementación a nivel de capa3:

Un modelo overlay de capa 3 (L3VPN) es a menudo una implementación con túneles "IP en IP" a través de protocolos tales como PPTP (Point to Point Tunneling Protocol), L2TP(Layer 2 Tunneling Protocol), GRE (Generic Routing Encapsulation) e IPsec (Figura 2.2.11).

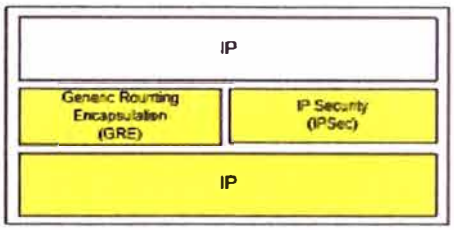


Figura 2.2.11 Overlay VPN a nivel de capa 3 [9]

Beneficios y Desventajas de la Implementación Overlay VPN

A través de una implementación Overlay VPN se puede tener los siguientes beneficios:

- Una VPN Overlay es bien conocida y fácil de implementar.
- El proveedor de servicios no participa en el enrutamiento del cliente.
- La red del cliente y del proveedor de servicio están aisladas.

Así mismo las desventajas son:

- Para un enrutamiento óptimo se requiere un full mesh de los circuitos virtuales.
- Los circuitos virtuales deben proporcionarse manualmente.

2.2.6.2 MODELO PEER-TO-PEER

El modelo Peer-to-Peer VPN fue introducido con el objetivo de aliviar las desventajas existentes con el modelo overlay. En este modelo el router PE intercambia directamente información de enrutamiento con el CE router. Es decir que, tanto la red del proveedor como la del cliente usan el mismo protocolo de red y todas las rutas del cliente son transportadas dentro de la red del proveedor de servicios. En la Figura 2.2.12 se puede observar de manera general el modelo peer-to-peer VPN y la función de los equipos.

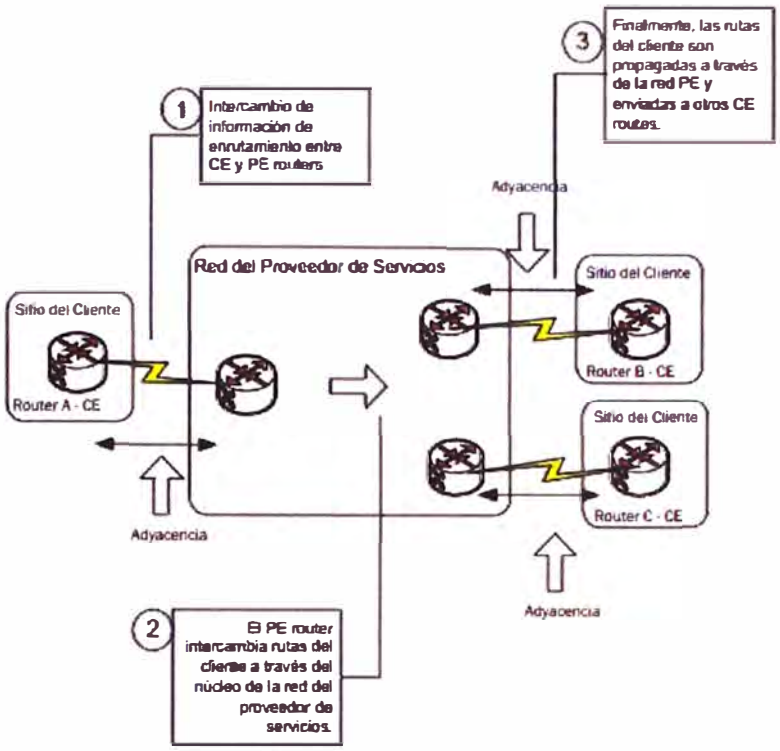


Figura 2.2.12 Modelo peer-to-peer VPN [9]

Modelo PE router compartido (Shared Router) [1]:

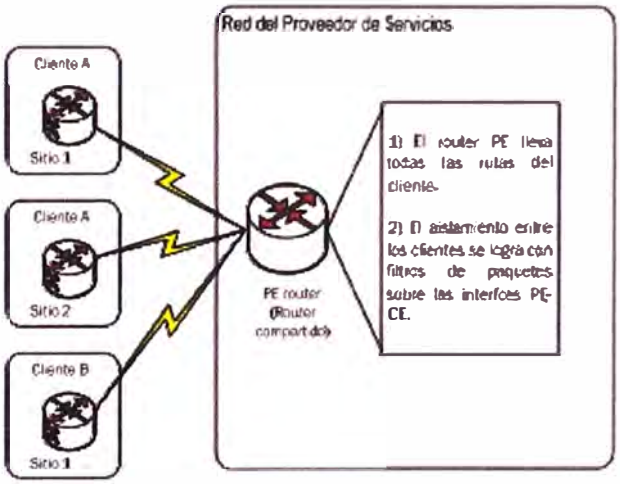


Figura 2.2.13 Modelo de router compartido "sharedrouter" [9]

En este modelo, varios clientes se pueden conectar al mismo PE router, pero listas de acceso son configuradas en cada interfaz PE-CE (es decir que, las rutas individuales de los clientes son separadas con filtros de paquetes en las interfaces PE-CE) de manera que se asegure el aislamiento entre los clientes VPN (Figura 2.2.13).

Al implementar este tipo de VPN se presentan las siguientes desventajas:

- Todos los clientes comparten en mismo espacio de direccionamiento.
- Altos costos de mantenimiento son asociados con filtros de paquetes.
- El rendimiento es bajo.

Modelo PE router dedicado (Dedicated Router):

En este modelo cada cliente VPN tiene un PE router dedicado que transporta únicamente sus propias rutas. A través de protocolos de enrutamiento cada PE router crea sus tablas, las cuales contienen sólo las rutas anunciadas por el cliente VPN conectados a ellos. De esta manera se logra aislar las VPN (Figura 2.2.14).

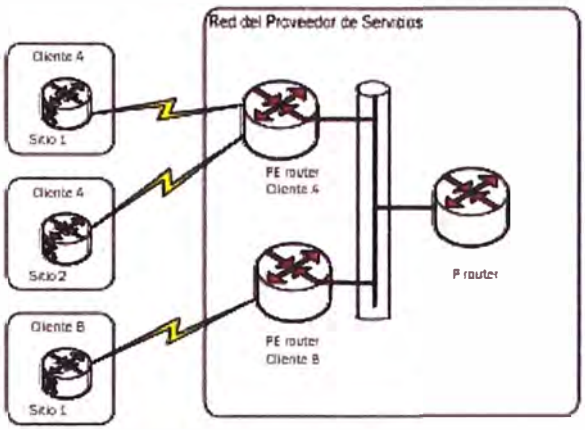


Figura 2.2.14 Modelo de router dedicado [8]

Al implementar este tipo de VPN se presentan las siguientes desventajas:

- Todos los clientes comparten el mismo espacio de direccionamiento.
- Cada cliente requiere un router dedicado para cada punto de presencia (POP).

2.2.6.3 MODELO MPLS VPN

Una VPN basada en MPLS usa el modelo peer-to-peer y combina los beneficios de overlay y peer-to-peer VPN: i) seguridad y características de segregación, ii) simplificación del enrutamiento del cliente, respectivamente.

La arquitectura de una MPLS/VPN es bastante similar al modelo PE router dedicado pero con la diferencia que los routers dedicados por cliente son implementados como tablas de enrutamiento virtuales dentro del PE router. Es decir que el aislamiento entre los clientes VPN es por medio de routers virtuales levantados en el PE router a través de enrutamiento y envío virtual (Virtual Routing and Forwarding [VRF]) los cuales pertenecen a diferentes clientes VPN.

Cabe resaltar algunas características puntuales de una MPLS/VPN lo cual surge de la combinación de beneficios de overlay y peer-to-peer VPNs.

- En una MPLS/VPN se permite el overlapping de direcciones en diferentes clientes/sitios VPN debido a que cada PE router virtual maneja su propia tabla de enrutamiento. Es decir los clientes pueden tener el mismo espacio de direcciones.
- La tabla de enrutamiento que almacena el PE router se reduce significativamente ya que sólo guarda la información de enrutamiento de la VPNs que están directamente conectadas.

- La cantidad de información de enrutamiento es proporcional al número de VPN conectadas al PE router, por tanto esta crece cuando el número de VPN directamente conectadas crece.
- Los PE routers participan en el enrutamiento del cliente pero asegurando el enrutamiento óptimo entre los sitios.
- Con MPLS/VPN el enrutamiento total dentro del backbone del proveedor de servicios ya no es necesario y tampoco el enrutamiento tradicional IP para enviar paquetes.

2.2.7 REQUERIMIENTOS QUE DEBE CUMPLIR UNA VPN

Debido al tipo de conexión que ofrece una VPN se debe garantizar a través de la misma la privacidad e integridad de los datos que viajan a través de la red pública, o de una red corporativa. Siendo así se considera que una solución VPN debe proveer a cada uno de los clientes lo siguiente:

- Autenticación de usuario: verificando la identidad del usuario y restringiendo acceso a la VPN a usuarios no autorizados.
- Administración de dirección: deberá asignar una dirección al cliente en la red privada y deberá asegurarse que mismas se mantengan sin cambios.
- Encriptación de datos: a través de la encriptación asegurar que los datos no serán leídos por usuarios no autorizados.
- Administración de llaves: generando y renovando las llaves de encriptación tanto para el cliente como para el servidor.
- Soporte de protocolo múltiple: la red VPN debe poder manejar protocoles comunes utilizados en redes públicas.

2.2.8 PROTOCOLOS USADOS EN REDES PRIVADAS VIRTUALES

Para establecer un túnel tanto del lado del cliente como del servidor se debe levantar el mismo protocolo de túnel. Los protocolos de túnel se pueden clasificar de acuerdo al modelo OSI en protocolo del túnel de Nivel 2 o de Nivel 3, en el primer caso corresponde a la capa de enlace y utiliza tramas como su unidad de intercambio y en el segundo caso corresponden a la capa de red y utiliza paquetes.

De acuerdo a lo mencionado anteriormente, PPTP (Point to Point Tunneling Protocol),L2TP (Layer 2Tunneling Protocol) y L2F (Layer 2 Forwarding) pertenecen al grupo de protocolos de túnel de nivel 2 los cuales que encapsulan la carga útil (datos transferidos por el túnel) en una trama del protocolo punto a punto PPP (Point to Point Protocol) sección 2.8.1.Y, IP sobre IP e IPSec (Internet Protocol Security) pertenecen al grupo de protocolos de túnel de nivel 3.

2.2.8.1 Protocolo punto a Punto (PPP)

Los protocolos de túnel de Nivel 2 dependen principalmente de las funciones que se

especifican en el protocolo punto a punto o PPP publicado por la IETF y estandarizado en la RFC 1661, siendo así cabe resaltar los aspectos más relevantes del mismo de manera que se logre entender los protocolos de túnel en cuestión.

PPP está diseñado para enlaces simples que envían paquetes entre dos pares; estos enlaces proveen operación simultánea bidireccional full duplex y se asume entregar los paquetes en orden. Generalmente se usa para enviar datos a través de conexiones de marcación o punto a punto dedicadas entre un cliente de marcación y un NAS. El protocolo PPP tiene tres componentes principales:

- Encapsulamiento, a través de la cual el protocolo PPP permite la multiplexación de diferentes protocolos de la capa de red operar sobre el mismo enlace.
- Un Protocolo de Control de Enlace (Link Control Protocol [LCP]) a través del cual se establece, configura y prueba la conexión PPO.
- Una familia de protocolos de control de red (Network Control Protocol [NCP]), los cuales alivian los problemas que surgen en enlaces punto a punto con la familia actual de protocolos.

2.2.8.2 Protocolo de Túnel Punto a Punto (PPTP)

Historia del Protocolo de Túnel Punto a Punto.

En junio de 1996 un grupo de trabajo conformado por compañías miembros entre las que se incluye Microsoft Corporation, Ascend Communications, 3Com/PrimaryAccess, ECI Telematics y US Robotics (ahora 3Com) presentaron un proyecto ante la IETF el mismo que está documentado en la RFC preliminar. El protocolo de túnel de punto a punto es un protocolo de Nivel 2 que encapsula tramas del PPP en datagramas IP para la transmisión sobre una red IP como por ejemplo el Internet, de esta manera permite la realización de transferencias seguras desde clientes remotos a servidores ubicados en redes privadas.

En la Figura 2.2.15 se puede observar un escenario típico donde opera el protocolo PPTP: el cliente de marcación establecerá una conexión dial-up con el NAS del proveedor; establecida la conexión, el cliente de marcación establecerá una segunda conexión ahora con el servidor PPTP ubicado en la red privada. El servidor PPTP es el servidor intermediario de la conexión establecida cuya función será recibir los datos del cliente externo y transmitirlos al destino en la red privada.

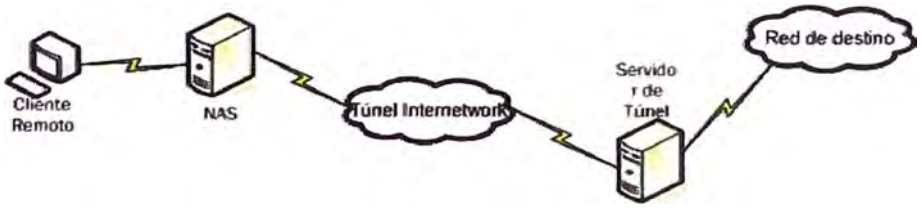


Figura 2.2.15 Escenario típico donde opera PPTP [8]

2.2.8.3 Protocolo de envío de capa 2 (L2F)

L2F, una tecnología propuesta por Cisco, protocolo cuyo objetivo es proporcionar un mecanismo de transporte de tramas a nivel de enlace. L2F permite que los servidores de acceso de marcación incluyan el tráfico de marcación en el PPP y lo transmitan sobre enlaces WAN hacia un servidor L2F (un ruteador). El servidor L2F envuelve entonces los paquetes y los inyecta en la red. A diferencia del PPTP y L2TP, L2F no tiene un cliente definido. Entre las principales ventajas que se pueden destacar del protocolo L2F se pueden mencionar: soporte multiprotocolo, multiplexación de múltiples sesiones remotas disminuyendo el número de túneles abiertos en un momento dado, gestión dinámica de los túneles por la cual los recursos de los servidores de acceso a la red se minimizan al iniciar los túneles únicamente cuando existe tráfico de usuario, L2F evita problemas de duplicidad debido al mantenimiento de un número de secuencia de las sesiones multiplexadas.

2.2.8.4 Protocolo de túnel de capa 2 (L2TP)

El protocolo de túnel de capa 2 es un protocolo que encapsula las tramas del PPP que se enviarán sobre redes IP, X.25, FrameRelay o ATM y combina las mejores funciones de los protocolos PPTP y L2F, los túneles L2TP pueden llevarse a cabo en redes públicas IP o no. En L2TP se crea el túnel mediante mensajes L2TP y utiliza UDP para enviar tramas del PPP encapsuladas del L2TP como los datos enviados por el túnel, las cargas útiles de las tramas encapsuladas PPP pueden encriptarse o comprimirse.

A pesar que PPTP y L2TP utilizan PPP para proporcionar un encapsulamiento inicial a los datos y luego incluir encabezados adicionales para transportarlos a través de la red y ser protocolos similares se pueden distinguir las siguientes diferencias:

- En PPTP se requiere que la red sea IP, en L2TP requiere sólo que los medios del túnel proporcionen una conectividad punto a punto orientada a paquetes: L2TP sobre IP, circuitos virtuales (PVCs), circuitos virtuales X.25, FrameRelay o ATM.
- PPTP soporta sólo un túnel único entre dos puntos, L2TP permite el uso de varios túneles entre puntos terminales.
- PPTP no proporciona autenticación de túnel, L2TP sí.

2.2.8.5 Protocolo de seguridad IPsec

El protocolo de Seguridad de Internet IPSec es un protocolo de capa 3 desarrollado por la IETF y definido en una serie de RFCs especialmente 1825, 1826, 1827, 2401-2402 mediante el cual se da soporte a la transferencia protegida de datos de extremo a extremo a través de una red IP.

Características de IPSec:

- Ipsec es un mecanismo de seguridad para transmitir datos a través de redes IP

pero asegurando confidencialidad, integridad autenticación de los datos sobre redes no protegidas como el Internet.

- IPsec actúa sobre la capa de red protegiendo y autentificando paquetes IP entre equipos IPsec pares.
- Es un estándar de capa 3 que provee confidencialidad, autenticación, integridad de los datos, replay detection.

2.2.9 BENEFICIOS DE UNA VPN

La implementación de una red VPN trae consigo algunos beneficios para las empresas entre los cuales se puede citar:

- Reducción de costos operacionales
- Simplificación de la de la topología de red.
- Alta seguridad mediante la utilización de algoritmos complejos de autenticación, encriptación, etc.
- La Asociación de Seguridad (SA) es el establecimiento de seguridad de la información entre dos entidades de la red para lograr una comunicación segura. Un SA puede incluir llaves criptográficas, certificados digitales, etc.
- Escalabilidad de la red.
- Seguridad, fiabilidad, administración de la red menos compleja.
- Entre otras.

2.3 REDES PRIVADAS VIRTUALES BASADAS EN LA TECNOLOGIA (MPLS-VPN)

Las redes privadas virtuales MPLS o MPLS VPN es una de las aplicaciones e implementaciones más populares de la tecnología MPLS. En la actualidad proveedores de servicios han optado por la migración de sus tradicionales redes FrameRelay y ATM a redes MPLS VPN.

MPLS VPN sigue teniendo un creciente interés dentro de la industria de las telecomunicaciones donde las grandes empresas lo ven como el próximo paso en el diseño de la red. La implementación y uso de estas redes puede proporcionar a los proveedores de servicios escalabilidad y facilitar a la vez el funcionamiento y administración de la red.

2.3.1 MPLS VPN

Como se ha mencionado en el transcurso del estudio, las redes privadas virtuales han existido antes del surgimiento de MPLS y las implementaciones más populares han sido a través de FrameRelay y ATM.

Ahora bien, las MPLS VPN a breves rasgos estudiada en la sección 2.2.7.3 es un ejemplo del modelo peer-to-peer altamente escalable, que combina las mejores características de una overlay VPN y una peer-to-peer VPN:

- Los PE routers participan en el enrutamiento del cliente lo cual garantiza y un óptimo ruteo entre los sitios y fácil provisionamiento.
- Los PE routers tienen la posibilidad de transportar un grupo separado de rutas para cada cliente emulando un PE dedicado. Los clientes pueden manejar el mismo espacio de direcciones.

Existen dos tipos de VPN que pueden ser implementadas a través de MPLS:

- MPLS VPN de capa 2 (MPLS L2 VPN): también conocidas como VPNs Martini/Kompella permiten la conectividad de capa 2 a través de una estructura MPLS.
- MPLS VPN de capa 3(MPLS L3 VPN): también conocidas como VPNs BGP MPLS usan las extensiones del protocolo de enrutamiento BGP para interconectar lugares remotos.

Modelo MPLS VPN

Similar a la terminología y dispositivos que se diferencian en una VPN común, una MPLS VPN también está conformada por un PE router, dispositivo de borde el mismo que tiene una conexión directa con el dispositivo de borde del cliente CE router de capa 3. El P router es un dispositivo que no tiene conexión directa con los routers del cliente y el router del cliente ó C router con el PE router (Figura 2.3.1).

En la Implementación de MPLS VPN:

Cuando se realiza una implementación MPLS VPN los routers P y PE deben correr MPLS de tal manera que puedan distribuir y enviar etiquetas entre ellos mientras que el CE router no necesita correr MPLS.

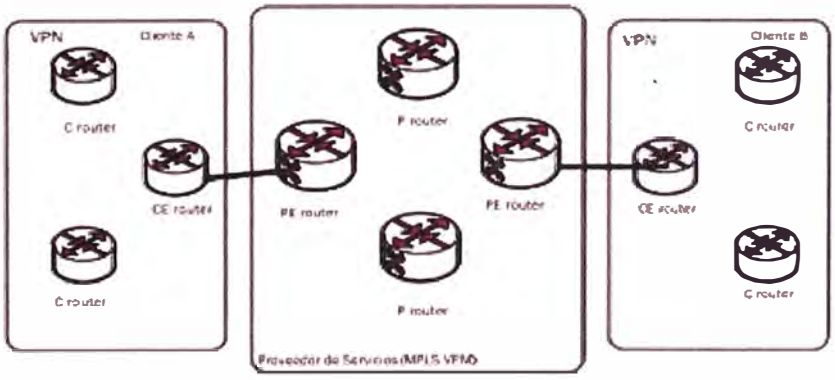


Figura 2.3.1 Terminología de dispositivos en la red MPLS VPN [8]

Se deben tener algunas consideraciones [2]:

- Los routers CE y PE interactúan a nivel de capa 3 por tanto necesitan correr un protocolo de enrutamiento dinámico o estático entre ellos.
- El CE router tiene únicamente un par fuera del sitio VPN el mismo que es el PE router. No puede tener otro par CE router de otro sitio VPN a través de la red del proveedor.

A través de MPLS, donde los paquetes IP son etiquetados en la red del proveedor de servicios para realizar una VPN por cada cliente. En este caso los P routers no necesitan corren BGP y tampoco tener la tabla de enrutamiento de los clientes, los routers VPN son únicamente conocidos por los PE routers es decir por los routers de borde en la red MPLS VPN, lo cual hace de MPLS VPN una solución escalable.

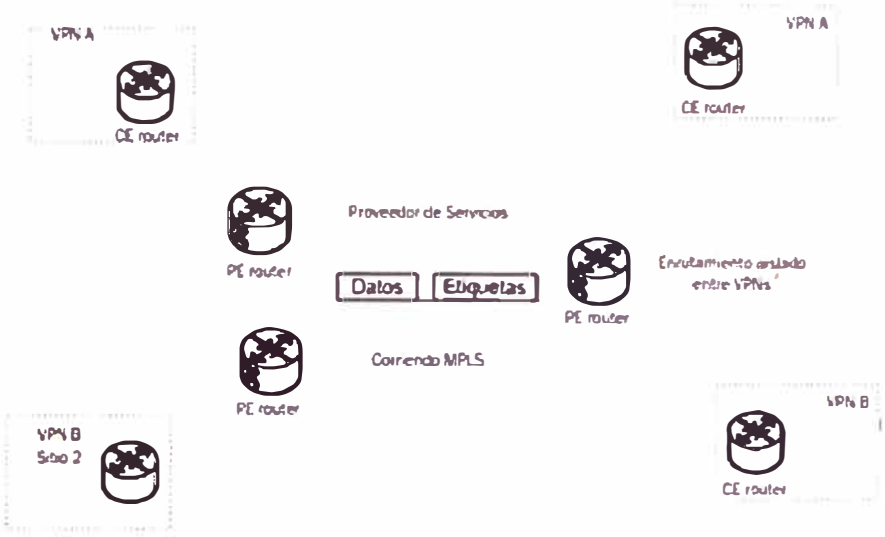


Figura 2.3.2 Modelo MPLS VPN [8]

En la Figura 2.3.2 se observa la interconexión que brinda el proveedor de servicios.

2.3.2 ARQUITECTURA MPLS VPN

Para lograr entender la arquitectura MPLS VPN es necesario estudiar cada uno de los bloques que conformar un PE router (ver Figura 2.3.3): Virtual Routing Forwarding (VRF), route distinguisher (RD), route targets (RT), propagación de rutas a través de Multi protocol BGP y reenvío de paquetes etiquetados [2].

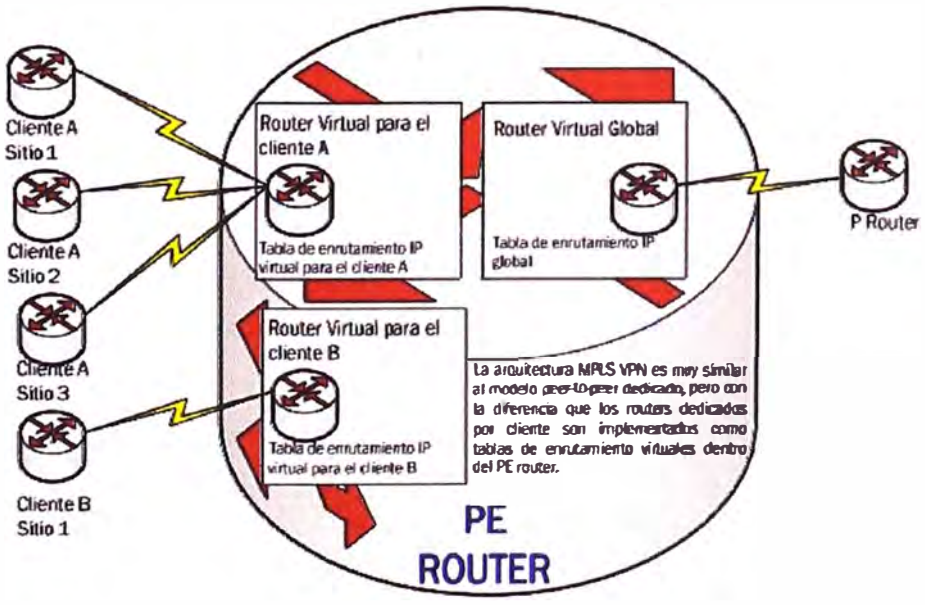


Figura 2.3.3 Arquitectura de un PE [10]

2.3.2.1 Virtual Routing Forwarding (VRF)

Se puede observar en la Figura 2.3.3 el PE router almacena una tabla de enrutamiento global y adicionalmente una tabla de enrutamiento separada y privada por cada VPN conectada al PE la cual se denomina tabla de enrutamiento VRF. Las tablas de enrutamiento VRF están en adición a la tabla de enrutamiento y reenvío global usada para tráfico no perteneciente a la VPN y contienen rutas de destino de los sitios locales y remotos de los clientes. En este escenario, la interfaz (física ó lógica) del PE router conectada al CE router puede pertenecer a una sola VRF, por tanto los paquetes IP recibidos en una interfaz VRF son identificados inequívocamente como pertenecientes a esa VRF.

2.3.2.2 Route Distinguisher (RD)

El protocolo BGP cumple con las características como protocolo de enrutamiento para transportar rutas VPN a través de la red del proveedor de servicios, BGP transporta prefijos IPv4 los mismos que deben ser únicos. Al ser así, en el caso de que los clientes tuviesen overlapping de direcciones IP, el enrutamiento podría ser erróneo. Para resolver este problema surge el concepto de Route Distinguisher a través del cual se logra hacer los prefijos IPv4 únicos y cuya combinación (IPv4 y RDs) es conocida como prefijo vpnv4. Así mismo para transportar los prefijos vpnv4 entre los PE routers es necesario el protocolo MP-BGP.

2.3.2.3 Route Targets (RT)

A través de la utilización de prefijos RD se identifica la pertenencia a una VPN pero la comunicación entre los sitios de diferentes VPNs no es posible. Siendo así, los route targets (RTs) fueron introducidos en la arquitectura MPLS con la finalidad de soportar complejas topologías de VPNs donde los sitios de los clientes pueden participar en más de una VPN. Los route targets son atributos adicionales añadidos a las rutas VPNv4 BGP con lo cual se indica pertenencia a una VPN. Para codificar dichos atributos se hace uso de comunidades extendidas de BGP las mismas que transportan los principales atributos.

Entre las características principales de un RT se pueden mencionar:

- Uno o más RTs pueden ser añadidos a la misma ruta.
- El mismo RT puede ser agregado a todas las rutas de un sitio en particular ó RTs diferentes pueden ser añadidos a cada ruta.
- En un sistema autónomo (AS) están habilitadas 232 RTs.

Los RTs pueden trabajar de dos maneras [9]:

- Export RT, identifican la pertenencia a una VPN y va adjunta a la ruta del cliente cuando ha sido convertida en una ruta VPNv4.

- Import RT, asociada con cada tabla de enrutamiento virtual y selecciona las rutas que van a ser insertadas en la VRF.

Tanto las Export RTs e Import RTs son el bloque central de las VPN debido a que la utilización de las mismas expresan las políticas que determinan la conectividad entre los sitios de los clientes.

2.3.2.4 Modelo de Ruteo en las MPLS VPNs

Según lo estudiado, las tablas VRF permiten separar las rutas de los clientes en el PE router, ahora bien la pregunta es cómo se transportan los prefijos a través de la red de proveedor de servicios y como los PE router reenvían los paquetes originados en la red del cliente.

Los requerimientos de enrutamiento en las redes MPLS VPN se resumen en tres puntos [9]:

- Los CE routers deben correr un software de enrutamiento IP estándar.
- Los routers PE soportan servicios de MPLS VPNs y enrutamiento de Internet.
- Finalmente los routers P no tienes rutas VPN.

Enrutamiento en la MPLS VPN: CE router

Desde el punto de vista de un CE router los PE routers corren son como cualquier otro router en la C-Network. Corren un protocolo estándar de enrutamiento IP: eBGP, OSPF,RIPv2, EIGRP y rutas estáticas. E intercambian updates con el PE router.

Enrutamiento en la MPLS VPN: PE router

El PE router intercambia rutas entre el CE router, P router y otros PE routers. Rutas de VPNs con los CE routers a través de protocolos de enrutamiento (mencionados anteriormente), rutas de core con los P y PE routers a través de IGP de core, y rutas VPNv4 con otros PE routers a través de sesiones MP-iBGP12.

Enrutamiento en la MPLS VPN: P router

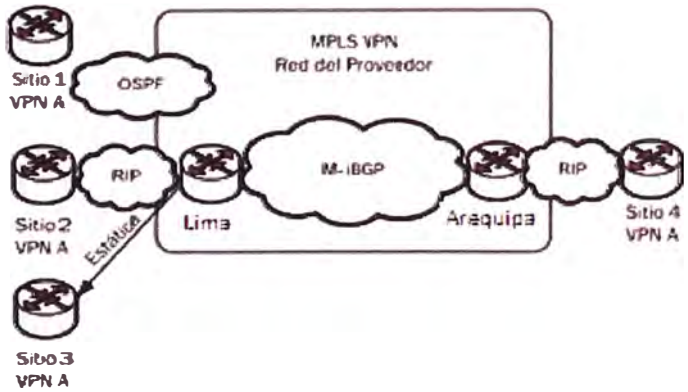


Figura 2.3.4 Protocolos de enrutamiento levantados en entre los dispositivos MPLS [1]

Los P routers no participan en el enrutamiento de las MPLS VPN y por tanto no transportan rutas VPN. Corren un IGP con los PE routers e intercambian información

global acerca de subredes (Figura 2.3.4).

Flujo de actualizaciones o updates:

En la Figura 2.3.5, se puede observar de manera global y como ejemplo la propagación de rutas en una red MPLS VPN.

Donde,

1. Los PE routers reciben rutas IPv4 desde el CE router a través de un IGP (Interior Gateway Protocol) o a través de un BGP externo (eBGP).
2. Las rutas IPv4 del sitio VPN son insertadas en la tabla VRF.
3. Un RD es añadido a la ruta IPv4 haciéndola una ruta VPNv4.
4. El PE router exporta las rutas VPNv4 a través de MP-BGP al PE de destino.
5. En el PE de destino remueve los RDs de la ruta VPNv4 y envía al CE router un update IPv4 a través de un protocolo IGP o eBGP.
6. La distribución de rutas hacia los CE routers es determinado por las comunidades BGP. Estas comunidades identifican las rutas del CE usando los RTs y el SOO (opcional).

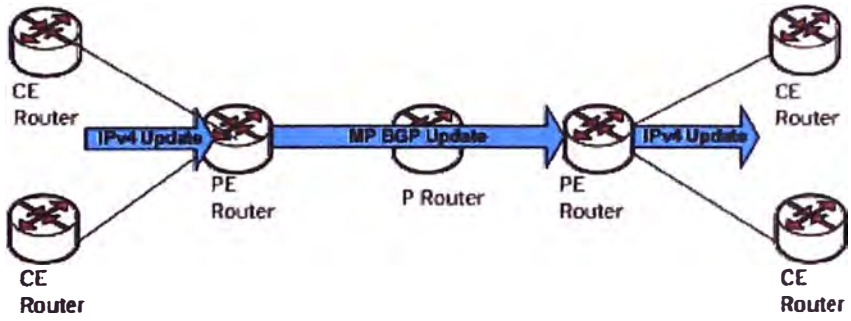


Figura 2.3.5 Flujo de updates de extremo a extremo [1]

Un update MP-BGP contiene lo siguiente [9]:

- Dirección VPNv4.
- Comunidades extendidas (route targets, opcional SOO).
- Etiquetas usadas por el envío de paquetes VPN.

2.3.2.5 Envío de Paquetes a través del Backbone MPLS VPN

Como se estudió en secciones anteriores, cuando un paquete IP ingresa al backbone MPLS VPN a través del PE router, un prefijo de 64 bits es añadido al paquete y esto lo hace único. Dentro del backbone MPLS VPN, es necesario también que el paquete sea singularmente reconocible.

Con la introducción de MPLS esta función es posible, cada paquete VPN es etiquetado por el PE router de ingreso y viaja a través de los routers donde dicha etiqueta es conmutada por otra hasta finalmente llegar al PE router de salida. A través de esta función de conmutación los routers no ven el paquete en sí sino su etiqueta.

El protocolo de distribución de etiqueta (Label Distribution Protocol [LDP]) es el camino más común y utilizado en este caso. LDP es configurado entre el P y PE routers donde todo el tráfico es etiquetado-conmutado entre ellos.

El envío de paquetes se lo puede analizar de la siguiente manera [2]:

El PE router debería etiquetar el paquete VPN con una etiqueta LDP para el router PE saliente y enviar los paquetes etiquetados a través del backbone MPLS. Los routers P realizan conmutación de etiquetas, y el paquete alcanza al router PE de salida Sin embargo, el router de salida no conoce cual VRF usar para el paquete conmutado y por tanto el paquete es eliminado.

Penultimate hop Popping en MPLS:

En un escenario MPLS el LSR de salida tiene dos funciones realizar una acción POP es decir remover la etiqueta y leer la cabecera IP para enviar el paquete fuera del dominio. Llevar a cabo estas dos acciones significa reducir el desempeño del nodo y puede incrementar la complejidad del hardware significantemente. Siendo así el concepto de Penultimate hop Popping fue introducido en la arquitectura MPLS de tal manera de resolver ambos problemas (Figura 2.3.6).

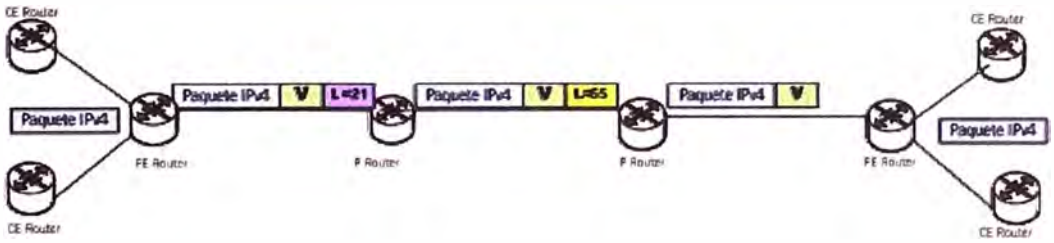


Figura 2.3.6 MPLS VPN Penultimate Hop Popping [1]

Penultimate hop Popping en VPN:

En las MPLS VPN, penultimate hop popping sobre la IGP label puede ser realizado sobre el último P router. El PE router realiza un lookup sobre la etiqueta de VPN o BGP label y envía el paquete al CE router correspondiente.

2.3.3 TOPOLOGIAS MPLS VPN

Dependiendo de las necesidades y requerimientos del diseño de la red, existe una gran variedad de topologías que pueden ser implementadas a través de la arquitectura MPLS VPN pero en la actualidad existen topologías que son mayormente usadas [10]. Cabe recalcar que cada una de estas topologías/modelos de conectividad VPN, son posibles debido a la utilización de RTs.

2.3.3.1 Topología Full Mesh MPLS VPN

En la topología full mesh todos los sitios de diferentes VPN pueden comunicarse directamente entre sí. En este tipo de conectividad un RT singular para importar y exportar políticas a todos los sitios.

2.3.3.2 Servicios Centrales MPLS VPN

Una de las topologías comúnmente implementadas en la tecnología MPLS VPN es la de servicios centrales VPN (Figura 2.3.7).

Características

- Los clientes necesitan acceder a servidores centrales.
- Los servidores tienen la posibilidad de comunicarse entre ellos.
- Los clientes pueden comunicarse con todos los servidores pero no entre ellos.

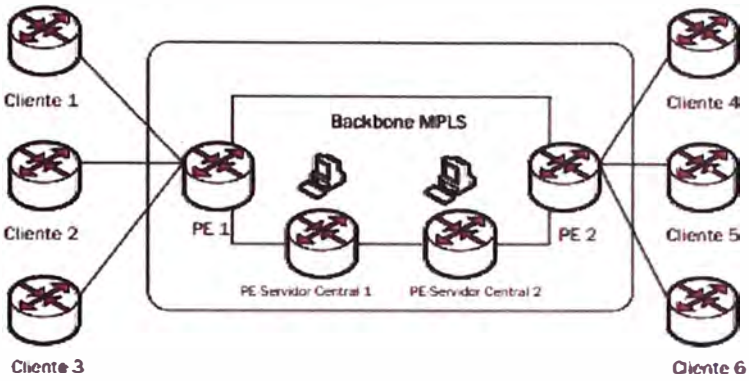


Figura 2.3.7 Topología de Servicios Centrales MPLS VPN [3]

- Las rutas de los clientes necesitan ser exportadas a un server site.
- Las rutas del servidor necesitan ser exportadas a los clientes y server sites.
- Las rutas no son intercambiadas entre los sitios de los clientes.
- El cliente VRF contiene las rutas del servidor y por tanto los clientes pueden hablar con los servidores.
- El servidor VRF contiene rutas de los clientes por tanto los servidores pueden hablar con los clientes.
- El cliente VRF no contiene rutas de otros clientes por tanto los clientes no pueden comunicarse entre sí.

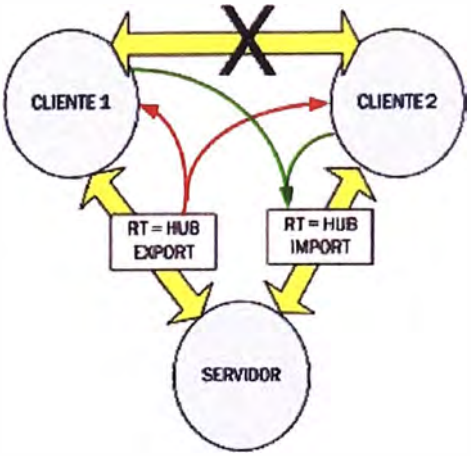


Figura 2.3.8 Enrutamiento en la MPLS VPN de servicios centrales [10]

Basados en dichas características, se puede diferenciar algunos de los requerimientos de

conectividad de una VPN de servicios centrales, siendo así se deben tener las siguientes consideraciones para configurar el sitio del cliente y el server site (Figura 2.3.8).

Sitio del cliente:

- Una VRF por cada tipo de servicio diferente.
- Un RD único por cada tipo de servicio diferente.
- Las rutas exportadas e importadas con RT del mismo valor por cada sitio del cliente.
- Rutas exportadas con un RT asociado con el server site.

Server Sites:

- Una VRF por cada tipo de servicio diferente.
- Un RD único por cada tipo de servicio diferente.
- Las rutas exportadas e importadas con RT del mismo valor por cada sitio del cliente.
- Las rutas exportadas del server site con un RT (servidor a cliente).
- Las rutas importadas con RT en el servidor VRF.

2.3.3.3 Modelo Overlapping MPLS VPN

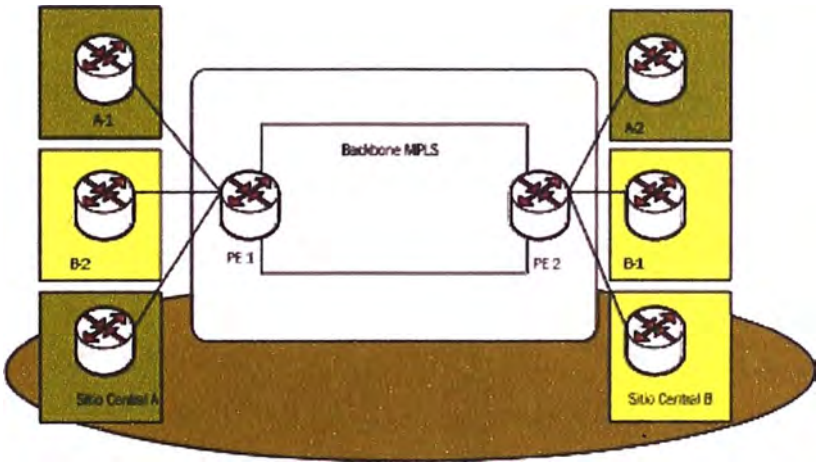


Figura 2.3.9 Topología Overlapping MPLS VPN [10]

Un modelo overlapping VPN surge de la integración de una extranet e intranet VPN, cuando se provee conectividad entre segmentos de dos VPNs (Figura 2.3.9).

Características:

- Los sitios que participan en más de una VPN importan y exportan rutas con RTs desde cualquier VPN en las cuales ellos están participando.
- Los sitios overlapping VPN son configurados con una VRF del mismo RD para un grupo de sitios que pertenecen a la misma VPN. Los RTs son configurados basados en la pertenencia de VPN de cada sitio.

2.3.3.4 Redefinición de una VPN

La arquitectura MPLS ha permitido el diseño e implementación de modelos complejos de VPN con lo cual su concepto tradicional comienza cada vez más a ser

obsoleto [9].

Se hace necesario entonces redefinir su concepto. Por tanto una VPN es una colección de sitios que comparten información de enrutamiento en común donde un sitio puede ser parte de diferentes VPNs y las diferentes topologías complejas pueden ser soportadas por múltiples tablas de enrutamiento virtual sobre los PE routers.

Todo ello conlleva a optimización de recursos físicos, mayor facilidad de administración de la red y amplia escalabilidad.

2.3.4 BENEFICIOS DE UNA IMPLEMENTACION MPLS VPN

La implementación de MPLS VPN ofrece a los proveedores de servicios una serie de ventajas y a su vez ayuda a la creación de nuevos servicios.

Los beneficios que resultan de una implementación VPN se pueden resumir en los siguientes puntos:

Seguridad

A través de la configuración de las tablas virtuales en el PE router es posible el aislamiento del tráfico entre VPNs donde el PE router es el único en tener conocimiento acerca de cada VPN que está configurada en el backbone.

Adicionalmente la utilización de etiquetas para distinguir los paquetes IP asegura que los paquetes serán entregados a la VPN correcta.

Escalabilidad de la red

MPLS VPN permite al proveedor de servicios la implementación de múltiples VPNs usando el mismo core de la red, donde la Routing Information Base (RIB) de la VPN es independiente de la tabla RIB del core haciendo de MPLS VPN más escalable.

La arquitectura e inteligencia de la red está implementada básicamente en los PE routers los mismos que mantienen una RIB por cada VPN permitiendo la implementación de VPNs que soportan overlapping (mismo espacio de direcciones) en el mismo core.

Extranets e Intranets

A diferencia de las implementaciones tradicionales de extranets e intranets mediante el uso de políticas de enrutamiento cuya administración se convierte en algo bastante complejo, mediante MPLS VPN se puede hacer de una manera bastante simple y rápida.

Otras

MPLS VPN permite al cliente "endosar" el enrutamiento de sus sitios al proveedor de servicios y al proveedor de servicios ofrecer servicios de valor agregado a sus clientes.

MPLS VPN mantiene un backbone virtual por cada cliente ya que permite en la misma infraestructura levantar múltiples clientes VPN.

La implementación de túneles PE-PE MPLS son usados para transportar tráfico para múltiples VPN y múltiples aplicaciones. En este contexto es una de las propiedades más poderosas y posibilita: enviar tráfico a direcciones que no son conocidas en el medio de la red, identificar tráfico perteneciente a una VPN en particular en el punto de salida de la red del proveedor de servicios y proveer protección fácil y a bajo costo.

CAPITULO III
METODOLOGIA PARA LA SOLUCIÓN DEL PROBLEMA

3.1 Análisis del problema

EL problema de ingeniería es la implementación de una red a nivel nacional que debiera unir todas las sedes de la institución gubernamental en una sola gran intranet dando una calidad de servicio óptimo en todas sus sedes y cubrir las necesidades del capítulo 1.3 "Formulación del problema de Ingeniería".

3.2 Alternativas de solución

En la Tabla 3.1 ubicado en el Anexo D se muestra los anchos de banda y las principales características de las tecnologías de comunicaciones que existen en nuestro país y que son brindadas por las principales operadoras de telecomunicaciones (Claro y Telefónica). Estas tecnologías nos permitirán la interconexión entre sedes.

De acuerdo a la tabla 3.1 ubicado en el Anexo D podemos ver que la tecnología más apropiada para poder transmitirla información de las diversas aplicaciones en la intranet y extranet, manteniendo niveles de seguridad deseados son las Redes Privadas Virtuales (RPVs).

En la Tabla 3.2 ubicado en el Anexo D se expone las principales características del servicio de RPV que son brindadas por TELEFÓNICA y CLARO.

El costo de conexión a la red de transporte IPVPN-MPLS de Claro y Telefónica es relativamente igual.

3.3 Solución del problema

De acuerdo a la Tabla 3.2 ubicado en el Anexo D podemos observar que para poder brindar una solución a los requerimientos de la institución Gubernamental mostrados en el Capítulo 1.3 "Formulación del problema de Ingeniería", se requiere una infraestructura de red IPVNP-MPLS.

En la Figura 3.1 muestra el diseño de conexión a la nube IPVPN MPLS que los proveedores de IPVPN MPLS ofertan. La nube llega a la sede con fibra directo a un modem/router el cual realiza la conversión del cable de Fibra óptica a Cable UTP y el ruteo de la información de ahí se conecta directo a un Switch el cual separa la información de voz y data, la información que de datos pasa a la Lan de la institución Gubernamental cada sede tendría el mismo diseño de conexión a la red IPVPN MPLS.

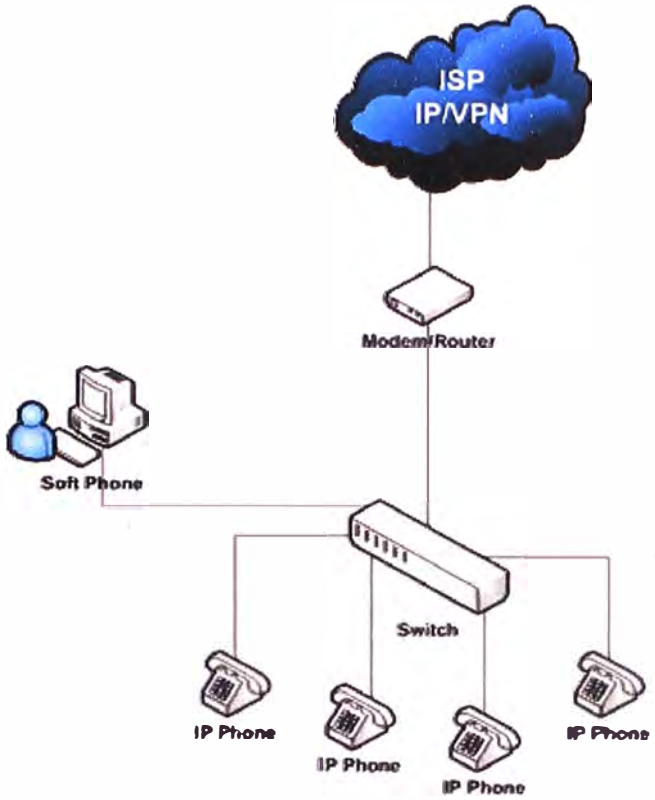


Figura 3.1 Elaborado - Diseño presentado por el proveedor de IPVPN-MPLS

En la Figura 3.2 muestra el diseño de conexión a la nube IPVPN MPLS de acuerdo a lo requerido por la institución Gubernamental.

La Institución Gubernamental cuenta con dos tipos de servicios: Aplicaciones cliente/servidor y aplicaciones web, que son consumidas a nivel nacional a través de la red, para el diseño de la conexión a la nube IPVPN MPLS se debe considerar que las aplicaciones cliente/servidor consumen más recursos de red, por ello se ha separado en dos bloques para optimizar el rendimiento y consumir los recursos asignados, la aplicación cliente/servidor (A) y la aplicación web (C) consumirán el primer circuito de conexión IPVPN MPLS y la aplicación cliente/servidor (B) y la aplicación web (D) consumirán el segundo circuito de conexión IPVPN MPLS, el primer y el segundo circuito se encuentra configurados en alta disponibilidad, si uno de los circuitos falla por averías el otro circuito asumiría toda la carga de entrada y salida de información a la respectiva sede.

Los circuitos de conexión a la nube IPVPN MPLS esta constituido de un convert Fc a Utp, de un Router Cisco 3900 y un Switch Cisco 3750 cada circuito de conexión a la red IPVPN MPLS es independiente, el Switch Cisco 3750 llega a la Lan de la sede con puertos Utp para la conexión a todos equipos de la Intranet de la sede.

El balanceo de la carga entre los circuitos previene posible saturacion de la red entre sedes y la contunuidad de los servicios ante la falla de uno de los circuitos.

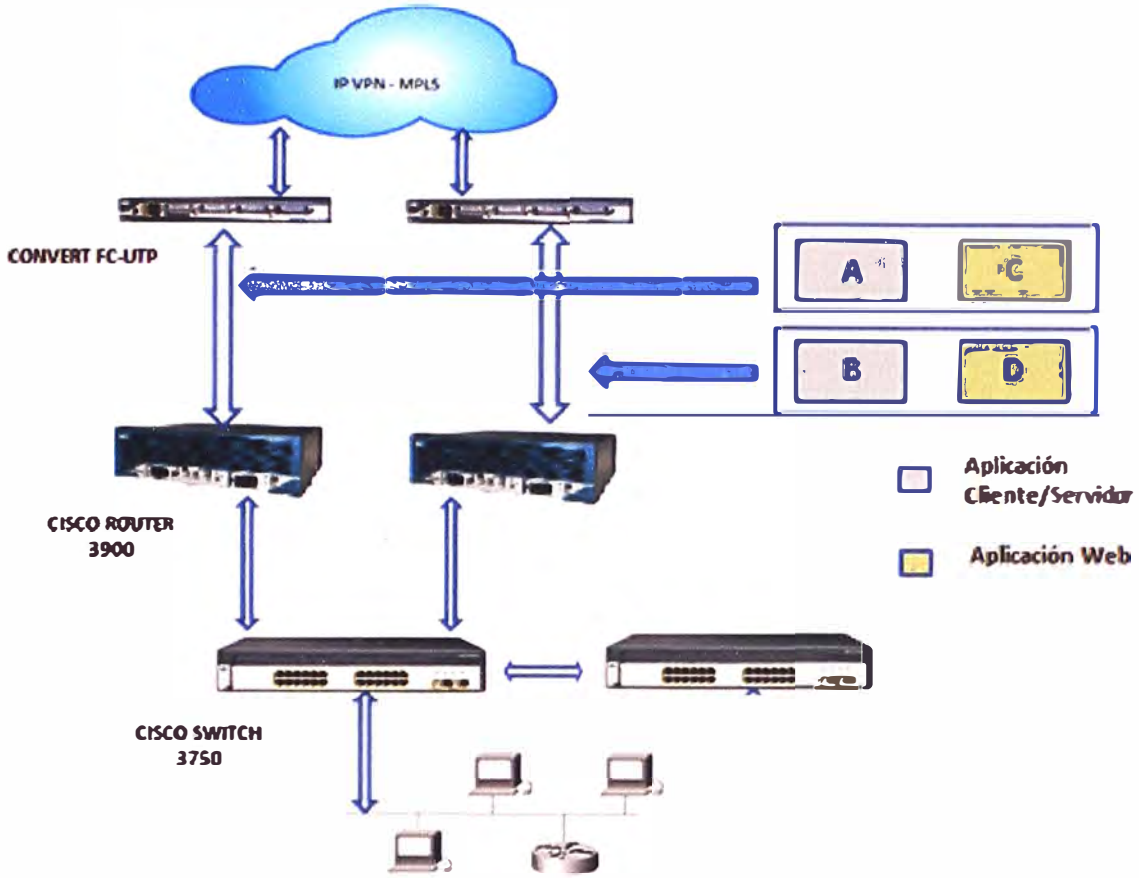


Figura 3.2 Elaborado - Diseño presentado por la Institución Gubernamental.

En la Figura 3.2 nos da una idea de cómo podemos optimizar el circuito backup que el proveedor nos entrega, el circuito backup que vendría hacer la contingencia en caso de que el circuito principal presentara algún falla en una diseño activo/pasivo, al optimizarlo lo llevamos aun diseño activo/activo cruzado reutilizando los recursos del circuito de backup como muestra la Figura 3.2.

3.4 Análisis de los requerimientos de la institución Gubernamental.

Cada uno de los puntos definidos en el capítulo 1.3 "Formulación del problema de ingeniería", serán analizados para demostrar que la red IPVPN-MPLS cumple con las condiciones solicitadas.

A.- Las sedes deben estar interconectadas con un ancho de banda adecuado de acuerdo al nivel de información que maneje y la zona geográfica donde se ubique.

Respuestas: Cada sede está configurada para navegar a través de la nube con un ancho de banda definido por el Tabla de la Figura 1.1 "sedes principales de la nube", con la posibilidad del cliente o usuario decida aumentar o disminuir dicho ancho de banda de acuerdo a su aumento o disminución de tráfico a través de la nube.

B.- Las sedes podrán compartir recursos entre ellas, la información que comparte será de acuerdo al ancho de banda que se le asigne a la sede y cada sede deberá mantener su distribución de Ips y la estructura de su LAN de cada sede deberá mantenerse Intacta.

Respuestas: Al formarse la nube IPVPN-MPLS todas las sedes se podrán ver unas con otras, como si estuvieran en una LAN, manteniendo su LAN interna de la sede intacta, conservando sus IPs y políticas de servicios.

C.- Las sedes podrán consumir recursos de otras sedes por medio de web service o información pública que ellas requieran mostrar.

Respuestas: Como todas las sedes pueden verse, la publicación de los web service será transparente, ya que se verían como si fuera una gran red LAN, dentro de la nube.

D.- Todas las sedes deben estar en una misma Intranet, en el cual todas las sedes pueden comunicarse, como si fuera una gran nube Gubernamental, esta Intranet debe estar aislada de otras redes externas y debe cumplir ciertas normas de seguridad.

Respuestas: Todas las sedes estarían interconectadas en una gran red (Intranet) y está aislada de otras redes, la nube IPVPN-MPLS-Gubernamental estará aislado de cualquier otra red IPVPN-MPLS existente en la nube, los paquetes de información que viajen en la nube estarán etiquetadas solo para que los nodos o sedes puedan interpretar dentro de la red IPVPN-MPLS-Gubernamental.

E.- Las sedes podrán consumir aplicaciones centralizadas de una sede hacia las otras, ya sea con aplicaciones cliente/servidor o por web service (servidor de aplicaciones) todo dentro una misma Intranet.

Respuestas: Como todas las sede se van a poder ver dentro una misma gran Lan (Intranet), los servidores que brinda servicios en una sede podrá ser consumidos por otra sede sin problema, al igual que las publicaciones por web service en una sede será consumida por cualquier otra sede.

F.- La Intranet debe permitir conexiones con otras redes externas, extranet y permitir la conexión a internet vía un tercer proveedor.

Respuesta: Todas las sedes están en una gran Lan (Intranet), esta red esta aisladas de otras redes IPVPN-MPLS que hay dentro de la nube y/o otra nube que hubiese, como por ejemplo la nube de internet. Pero puede conectarse por medio de un Tunel a otras redes y consumir recursos de estas redes externas (extranet), como la conexión de intemet publicada por otro proveedor.

G.- Las sedes deben acceder al Portal Corporativo vía la intranet para consumir recursos de los servicios privado del Gobierno que este brinde y este Portal Corporativos debe tener salida externa para sus servicios públicos, para que otras instituciones públicas o privadas requieran consumir por medio la extranet (ejemplo La Reniec, El Poder Judicial y El Banco Central de la Reserva, publican sus servicios públicos para que otras instituciones consuman sus recursos y ellos consumen servicios de otras instituciones).

Respuesta: El portal Corporativo estaría publicado dentro de la Intranet en la nube, para

que puedan ser consumidos por las sedes y tiene salida hacia fuera a través de internet y estar conectada a otras redes que están dentro o fuera la nube IPVPN-MPLS, para consuman sus servicios publicados o consumir recursos externos.

H.- Cada sede puede publicar servicios en la Intranet y también deberá poder consumir servicios de la misma intranet de otra sede.

Respuesta: Como todas las sedes se pueden ver dentro de la Intranet, los recursos publicados por una sede pueden ser consumidas por las otras sedes.

I.- La Infraestructura de las solución debe permitir crear grupos de trabajos entre las sedes, como sub redes dentro de la misma nube, donde los trabajos dentro de la sub nube sea comunes entre las sedes de la misma sub nube.

Respuesta: Como todas las sedes están dentro de una misma Intranet en un gran nube IPVPN-MPLS, dentro de la nube se pueden crear sub nubes entre un grupo de sedes, que tiene un trabajo en común, será como una sub nube privada para las sedes miembros, y pueden publicar sus trabajos a la gran nube.

J.- La infraestructura propuesta debe separar el empaquetado de información de voz y data, la voz debe tener mayor prioridad en la transferencia de paquetes, ambas formas deben considerarse críticos, no deben existir pérdidas de paquetes en la transferencia.

Respuesta: En las redes IPVPN-MPLS existe criterios de Calidad de servicio, los comunes son gold, silver y bronze, los más usados son gold y silver, gold es usado específicamente para voz (telefonía IP) y tiene mayor preferencia en las colas o transferencia, silver es usado específicamente para data tiene menor prioridad en las colas o transferencia, ambas son consideras a críticas, no existe perdidas de paquetes en ambos casos.

K.- En cada sede debe implementar conexión activa llamada principal y otra pasiva llamada backup, en caso que el principal tuviese problemas el backup tendría asumir la carga del principal sin problemas y así mantener la continuidad de los servicios.

Respuestas: Cada sede tendría dos circuitos de conexión a la nube IPVPN-MPLS, un circuito que será la principal que estará operativo con el ancho bando definido por el Tabla de la Figura 1.1 "sedes principales de la nube" y otro circuito que sería el backup que estaría en modo pasivo en espera que la principal tuviera problemas de conexión.

L.- Cada sede podría emitir videoconferencias hacia las demás sedes sin saturar o congestionar la nube propuesta.

Respuestas: Cada sede tendría su propio ancho de banda de acuerdo al Tabla de la Tabla 1.1 "sedes principales de la nube" este ancho de banda es independiente a la que se asigne a otra sede, los videoconferencia estaría en el servicio de calidad de datos silver, si es que llega a los umbrales el ancho de banda asignado, tomaría el ancho del

servicio gold evitando su saturación.

M.- La información Transferida debe tener niveles de seguridad en toda la nube propuesta, los paquetes no deben ser alterados a lo largo de la transferencia.

Respuestas: Los paquetes que ingresan a la nube son etiquetados con niveles de seguridad que se guardan en el paquete de datos esto evita que se pierdan los paquetes y nos da márgenes de seguridad en la transferencia de la información.

N.- La rapidez de transferencia de información en la nube debe estar garantizada, desde una sede hacia otro.

Respuestas: En la red IPVPN-MPLS son independiente los ancho de banda asignados a cada sede tanto ancho de banda del principal como la del backup.

O.- En la implementación de red o nube, se debe considerar que troncales principales de la red o nube deben ser de Fibra óptica en su mayoría, para tener una mayor eficiencia en la transferencia de información.

Respuestas: En la infraestructura de la IPVPN-MPLS los troncales principales están formados de Fibra óptica, para el óptimo rendimiento de las redes IPVPN-MPLS.

La infraestructura de red IPVPN-MPLS puede interconectar diversas sedes a nivel nacional debido a que existe una interconexión de red a nivel nacional con fibra óptica por parte del proveedor. En el anexo C Figura 3.4 nos muestra la cobertura de la Fibra óptica a nivel nacional, características de la Fibra óptica:

- Diámetro y peso reducidos lo que facilita su instalación.
- Excelente flexibilidad.
- Inmunidad a los ruidos eléctricos (interferencias).
- No existe diafonía (no hay inducción entre una fibra y otra).
- Bajas pérdidas, lo cual permite reducir la cantidad de estaciones repetidoras.
- Elevada capacidad de transmisión de la información.
- Estabilidad frente a variaciones de temperatura.
- Al no conducir electricidad no existe riesgo de incendios por arcos eléctricos

IPVPN MPLS es un servicio que garantiza el 100% de la velocidad contratada tanto de subida y bajada. Este servicio garantizara la comunicación entre sedes a nivel nacional la información se transmitan en forma rápida y segura con un ancho de banda ya definido.

En la Figura 3.3 podemos observar como seria la topología de red para una institución Gubernamental. En el cual se observa una red IPVPN-MPLS con dos sede unidas por una nube que llamaremos nube IPVPN-MPLS cada sede cuenta con un router (rourter CE) localmente que se conecta a la entrada de la nube IPVPN-MPLS a los routers de entrada (routers PE) que internamente se conecta con un enmallado de

routers (routers P) en la red interna de la nube IPVPN-MPLS, estos routers hacen posible las conexiones entre sedes y arman las redes virtuales necesarias para la transferencia de información.

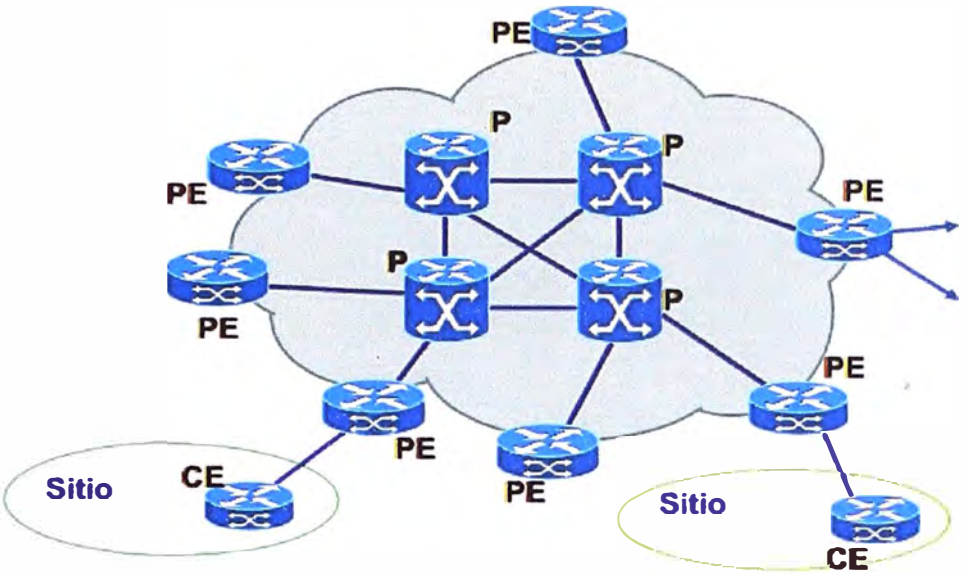


Figura 3.3 Topología de red [1]

El proveedor del servicio IPVPN-MPLS, debe permitir niveles de calidad de servicio a lo largo de toda su plataforma de red o nube y los niveles de servicios determinan tres tipos de tráfico, los cuales se basan en clases de servicio y estos son:

- Clase oro- telefonía IP
- Clase plata- datos críticos
- Clase bronce - datos no críticos

De acuerdo a esta clasificación de los servicios, la clase bronce es la clase que tiene menor prioridad, este nivel de servicio no es muy usado actualmente, básicamente es la clase que agrupa todo el tráfico que se dirige hacia el internet. En la clase plata se agrupa todo el tráfico destinado a los servidores de base de datos y servidores de aplicaciones para los sistemas centralizados cliente/servidor y web dentro de la intranet o nube. Y finalmente tenemos la clase oro, la cual tiene la más alta prioridad, en esta clase se agrupa todo el tráfico telefonía IP, esta clase debe cumplir las condiciones de ser los más pequeño posible para evitar congestionamiento con la clase de plata dentro de las buenas practicas esta clase es solo usada para transferencia de voz (telefonía IP).

Los equipos de comunicaciones que definen los niveles de la calidad de servicio y enrutamiento de los paquetes, se instalaran en las diversas sedes a nivel nacional son conocidos como enrutadores o routers. Telefónica usa los enrutadores de la marca Cisco debido a que es una marca reconocida internacionalmente. Estos equipos permitirán la conexión de todas las sedes a nivel nacional por la nube IPVPN-MPLS.

Los enrutadores Cisco configurados e instalados en cada una de las sedes institucionales deben garantizar la conexión a la nube IPVPN-MPLS y de ahí a sedes, cada sede podrá acceder a otra sede para consumir servicios y recursos que requiera.

IPVPN-MPLS al ser una red privada no está sujeta a los niveles de vulnerabilidad que si presenta nuestra infraestructura de red actual, de esta forma se garantizara la confiabilidad y seguridad de la información de una sede institucional hacia otra, con la rapidez necesaria.

3.5 Propuesta Técnica

De acuerdo al análisis de las propuestas de los proveedores la institución gubernamental requiere alquilar una infraestructura de red de un proveedor para interconectar con todas sus sedes.

El proveedor debe considerar:

1.- Entrega de una equipamiento en cada sede tal como indica en el Tabla 3.3 "Equipamiento en el sede - sitio"

Tabla 3.3 Equipamiento en el sede - sitio

Equipamiento	Nombre	Funcion
Routers Cisco 3900	Cisco-01	Router CE
	Cisco-02	Router CE
Switch Cisco 3570	switch-01	Switch -Lan
	switch-01	Switch -Lan
Convert FC-Utp	Convert-01	Convert FC-Utp
	Convert-01	Convert FC-Utp

Implementado de acuerdo al diseño de la Figura 3.2 "Diseño presentado por la Institución Gubernamental" en cada sede en el diseño existe redundancia a nivel del Router Cisco y Switch Cisco.

2.- Los dos (2) Routers CE tendría una configuración Activo-Activo Cruzado.

En los Routers CE (que están ubicados en las sede) deben estar activado el servicio HSRP (Hot Standby Router Protocol) que permita la alta disponibilidad entre los Routers. Para ello deben estar en la misma Vlan con conectividad en capa 2 por medio de un Switch Cisco 3750.

Cada servicio debe estar en una Vlan distinta para la Figura 3.2 "Diseño presentado por la Institución Gubernamental" existen los 4 servicios (A, B, C y D), los servicios (A y C) estaría activos en Router Cisco-01 y tienen como backup el Router Cisco-02 y los servicios (B y D) activos en Router Cisco-02 y como backup Cisco-01. El servicio se muestra al usuario con una sola IP virtual tal como indica el Tabla 3.4. En caso que fallara el Router Cisco-01 la Ip virtual que está asociada al IP del Router Cisco-01 se asociaría al Ip del Router-02, esto permitiría la continuidad del servicio a través del Ip virtual.

Tabla 3.4 Configuración e el Router CE, lado del Cliente.

Servicio	Vlan	Cisco Router 3900	Estado	IP en Router	IP Publico
A	Vlan-A	Cisco-01	Activo	192.168.202.21	172.168.202.20
		Cisco-02	Pasivo	192.168.202.22	
B	Vlan-B	Cisco-01	Pasivo	192.168.203.31	192.168.203.30
		Cisco-02	Activo	192.168.203.32	
C	Vlan-C	Cisco-01	Activo	192.168.204.41	172.168.204.40
		Cisco-02	Pasivo	192.168.204.42	
D	Vlan-D	Cisco-01	Pasivo	192.168.205.51	192.168.205.50
		Cisco-02	Activo	192.168.205.52	

En la Tabla 3.4 "Configuración e el Router CE, lado del Cliente" se detalla la configuración de los cuatro servicios (A, B, C y D).

3.- Los Routers CE y Routers PE se configuraría para que trabaje en capa 3, y los Router Ciscos P se configuraría para que trabajen a nivel de capa 2.5, los Router Cisco no debieran conocer las redes virtuales privadas, ellos solo deben manejar el etiquetado de los paquetes, capa 2.5 (capa de etiquetas).

4.- El Postor debiera cumplir u servicio 7x24 de toda la infraestructura de la red a nivel nacional que debe cubrir tanto a los equipos implementados en la sede como la red MPLS para garantizar la continuidad.

CAPITULO IV
ANALISIS Y PRESENTACION DE RESULTADOS

4.1 Objetivos

Los objetivos de este capítulo son:

1.- Analizar los tiempos de respuesta del proyecto sugerido y compararlo con los tiempos de respuesta del sistema actual.

2.- El análisis de los costos necesarios para la implantación de la infraestructura de red que interconectara las sedes de la institución Gubernamental.

3.- Los tiempos de Ejecución para la implantación y dejar operativo la infraestructura de red IPVPN-MPLS a nivel nacional, tiempos por sedes.

4.- El análisis de la rentabilidad socio-económica de la implantación de la infraestructura de red IPVPN-MPLS (Figura 4.1).

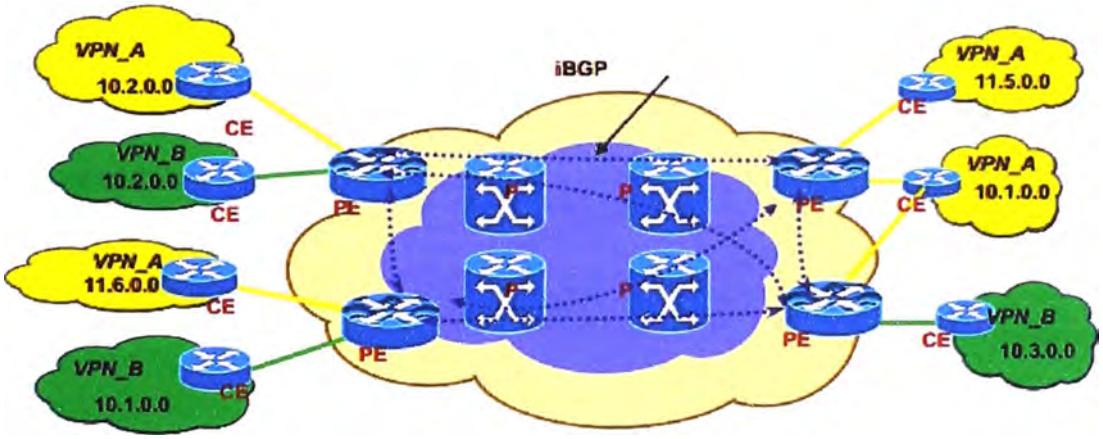


Figura 4.1 Topología de Red [1]

4.2 Análisis de los Tiempos de respuesta.

Al analizar los tiempos de respuesta en una demostración, se obtiene los siguientes resultados. En la Tabla 4.1 "Tiempos de respuesta por horas" se observa que los tiempos de respuesta con la infraestructura IPVPN MPLS son más rápido en comparación a la infraestructura actual, tener en cuenta que la institución tiene sus horas picos entre las 8-10 a.m. y 14-16 p.m. la conexión radio enlace que se tiene con algunas sedes y otras por internet hace que el tiempo de respuesta sea lento.

El tiempo de respuesta en las horas picos en el sistema actual es demasiado lento para que el usuario final, esto es un de los ítems que se desea mejorar.

Tabla 4.1 Tiempos de respuesta por horas

	Tiempos de Respuesta	
Horas(0-24)	sin IPVPN(seg)	con IPVPN(seg)
8-10	2.66	0.82
10-12	1.40	0.56
12-14	0.86	0.45
14-16	2.22	0.72
16-18	1.25	0.54

En la Tabla 4.2 "Tiempos de respuesta por Aplicación en horas pico" nos muestra el tiempo de respuesta en horas pico de las aplicaciones cliente/servidor (A) y (B) además de las aplicaciones web (C) y (D), la respuestas con el sistema actual son muy elevadas, para los usuarios finales se requiere optimizar estos tiempos.

Tabla 4.2 Tiempos de respuesta por Aplicación en horas pico.

	Tiempos de Respuesta (en horas pico)	
Aplicación	sin IPVPN(seg)	con IPVPN(seg)
App c/s (A)	2.52	0.86
App c/s (B)	2.68	0.89
App web (C)	1.85	0.70
App web (D)	1.22	0.66

4.3 Análisis de costos de la infraestructura.

El proyecto consta de la adquisición de una infraestructura de red a nivel nacional para interconectar todas las sedes, la adquisición de una infraestructura sería muy costoso y muy difícil de implementar, la solución IPVPN-MPS te permite alquilar redes virtuales para conectar sedes distantes y tenerlos todo como si fuera una gran Lan (dentro de una intranet), el proveedor alquilaría su infraestructura de acuerdo a lo solicitado por la institución Gubemamental y los equipos necesarios para la conexión a su red (la infraestructura de la nube IPVPN-MPLS) bajo un costo mensual y con servicio de soporte 7x24 en caso hubiera incidencias, en caso de averías de conexión tendría un plazo no más de 4 horas para dar solución el problema, manteniendo la continuidad de la solución de la infraestructura.

La infraestructura se entregaría como una entrega llave en mano y con una renovación de un año cada servicio.

En la Tabla 4.3 "Equipos necesarios para la conexión a la nube IPVPN-MPLS" cada sede estaría equipado de dos (2) routers Ciscos series 3900 y dos (2) convert FC a UTP y dos (2) switches Cisco 3570 para conexiones al red IPVPN MPLS, el proveedor implementaría todo el equipamiento, estos equipos estarían en la institución en calidad de préstamo hasta que termine el servicio de acceso a la red IPVPN MPLS y el proveedor debe brindar un servicio de soporte a estos equipos 7x24 en caso de alguna falla seria cambiado automáticamente.

Tabla 4.3 Equipos necesarios para la conexión a la nube IPVPN-MPLS

servicio / sede	Cantidad	Precio total ($.) Mensual	Precio Total ($.) Anual
Routers Cisco 3900	2		
Convert FC a UTP	2		
Switchs Cisco 3570	2		
Servicio de acceso a la red IPVPN-MPLS	2	1360,00	16320,00
	TOTAL ($)	1360,00	16320,00
	TOTAL (S/.)	3808,00	**45696,00**

El proveedor debe incluir un servicio de soporte 7x24 con un tiempo de respuesta y solución de 4 horas, desde que se reportó la incidencia, el proveedor es responsable de toda la nueva infraestructura de red, en el Anexo E se indican las características de los equipos que se usaran en la implementación de la red IPVPN-MPLS.

4.4 Tiempos de ejecución de la implantación de infraestructura de la red

El tiempo que demora la instalación de los equipos de comunicaciones en las sedes institucionales, que permitirá la interconexión entre las sedes, según el proveedor del servicio de IPVPN, puede durar aproximadamente 60 días, lo cual dependerá de las facilidades técnicas que se presenten en cada sede. El tiempo iniciaría después de la firma del contrato. Cabe destacar que dentro de la instalación de los equipos, están incluidos los routers Cisco para cada sede, estos routers son gestionados por el proveedor del servicio.

Tiempos solicitados por el proveedor, para la instalación y configuración en cada sede, que entraría en vigencia después de la firma del contrato.

Tiempos distribuidos por el provevedor:

- Recopilación de información de la red de la sede (15 días).
- Entrega e instalación de los equipos para interconexión con la nube (15 días).
- Configuración y ajustes de la interconexión a la nube (15 días).
- Una ventana de pruebas y testing y resolución de incidencias (15 días).

4.5 Análisis de la rentabilidad socioeconómica de la implantación de la red IPVPN–MPLS

Como se observa en la parte de análisis de costos, vemos que el costo total proyectado a un año sería de $16,320 dólares por sede.

Se debe considerar las limitaciones de la infraestructura red actual para cubrir los servicios vigentes a través de la red.

Existen servicios nuevos para ser implementados en la institución Gubemamental,

estos servicios nacen de un proyecto de implantación y cuentan con un presupuesto de implantación y mantenimiento, estos nuevos proyectos que toma como base que todas las sedes deben estar interconectadas para que consuman sus servicios en forma eficientes, en tal motivo estos proyectos de servicios nuevos separan un parte de su presupuesto para el proyecto de interconexión de las sedes institucionales, con el objetivo que los servicio nuevos del proyecto funcionen sin problema alguno.

De acuerdo al Tabla 4.4 "Presupuestos separados de proyectos de servicios nuevos" los presupuesto de los proyectos nuevos que se van implementando en la institución Gubernamental, que necesitan una infraestructura de red que permita la interconexión de las sedes institucional, separan una parte de su presupuesto para mantener la nube IPVPN-MPLS, cada proyecto nuevo a implementar viene con su propio presupuesto.

La arquitectura de los servicios de una u otra forma requiere que las sedes estén interconectadas para que puedan consumir los servicios centralizados o que están dentro de la intranet, la necesidad de una infraestructura de red que pueda unir las sedes institucionales es necesaria para cubrir los servicios que están implantados en las sedes y desde otras sedes.

Tabla 4.4 Presupuestos separados de proyectos de servicios nuevos

Proyectos nuevos	% del presupuesto separado	Presupuesto Separado Mensual ($.)	Presupuesto Separado Anual ($.)
Servicio Web CEJ a nivel nacional	30%	720,00	8640,00
Servicio Web MSIAP a nivel mundial	25%	620,00	7440,00
Servicio Web notificaciones de expedientes	25%	775,00	9300,00
Servicio Web tramite de antecedentes penales	30%	640,00	7680,00

CONCLUSIONES Y RECOMENDACIONES

1.- La Arquitectura IPVPN MPLS es la arquitectura adecuada para la institución por su amplia cobertura a nivel nacional, por su bajo costo en comparación con otras tecnologías y su óptimo nivel de seguridad.

2.- El diseño para la interconexión con la red IPVPN MPLS es la más óptima utiliza los dos circuitos principal y backup, balancea la carga, existe una continuidad de servicios ante la falla de alguno de los circuitos.

3.- La tecnología IPVPN MPLS cumple todos los requerimientos mínimos que la Institución Gubernamental ha solicitado para la interconexión de sus sedes a nivel nacional.

4.- La institución Gubernamental posee un gran número de sedes a nivel nacional, por la geografía del territorio peruano optar por implementar una red física para interconectar las redes será muy costoso, lo más económico seria alquilar la red de un proveedor como Telefónica y Claro.

5.- Las instituciones Gubernamentales posee una información delicada y por ello requiere una red segura y que lo garantice un proveedor reconocido en el mercado nacional dedicado al negocio de la redes y que posea una infraestructura óptima para que brinde su servicio.

6.- Las redes IPVPN-MPLS es considerada una arquitectura que enlaza instituciones lejanas y de territorio geográfico difícil usando las redes ya implementadas, cuenta con un nivel de seguridad oprimo para interconectar instituciones privada o públicas.

7.- MPLS es un campo tecnológico innovador, convergente, el presente y futuro de la nueva generación de redes cuyo campo de aplicación no se limita a los estudios hasta ahora realizados, sino que está ampliamente abierta a la investigación y desarrollo de nuevas y transformadores aplicaciones.

ANEXO A
GLOSARIO DE TERMINOS

GLOSARIO

AES	Advanced Encryption Standard. Esquema de cifrado por bloques, estándar de adoptado por gobierno de Estados Unidos.
AppleTalk	Conjunto de protocolos desarrollados por Apple Inc., para conexión de redes.
AS	Security Association. Protocolo criptográfico que constituye la base del protocolo de intercambio de claves IKE. Definido en el RFC 2408
AS	Autonomous System. Conjunto de redes que se encuentran administrados por determinada entidad y que cuenta con determinadas políticas de red.
ATM	Asynchronous Transfer Mode.
Backbone	Referido a las conexiones principales y troncales al Internet.
BGP	Border Gateway Protocol. Protocolo de enrutamiento que opera entre sistemas autónomos diferentes.
CEF	Cisco Express Forwarding. Tecnología de conmutación de capa 3 avanzada usadas en el núcleo de la red o el Internet.
CLR	Conservation Mode Retention. Modo de distribución de etiqueta donde un LSR retiene las asignaciones de los routers downstream vecinos.
Core	Red troncal.
CPE	Customer Premises Equipment. Equipo local del cliente.
CR-LDP	Constraint-based Routing BGP. Protocolo de señalización desarrollado para soportar túneles.
DLCI	Data Link Connection Identifier. Identificador del canal del circuito establecido en Frame Relay.
EBGP	External Border Gateway Protocol.
Edge-LSR	Equipo de borde en una red MPLS.
EIGRP	Enhanced Interior Gateway Protocol.
Ethernet	Estándar de redes de área local con acceso al medio a través de CSMA/CD.
FEC	Forwarding Equivalence Class. Conjunto de paquetes que comparten los mismos atributos.
GRE	Generic Routing Encapsulation. Protocolo para el establecimiento de túneles a través de Internet.
IANA	Internet Assigned Numbers Authority. Ente de asignación de números de Internet.
IBGP	Internal Border Gateway Protocol.
IETF	Internet Engineering Task Force.

IGP	Interior Gateway Protocol.
IPsec	IP security.
IPv4	Versión 4 del protocolo IP, usa direcciones de 32 bits.
IPv6	Versión 6 del protocolo IP, usa direcciones de 128 bits.
KeepAlive	Define el tiempo que un nodo LDP espera antes de que decida que la sesión falló.
L3VPN	Layer 3 Virtual Private Network.
L2TP	Layer 2 Tunneling Protocol. Creado para corregir las deficiencias de PPTP y L2F.
L2VPN	Layer 2 Virtual Private Network.
LDP	Label Distribution Protocolo. Publicado en el RFC 3036.
L2F	Layer 2 Forwarding.
LFIB	Label Forwarding Information Base. Tabla que almacena un LSR y es usada en el reenvío de paquetes etiquetados
LIB	Label Information Base. Tabla que guarda las etiquetas de los paquetes que se usan como índice para una asignación etiqueta/FEC
LLR	Liberal Label Retention.
LSR	Label Switching Router. Un router que puede enviar paquetes basados en un valor de etiqueta que está añadida al paquete.
LSP	Label Switched Path.
MP-BGP	Multiprotocol Border Gateway Protocol. BGP con extensiones, permite a BGP transportar información de ruteo por múltiples protocolos de capa de red.
MPLS	Multiprotocol Label Switching.
MPLS-TE	Multiprotocol Label Switching Traffic Engineering.
OSPF	Open Shortest Path First. Protocolo de estado de enlace.
PDU	Protocol Data Units. Utilizado para el intercambio entre unidades parejas dentro de una capa del modelo OSI.
PHP	Penultimate hop Popping. Acto de remover la etiqueta MPLS un salto antes del LSR de salida.
PPTP	Point to Point Tunneling Protocol
PVC	Permanent Virtual Channel
QoS	Quality of Service. Medida de desempeño que refleja la calidad de servicio y su disponibilidad.
RD	Route Distinguisher. En el contexto de BGP MPLS L3 VPN, cadena de 8 bits que se concatena con un prefijo VPN.
RIB	Routing Information Base.

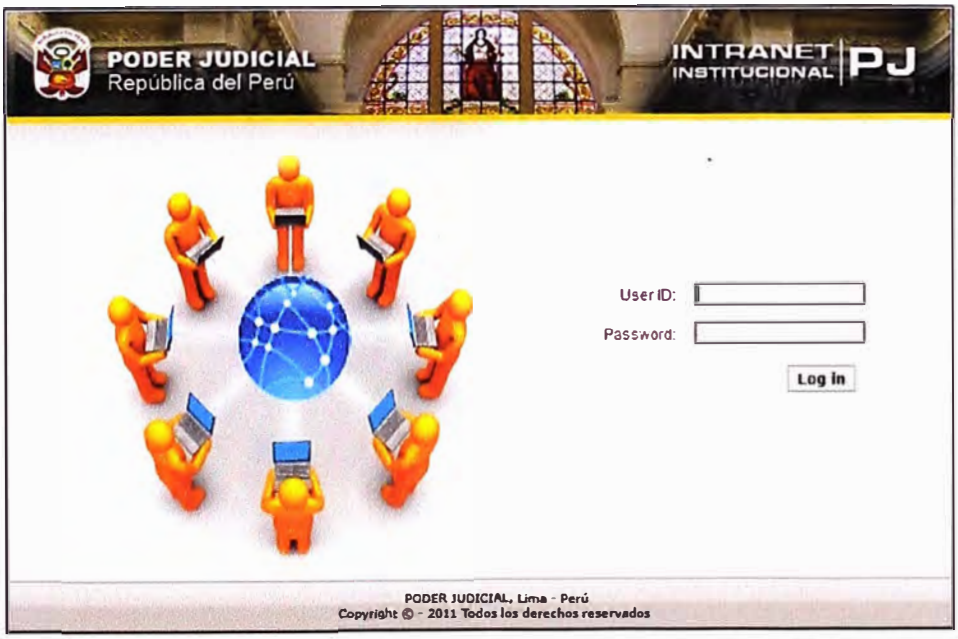
RIPv2	Routing Information Protocol version 2
RSVP	Resource reservation Protocol.
RSVP-TE	RSVP extendido que soporta túneles.
RT	Route Target. En el contexto de BGP MPLS L3 VPN, es una comunidad extendida de BGP la cual se añade al prefijo VPN. Define
SOO	Site of Origin. Comunidades extendidas que se puede usar en lugar de los RT.
SVC	Switched Virtual Circuit. Circuito que puede ser establecido por demanda.
IS-IS	System-to-Intermediate System.
TCP	Transmission Control Protocol. Protocolo de transporte seguro usado en IP.
TDM	Time Division Multiplexing.
TDP	Tag Distribution Protocol. Protocolo de distribución de etiquetas que antecedió a LDP.
TLV	Type-Lenght-Value. Tipo de codificación de información en mensajes de protocolo.
TTL	Time to Live.
UDP	User Datagrama Protocol. Protocolo de transporte poco fiable usado en IP.
VCI	Virtual Channel Identifier.
VPDN	Virtual Private Dial-up Network.
VPI	Virtual Path Identifier.
VPN	Virtual Private Network. Una red privada virtual realizada sobre una infraestructura compartida.
VRF	Virtual Routing and Forwarding. Tabla de enrutamiento y envío que permite el aislamiento entre diferentes VPN.

Web Service Servicio de Aplicaciones Web.

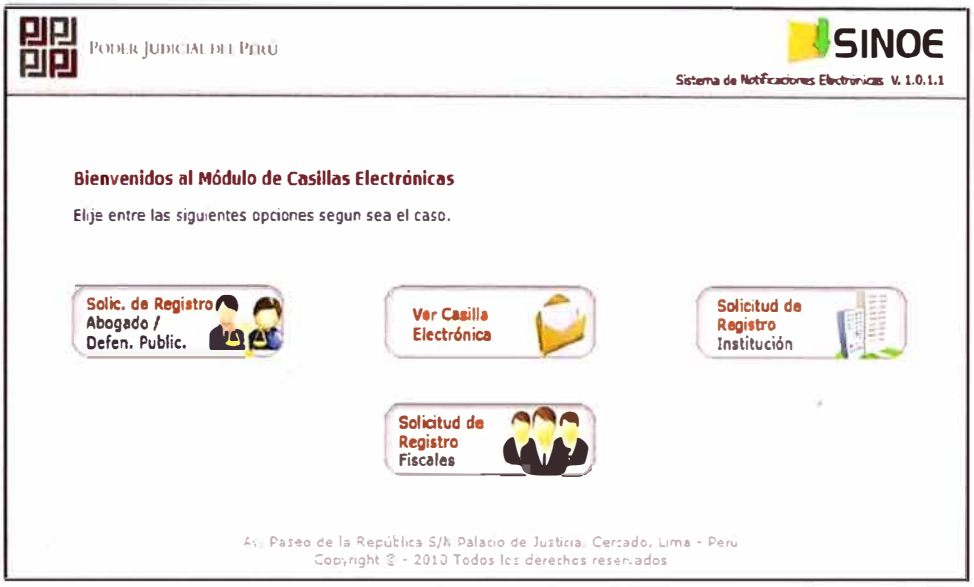
ANEXO B
SERVICIOS QUE CONSUMEN LA INTRANET A NIVEL NACIONAL

Sistema de Consulta Expediente a nivel nacional para todas las Cortes Superiores de Justicia a nivel nacional.

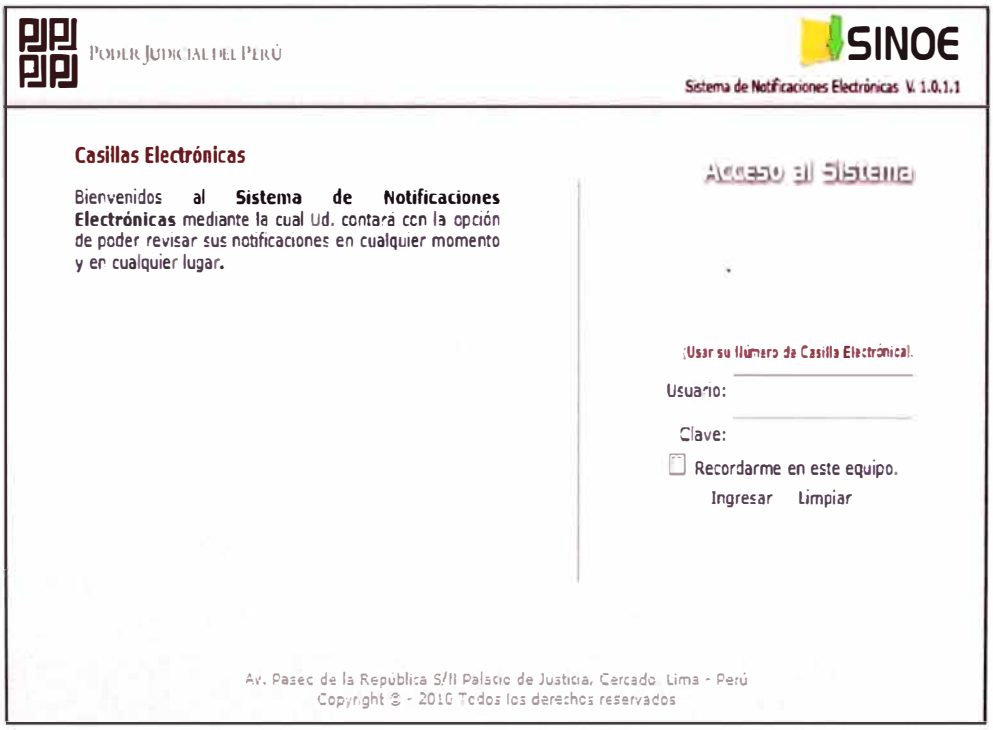
Intranet del Poder Judicial, donde se comparten información envíos de archivos documentos.



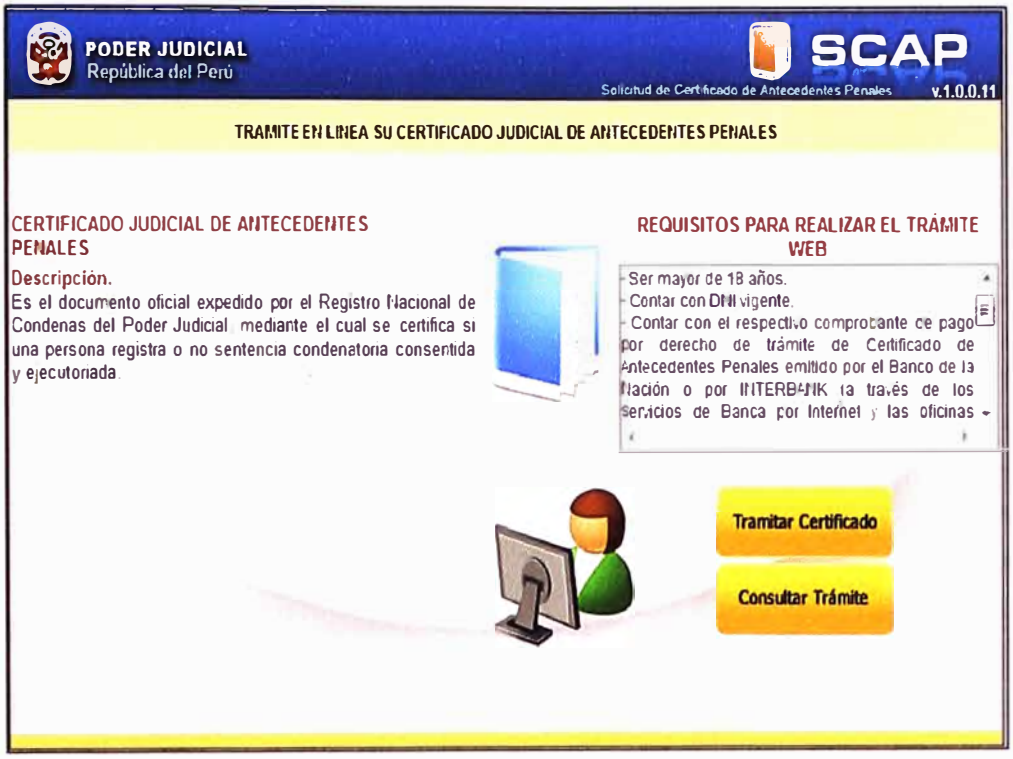
Sistema de notificaciones electrónicas. Envió de las notificaciones a nivel nacional (resolución cedulas y anexos)



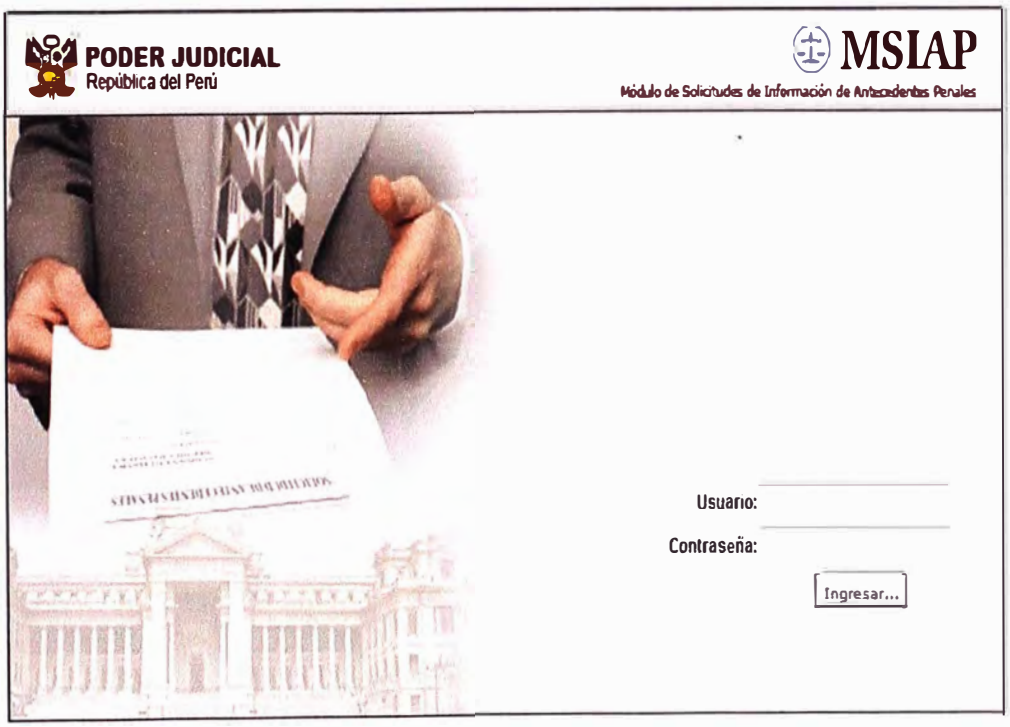
Casillas electrónicas de los abogados que son notificados.



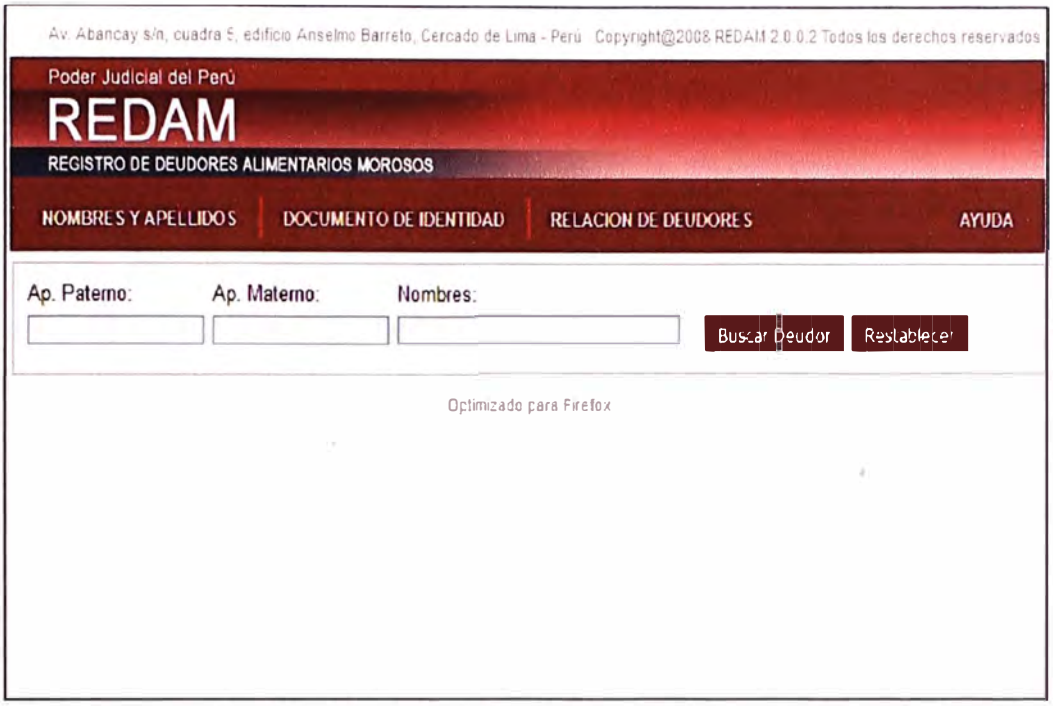
Trámite para solicitar un certificado de antecedentes penales.



Solicitud de información de los antecedentes penales de otros países.



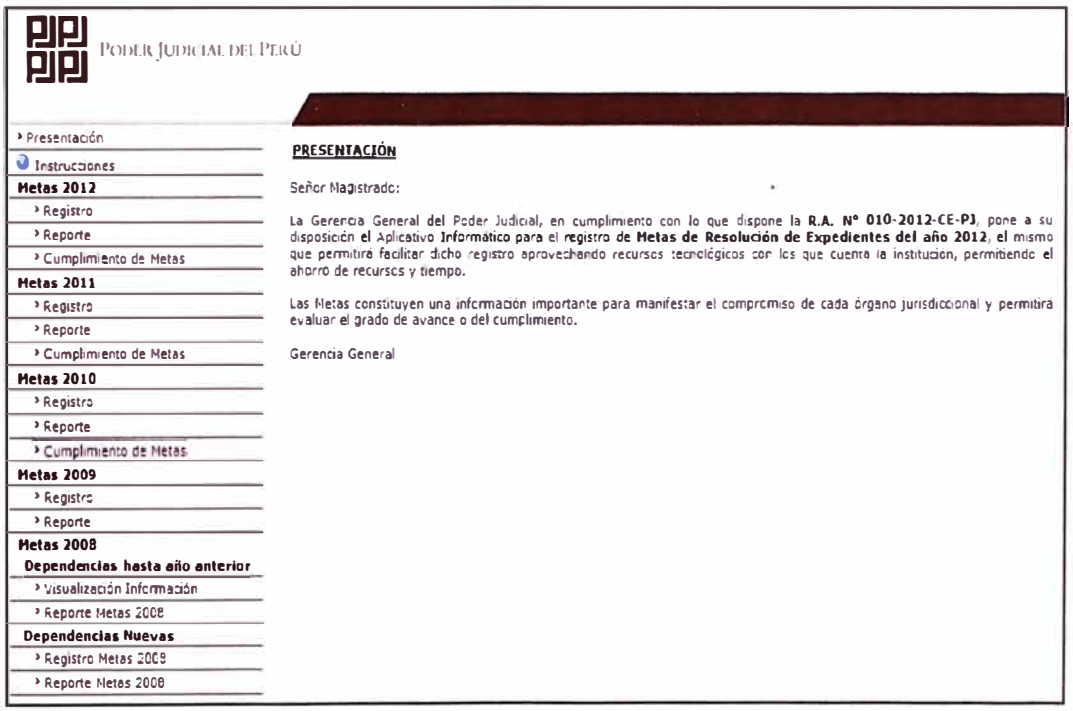
Solicitud de Reportes de los Registro de deudores de padres morosos.



Sistema de rendición de cuentas con el país (viáticos de viajes y comisiones).

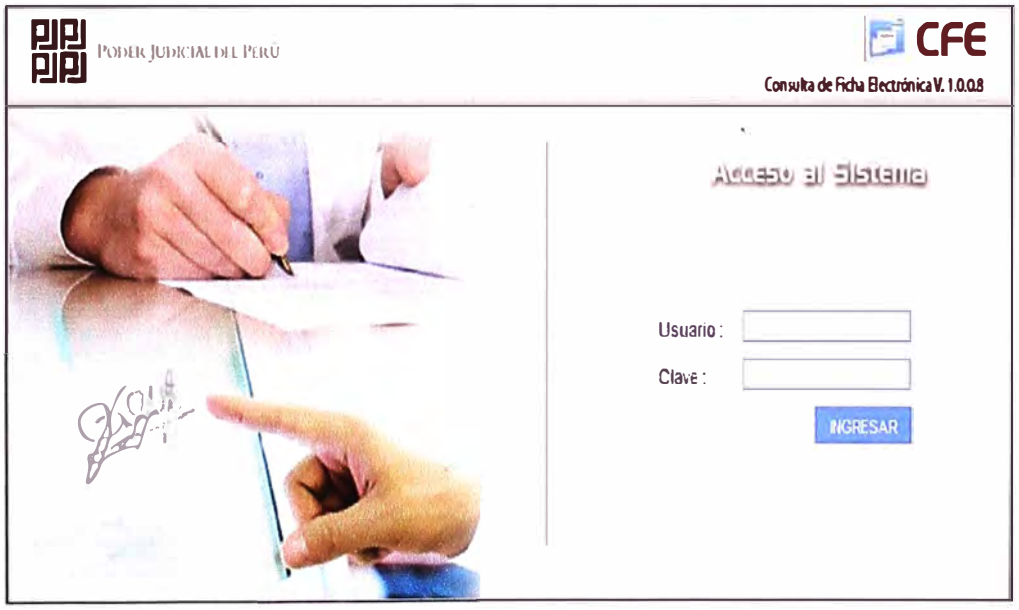
Sistema de postulación interna, exteman y CAS (Postulación a un puesto de trabajo en la institución gubernamental).

Sistema de Objetivos y metas, nos da indicativo de los adjetivos y metas cumplidos por cada miembro que la labora en la institución, para la otorgación de los incentivos y bonos.

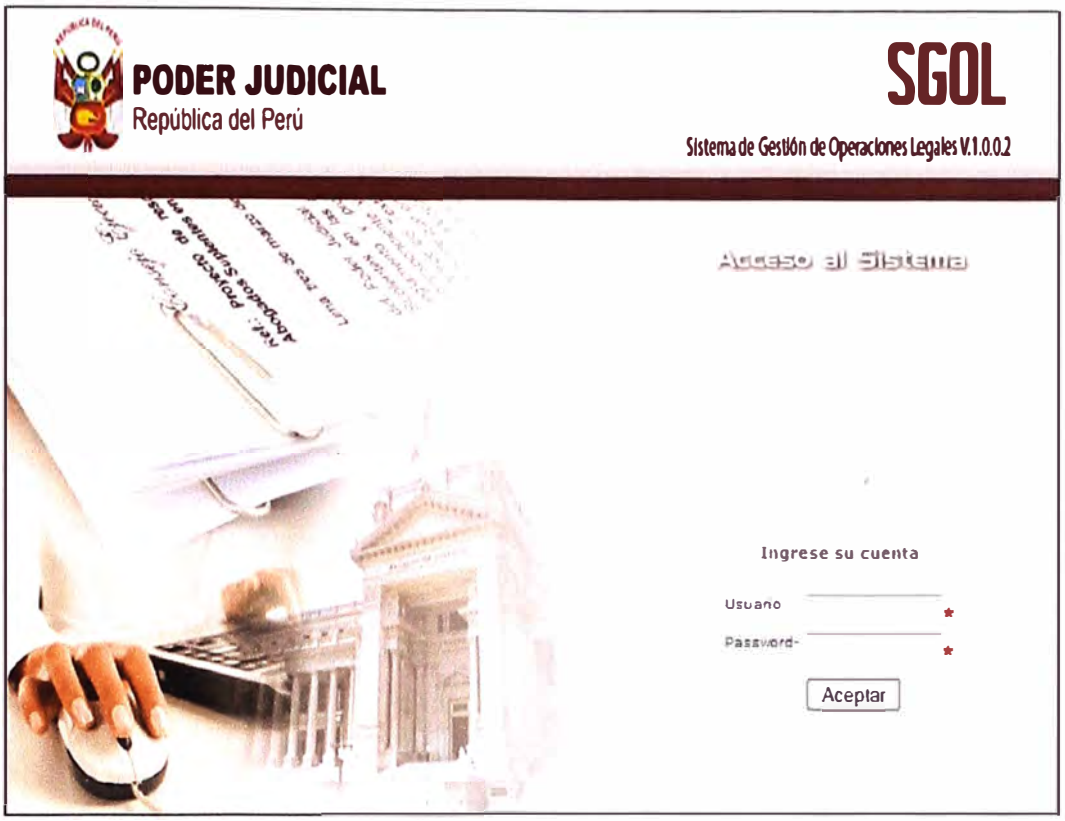


Sistema de Formulario estadísticos electrónicos 2012

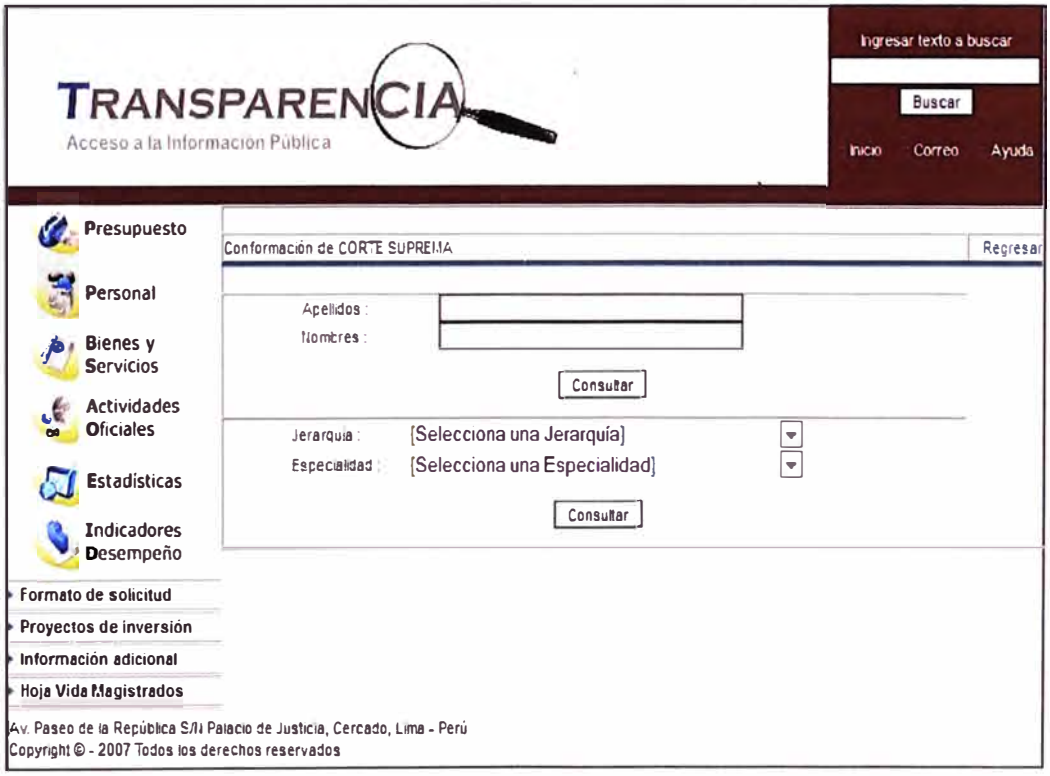
Consulta de Ficha fichas electrónicas



Sistema de gestión de operaciones legales



Sistema de Trasparencia.



ANEXO C
COBERTURA DE FIBRA ÓPTICA DE TELEFÓNICA DEL PERÚ

COBERTURA DE FIBRA OPTICA DE TELEFONICA DEL PERU

El Grupo Telefónica se ha propuesto realizar inversiones para expandir sustancialmente las comunicaciones en el periodo 2010-2013 en el orden de US$ 1,500 millones de dólares, esta inversión permitirá ampliar la red de transporte de fibra óptica en más de 1,000km para ofrecer servicios de banda ancha fija e internet móvil en las ciudades de Pucallpa, Tingo María, Huánuco, Huancavelica, Cusco, Abancay, Andahuaylas y Ayacucho. La Figura 3.4 muestra la cobertura de fibra óptica que tendrá el Grupo Telefónica al año 2013

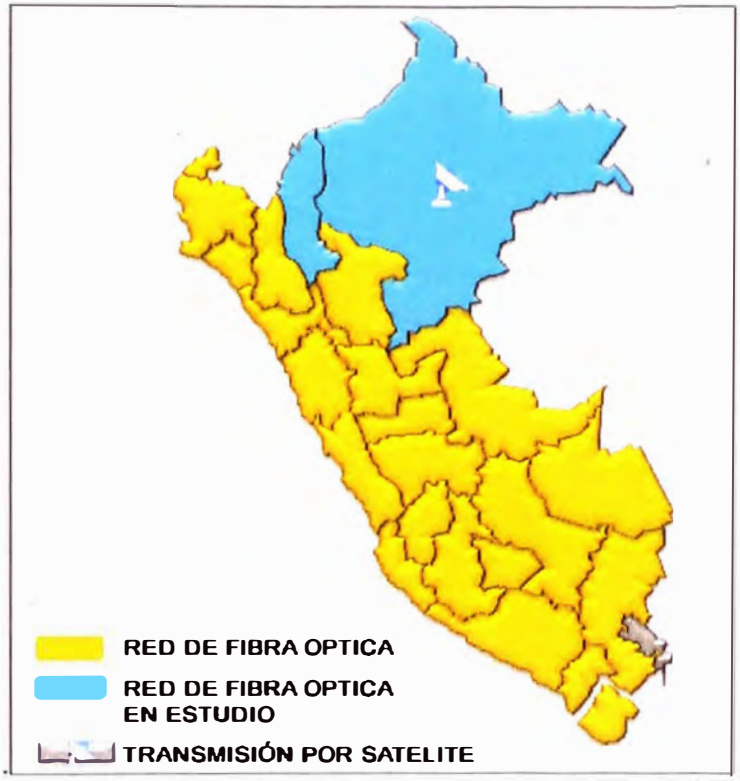


Figura 3.4: Cobertura de fibra óptica al año 2013

Fuente: página web de Telefónica del Perú.

Según la Figura 3.4, vemos que para el año 2013, prácticamente todo el país estará interconectado por medio de la fibra óptica del Grupo Telefónica, esto permitirá que se pueda implementar servicios interconexión a nivel nacional.

ANEXO D
TABLAS DE REFERENCIAS

Tabla 3.1 Tecnologías de transmisión de datos

Tecnología		Velocidad de transmisión	QoS	Características
Redes Privadas Virtuales		Enlaces desde 64 Kbps hasta 1Gbps	Si	* Servicio de transmisión de datos con clasificación por clases de servicio. * Velocidad de transmisión garantizada por cada clase de servicio * Servicio indicado para el transporte de aplicaciones de tiempo real, como voz y video. * Garantías de nivel de Servicio (SLA). * Servicio Simétrico
Lineas Privadas		Enlaces desde 128Kbps hasta 155Mbps	No	* El servicio de líneas privadas, proporciona a través de una plataforma SDH de última generación, escalable y de gran capacidad, una conectividad de canal transparente entre las sucursales o sedes de un cliente * Servicio Simétrico
VPN ADSL		600/256 Kbps , 900/256 Kbps	No	* Acceso asimétrico (velocidad de bajada mayor al de subida). * Garantía del 10% de la velocidad de transmisión contratada. * Medio de acceso: Cobre. * Requiere tener activa una línea telefónica contratada a TdP (se excluyen: líneas prepago, troncales y RDSI)
Enlaces satelitales	SCPC	Desde 64Kbps hasta 4096Kbps.	No	* Servicio simétrico * Enlaces punto a punto * Una sola portadora por canal
	VSAT	128Kbps/32Kbps, 256Kbps/64Kbps, 512Kbps/128Kbps, 768Kbps/256Kbps 1024Kbps/256Kbps.	No	* Servicio Asimétrico * El retardo de propagación típico es de 0.5s * Enlaces punto a multipunto * Varias portadoras por canal
Datos Móviles	GPRS, EDGE, UMTS	5MB-256Kbps 50MB-1500Kbps 200MB-1500Kbps 450MB-1500Kbps	Si	* Cuando la línea alcanza tal consumo en el ciclo de facturación la Vmax alcanzable se reduce a 256 Kbps Una vez que se Reinicie el ciclo de facturación la velocidad será la indicada. * Servicio Simétrico.

Tabla 3.2 Diferencias entre la RPV de CLARO y MOVISTAR

	Proveedor Claro	**Proveedor Telefónica**
Nombre	RPV Multi-servicios	IP VPN
Velocidad	Desde 64Kbps hasta 100Mpbs	Desde 64Kbps hasta 1Gbps
Cobertura	Su red de fibra óptica abarca toda la costa peruana y la ciudad Juliaca. Las otras ciudades se encuentran conectados por radioenlaces o enlaces satelitales	Su red de fibra óptica abarca toda la costa peruana y los departamentos de Cusco y Puno. Para fines del 2013 todas las ciudades de la sierra estarán conectadas por la red fibra óptica de Telefónica.
Clases de servicio	Permite diferenciar, clasificar y priorizar los diferentes tipos de tráfico en base a clases de servicio denominadas : * Clase Cos1 :Datos no críticos * Clase Cos2: Datos críticos * Clase Cos3: Video y voz	Permite diferenciar, clasificar y priorizar los diferentes tipos de tráfico en base a clases de servicio denominadas : * Clase Bronce :Datos no críticos * Clase Plata: Datos críticos * Clase Oro: Video y voz
Garantía del servicio	* Flexibilidad para implementar anchos de banda, prioridades, accesos remotos, nuevos servicios, entre otros. * Optimización de trayectorias de forma rápida y controlada. * Mantenimiento preventivo. * Escalabilidad en atención a fallas.	* Las conexiones se realizan de modo cerrado, permitiendo únicamente las comunicaciones entre las redes de área local definidas por el cliente. * Permite la utilización de direccionamiento IP público o privado, o de protocolos distintos de IP.
Tecnología utilizada	Utiliza la tecnología IP MPLS (Multiprotocolo de Intercambio de Etiquetas)	Es un servicio conexión de redes de área local sobre MPLS

ANEXO E
CARACTERISTICAS TECNICAS DE LOS EQUIPOS

1. **Router Cisco 3900 Series.**

	- The Cisco 3900 Series offers embedded hardware encryption acceleration, voice- and video-capable DSP slots, optional firewall, intrusion prevention, call processing, voicemail, and application services. In addition, the platforms support the industry's widest range of wired and wireless connectivity options such as T1/E1, T3/E3, xDSL, copper, and fiber Gigabit Ethernet.

2. **Módulo de Router Cisco 3900 Series.**

Cisco Services Performance Engine (SPE) 	- The Cisco 3900 Series offers field-replaceable SPEs.Módulos de SpO2 y PImax-PEmax. - These SPEs allow you to protect your initial investment in the Cisco 3900 platform for a longer time period and scale router performance as your network and branch-office needs grow.

3. **Convert FC a UTP Series.**

	- RAM incorporado 128Kb. - Connect de UTP: RJ-45, 10/100Mbps; Connect FC: ST/SC/FC, 100Mbps - Cable: UTP: Gato. 5 (distance max - 100m) - FC modos: 50/125, 62.5/125& MU; M (distance max 2km to 5km) - FC unimodal: 8/125, 8.7/125, 9/125, 10/125& MU; M (distance max until 20 -120km)

4. **Switch Cisco 3750 – 24 Puertos**

	- The Cisco Catalyst 3750 v2 Series consumes less power than its predecessors and is an ideal access layer for enterprise, retail, and branch environments. It helps increase productivity and protects your network investment by providing a unified network for data, voice, and video.

ANEXO F
MONITOREO DE LAS SEDES CON EL IPSWITCH

La Herramienta "Ipswitch" que usa para para monitorear nuestras conexiones a nivel nacional.

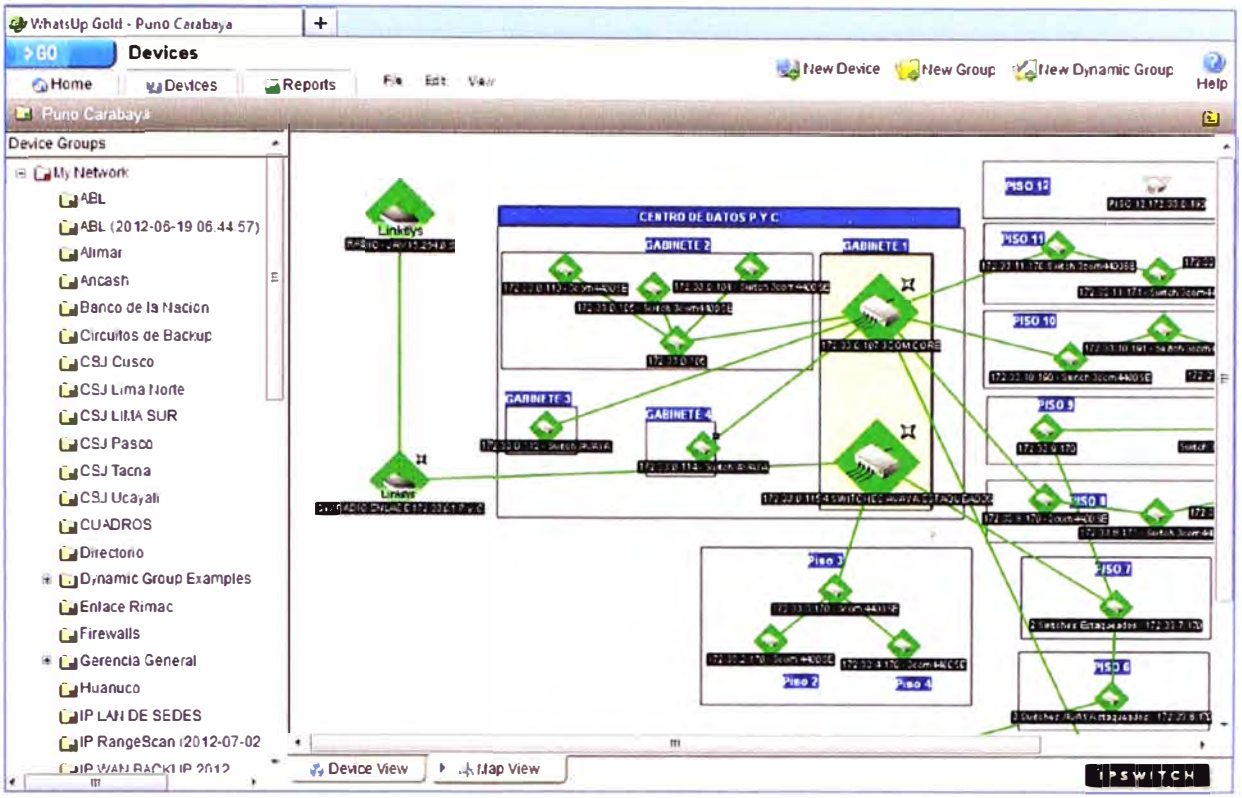


Figura 1.1 Monitoreo de red de cada sede con "IpSwitch"

Aquí se observa la inestabilidad de la conexión VPN por internet y radio enlace hacia algunas sedes monitoreo de las sedes de JUNIN y ICA.

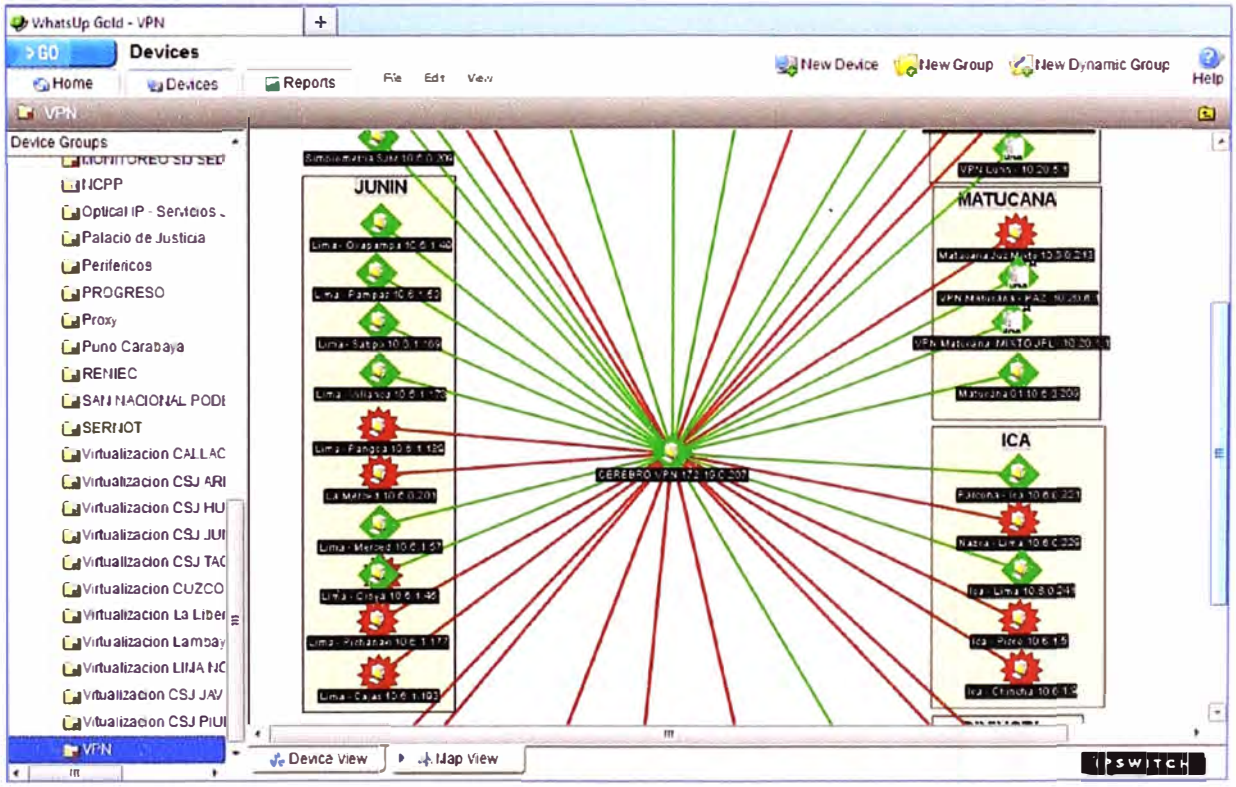


Figura 1.2 Monitoreo de las sedes Junín y Ica

Sedes Interconectadas con IPVPN MPLS (Propuestas)

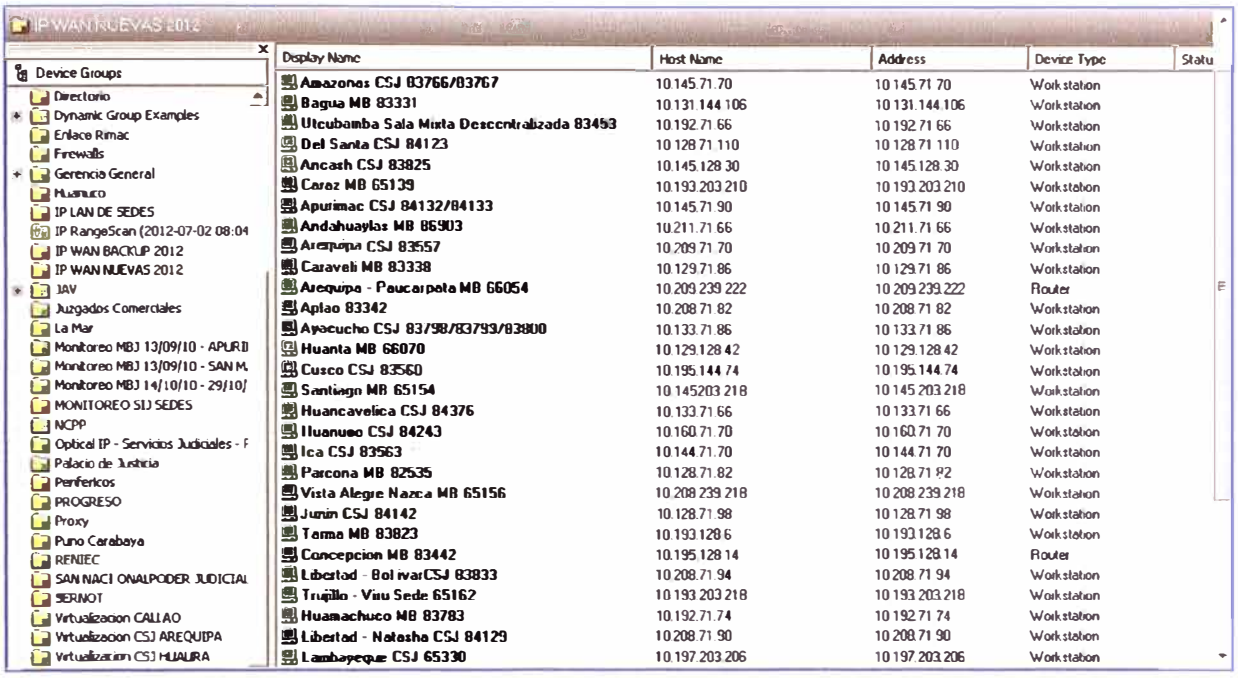


Figura 1.3 Cortes que se están monitoreando

Sedes Interconectadas – en forma grafica

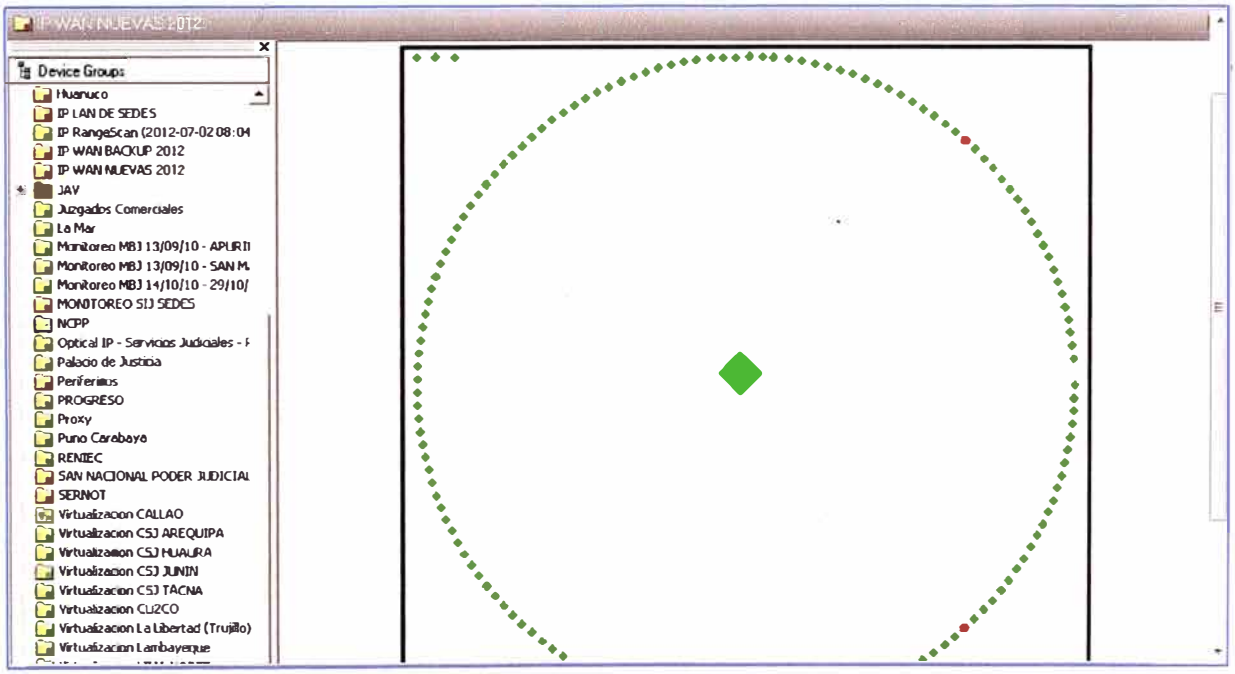


Figura 1.4 Enfoque de conexiones IPVPN a todas a las sedes a nivel nacional

Ampliación de las sedes interconectadas

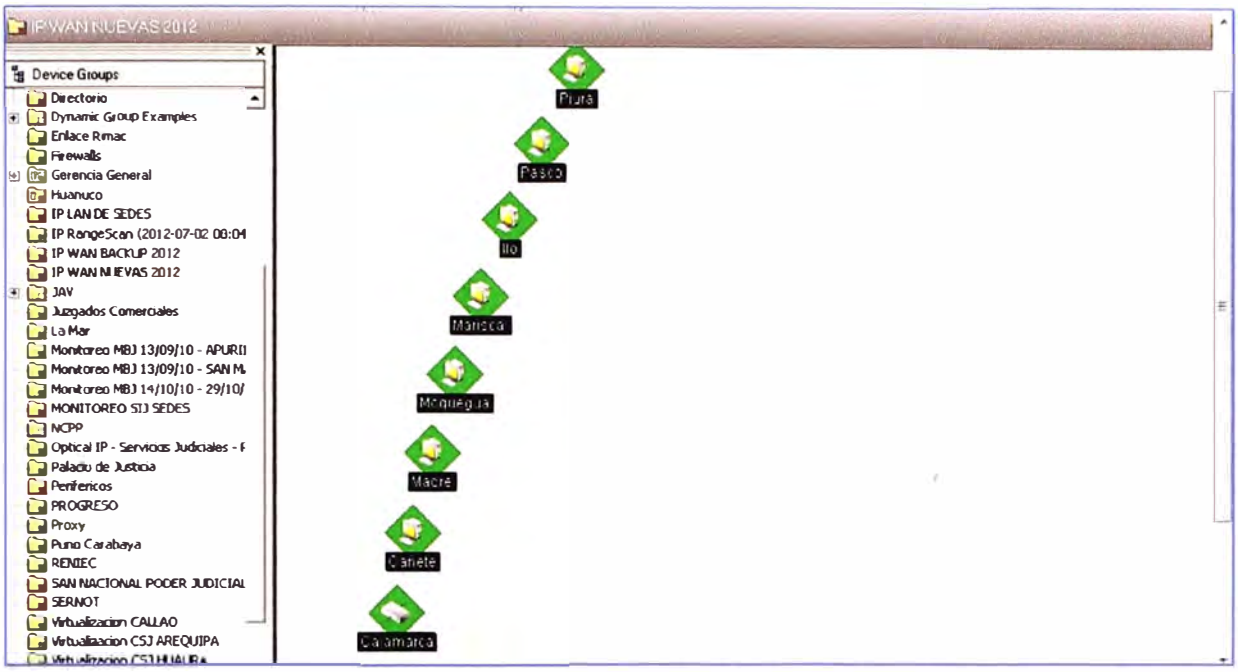


Figura 1.5 Ampliación del Enfoque de conexiones IPVPN a todas a las sedes

Sedes Interconectadas a nivel Nacional

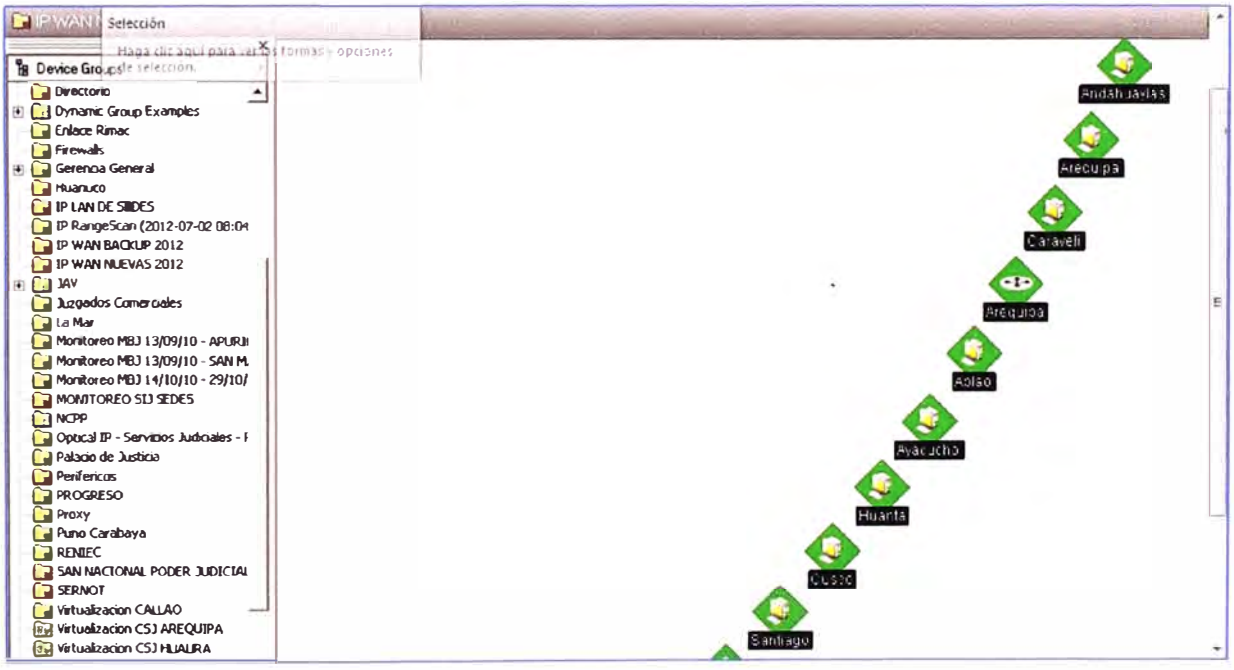


Figura 1.6 Ampliación del Enfoque de conexiones IPVPN a todas a las sedes

Conexión con la RENIEC

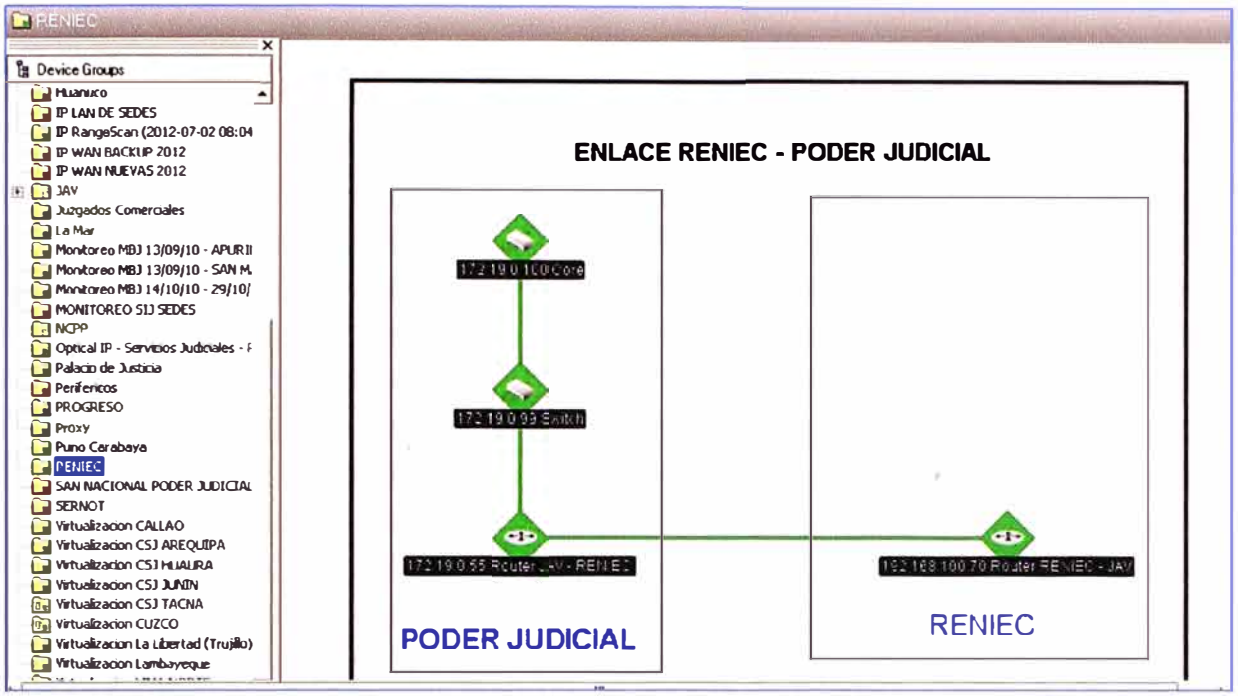


Figura 1.7 Conexiones a la RENIEC desde las sedes a nivel nacional

Conexión con Banco de la Nación

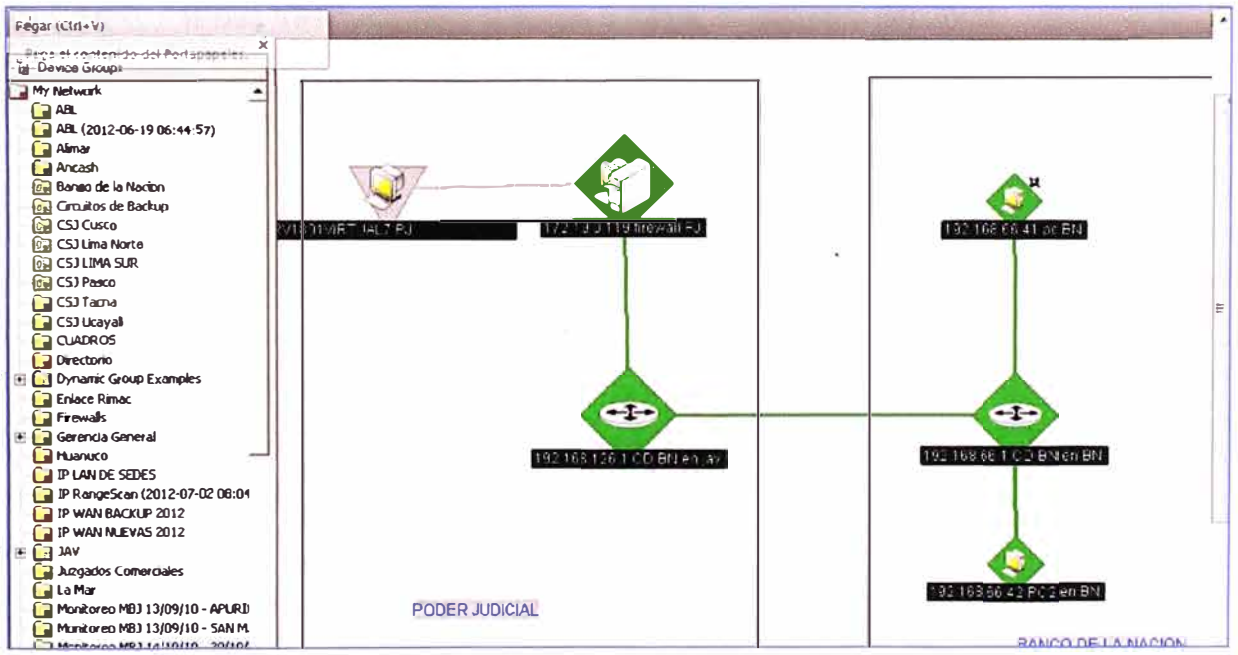


Figura 1.8 Conexiones a la Banco de la Nación desde las sedes a nivel nacional

BIBLIOGRAFÍA

[1] PEPELNJAK, Ivan y GUICHARD, Jim. **MPLS and VPN Architectures**, tomo 1, tercera edición, Cisco Press, Estados Unidos, 2001.

[2] GUEIN DE, Luc, **MPLS Fundamentals**, tomo 1, segunda edición, Cisco Press, Estados Unidos, 2007.

[3] DAVIE, Bruce S. y FARREL, Adria, **MPLS: Next Steps**, volumen 1, primera edición, Elsevier, Estados Unidos, mayo 2008.

[4] Cisco System Learning, **Implementing Cisco MPLS**, volumen 1, Version 2.2, Student Guide. Text part Number 97-2389-02.

[5] TAN, Nam-Kee, **Building VPNs with IPsec and MPLS**, tomo 1, primera edición, Mc- Graw-Hill, Estados Unidos, julio 2008.

[6] CCNP2, **"IPsec VPN", CCNP2 Módulo 3**, Lima, septiembre del 2008.

[7] OSBONE, Eric **"Traffic Engineering with MPLS"**, segunda edición, Cisco Press, Estados Unidos, 2002.

[8] PEPELNJAK, Ivan; APPCAR Jeff y GUICHARD Jim **"MPLS and VPN Architectures"**, Volumen II, segunda edición, Cisco Press, Estados Unidos, 2003.

[9] VIVEK Alwayn, "**Advanced MPLS Desing and Implementation**", Cisco Press Estados Unidos, 2002.

[10] Cisco Document ID: 14106, How Virtual Private Networks Work, http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a0080094865.sht ml, 13 octubre de 2008, Martes 20 de Octubre de 2011.

[11] TYSON, Jeff, How Virtual Private Networks Work, http://www.howstuffworks.com/vpn.htm, Martes 21 de Julio de 2009.

[12] Microsoft Corporation, Windows NT Service, Microsoft Corporation, Estados Unidos, 1998.