UNIVERSIDAD RICARDO PALMA
FACULTAD DE INGENIERÍA

PROGRAMA DE TITULACIÓN EXTRAORDINARIA

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

MIGRACIÓN E IMPLEMENTACIÓN HACIA UNA RED MPLS-VPN APLICADO A UNA ENTIDAD EMPRESARIAL EN LA CIUDAD DE LIMA

PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO ELECTRÓNICO

PRESENTADO POR:

Bach. CASTILLO MEZA JOEL OMAR

ASESOR: Ing. LUIS ALBERTO CUADRADO LERMA

LIMA – PERÚ

AÑO: 2015

DEDICATORIA

Dedico este trabajo a mi familia que gracias a su apoyo pude concluir mi carrera.

A mis padres por su apoyo y confianza, Gracias por ayudarme a cumplir mis objetivos como persona y estudiante. A mi padre por brindarme los recursos necesarios y estar a mi lado apoyándome y aconsejándome siempre. A mi madre por hacer de mí una mejor persona a través de sus consejos y enseñanzas y amor. A mi compañera mi esposa por desvelarse para ayudar a terminar mi proyecto. A mi hijo que es el motor de mi vida para salir adelante.

INDICE

INDICE DE GRAFICOS

INDICE DE TABLAS

RESUMEN

En la presente tesina se realiza una descripción de la tecnología de Conmutación Multi-Protocolo mediante etiquetas usando una red privada virtual para la comunicación de una entidad empresarial. Se realizó una descripción de la tecnología MPLS con VPN mostrando sus cualidades, ventajas y desventajas, se promueve la esta tecnología a la red de comunicación de datos de la empresa tenga un performance y confidencialidad en los datos transmitidos, diseñando un esquema así como la infraestructura que podría ser usada en esta implementación, con características modulares las cuales permitirá a la empresa ir creciendo a la medida de que su tráfico o demanda de transporte vaya aumentando al igual que la integración de las demás extensiones se amerita el caso; para el diseño nos ayudaremos del programa de simulación “GNS3” el mismo que se hará un bosquejo de la configuración y modelo para la transmisión de sucursal a matriz y viceversa.

PALABRAS CLAVES

Multiprotocolo de conmutación de etiquetas (MPLS); Red Privada Virtual (VPN); Protocolo Puerta de Frontera BGP

ABSTRACT

This thesis is a description of MPLS VPN using a communication from the business entity. Was a description of MPLS VPN showing his qualities, advantages and disadvantages, promotes the introduction of this technology to the data communication network of the company to have a performance traffic and confidentiality of the data transmitted, designing scheme as well as the infrastructure that could be used in this implementation, modular features which allow the company to grow to the extent that their traffic and transport demand will increase as the integration of other extensions are merited case, to help us design simulation program "GNS3" the same to be made a sketch of the model configuration and transmission branch to parent and vice versa.

KEYWORDS

Multiprotocol Label Switching (MPLS); Virtual Private Network (VPN); Border Gateway Protocol (BGP)

INTRODUCCION

Actualmente las tecnologías existentes como IP están diseñadas para que brinden seguridad y sean capaces de restablecer la conectividad luego de que se presente alguna falla en algún elemento de red. Aunque la conectividad pueda restablecerse, el tiempo que esto demande podría no estar en el límite para lo aceptable en lo que respecta a servicios de alta prioridad. Con el crecimiento han despertado un gran interés por los mecanismos de transporte de datos y sus diferentes aplicaciones, dentro de ello encontramos a las Redes Privadas Virtuales o VPNs (Virtual Private Networks). Para hacer posible su despliegue, tecnologías como MPLS (Multi Protocol Label Switching) han tenido gran aceptación debido a sus múltiples ventajas y características que la han convertido en la tecnología ideal para muchas grandes empresas. Las MPLS-VPN, además de proporcionar escalabilidad, permiten dividir una gran red en pequeñas redes separadas, lo cual es muchas veces necesario en grandes compañías, donde la infraestructura tecnológica debe ofrecer redes aisladas a áreas individuales.

Sin embargo, al igual que con el Internet, las empresas crecen junto con sus necesidades. Dichas necesidades incluyen la conectividad privada a grandes distancias, o conectividad con más de un proveedor a la vez.

CAPÍTULO I

FUNDAMENTOS

1.1 MARCO SITUACIONAL

La situación de la empresa es que en sus oficinas remotas están aisladas de toda comunicación con la oficina principal, cada una de estas tiene su propio esquema de nombres, sus propios protocolos que difieran de los usados en otras sucursales, su propio sistema de email. Con esto se puede decir que en cada lugar existe una configuración totalmente local, que no necesariamente debe ser compatible con alguna o todas las demás configuraciones de las otras áreas dentro de la misma empresa.

Actualmente la sede principal y sedes remotas comparten la información, mediante mail, USB y medios de almacenamiento externo, con el fin de consolidar dicha información debido a que ninguna se comunica por la red para acceder al servidor principal. Con esta modalidad no se tiene la seguridad necesaria para el manejo de la información, lo que hace que en ocasiones ésta pueda perderse, y ocasionar cuantiosas pérdidas a la empresa.

1.2 PROBLEMÁTICA DEL PROYECTO

La empresa está dedicada a la producción y distribución de consumos informáticos, con más de 10 años de experiencia en el sector, está atravesando una gran problemática en cuanto a la comunicación de información entre las sedes de las mismas. Estas sedes se encuentran ubicadas en distintas partes dentro de la capital: cuenta con una oficina

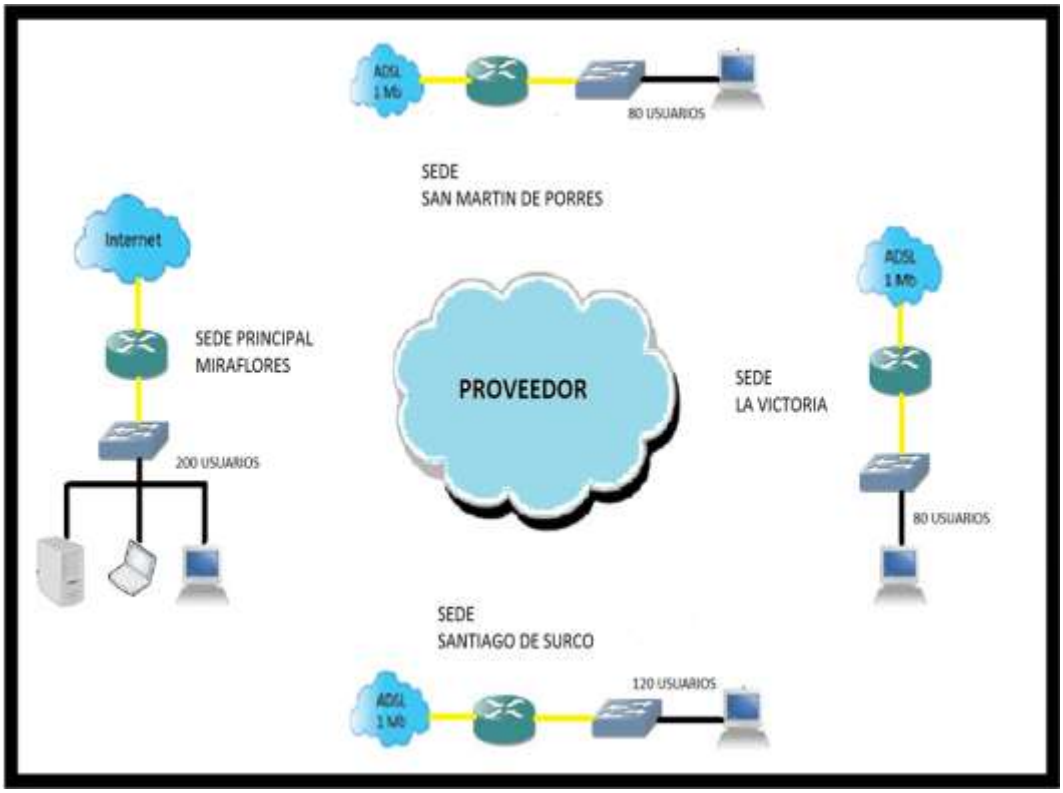
principal en Miraflores y 3 sucursales, uno en San Martin de Porres, uno en La Victoria y otro en Santiago de Surco.

En la siguiente gráfica (ver Figura 1.1) se puede observar que cada sucursal está aislada la una de la otra, sin ninguna conexión o vinculación entre ellas. Esto es muy perjudicial para la empresa, ya que no comparten la información en tiempo real de lo que sucede en cada una de sus sedes, causando así grandes pérdidas económicas.

La situación actual de la empresa con respecto a la tecnología que usan para sus servicios básicos como por ejemplo el internet, telefonía básica, se estructura de la siguiente manera:

- Sede Principal (Miraflores) = Internet 2Mb con overbooking de 1:8 y telefonía básica.
- Sede San Martin de Porres = Internet por ADSL de 1Mb con overbooking de 1:8
- Sede La Victoria = Internet por ADSL de 1Mb con overbooking de 1:8
- Sede Santiago de Surco = Internet por ADSL de 1Mb con overbooking de 1:8

Figura 1.1 Estado actual de la red de la empresa.



Fuente: Elaboración Propia

La problemática que pasa la empresa se enumera de la siguiente manera:

a) No poder compartir información y transferencia de archivos mediante un sistema propio centralizado y en tiempo real.
b) Comunicación de las sucursales y la principal mediante la telefonía móvil propia de los trabajadores.

1.3 OBJETIVOS

1.3.1 Objetivo General

La migración e implementación hacia una red MPLS – VPN para una empresa en la ciudad de Lima, para la comunicación entre sus sedes distantes geográficamente utilizando recursos públicos.

1.3.2 Objetivos Específicos

- Estudiar los elementos teóricos y técnicos para uso de la tecnología VPN con MPLS, así como la comparación de los modelos de red que existen para su implementación.
- Comprender la necesidad de brindar servicios de redes privadas virtuales a clientes corporativos.
- Realizar una simulación de configuración básica de tecnología VPN con MPLS teniendo como herramienta GNS3.
- Seleccionar los dispositivos que soporte la tecnología así como la implementación a nivel de configuración.

1.4 IMPORTANCIA

Este proyecto busca mejorar el desempeño de los dispositivos y el desempeño de la red en general, y por esto se dice que es la solución definitiva al encaminamiento rápido de paquetes. La intención de este proyecto no es dar una clase teórica completa sobre MPLS pero considero que una descripción básica de su funcionalidad ayudará a comprender su importancia y por qué empresas y operadores se decantan por estas redes.

1.5 HIPÓTESIS

El uso de una aplicación permitirá simular la forma de configuración de los equipos del núcleo de una red MPLS demostrando las ventajas que ofrece la tecnología y obtener una red con mayor escalabilidad.

1.6 ESTRUCTURA DEL PROYECTO

La estructura de este proyecto se compone de 3 capítulos.

En el capítulo 1, la necesidad de realizar un estudio y los objetivos del trabajo.

Seguidamente, en el capítulo 2 estudios de las redes MPLS-VPN tanto en su arquitectura así como los protocolos y tecnologías que las conforman.

A continuación, en el capítulo 3 corresponde al desarrollo del proyecto, Y para finalizar el capítulo 4, que corresponde a los costos y beneficios del proyecto.

CAPÍTULO II

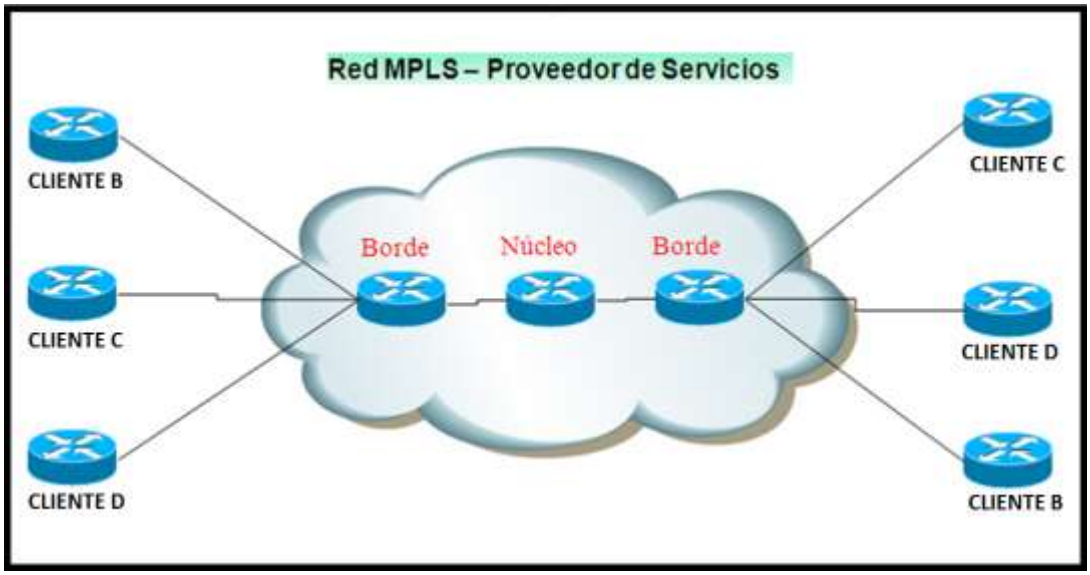
MARCO TEORICO

2.1 BASES TEÓRICAS

Una de las aplicaciones más importantes y utilizadas de una red MPLS es la llamada MPLS-VPN (Virtual Private Network MPLS). MPLS-VPN proporciona direccionamientos privados e independientes entre sí. Por ejemplo supongamos que un proveedor de servicios de internet tiene diferentes clientes, los clientes de una entidad en concreto no desearon que el direccionamiento sea conocido por otro cliente del proveedor.

Con MPLS-VPN cada cliente es totalmente anónimo y privado para otro y su enrutamiento desconocido (Ver Figura 2.1). Sería lo que podríamos decir entornos de routing independientes. MPLS-VPN consigue las diferentes tablas de routing mediante las llamadas VRF (Virtual routing and forwarding). Cada cliente tendría asignado su VRF y por otro lado su propia tabla de enrutamiento. Al tratarse de tablas de routing independientes y privadas podemos duplicar IPs mientras estas no se encuentren dentro de la misma VRF. Este hecho es una gran ventaja si lo comparamos con otro tipo de redes.

Figura 2.1 Estructura básica de MPLS de cada cliente



Fuente: Elaboración Propia

A continuación se muestra los términos y rol de equipos que conformar una red MPLS.

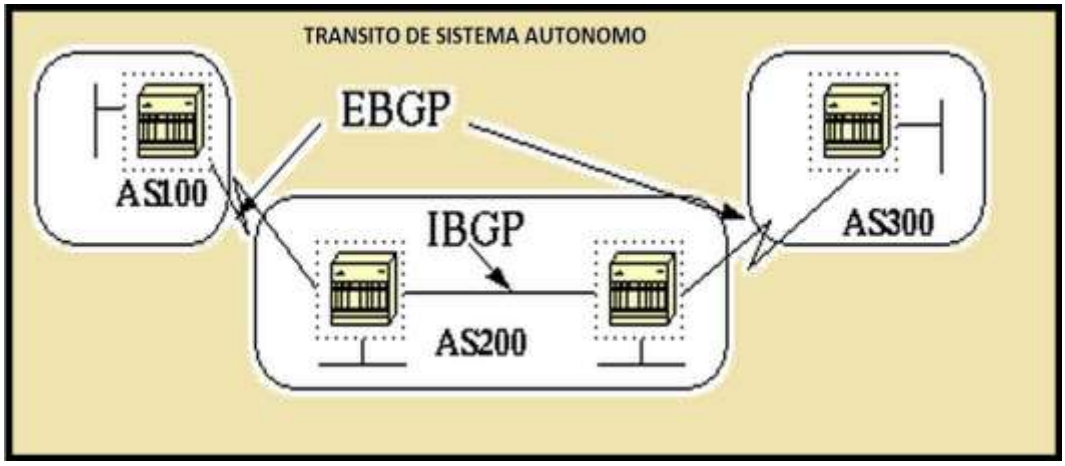
- CPE (Customer Premises Equipment): dispositivo que se encuentra fuera de la red MPLS y por lo tanto no utiliza sistema de etiquetado (Generalmente es el cliente de un ISP).
- PE (Provider Edge): Equipo que comparte al menos un enlace con un CPE y otro dentro de la red MPLS. Se encarga de introducir las VRFs y realizar la función de POP
- P (Provider): Router que estaría totalmente dentro de la red MPLS. No tendría ningún enlace conectado directamente a un CPE.

Entre los dispositivos del tipo P y PE se realiza el MPLS unicast y básicamente se usa el protocolo de routing OSPF y LDP para asociar etiquetas con IPs. El direccionamiento del OSPF no sería de los clientes si no el de los diferentes elementos de la red MPLS.

Por otra parte el PE debe aprender las rutas del CPE, por lo tanto las rutas de los clientes. Estas rutas aprendidas por el PE deben intercambiarse con otros PE. Para ellos se utiliza el protocolo de routing BGP (Ver Figura 2.2). BGP nos permite establecer vecinos sin que estos estén directamente conectados e intercambiar las diferentes rutas (siempre y cuando un vecino BGP sepa cómo llegar hasta otro).

Como internamente dentro de nuestra red MPLS hemos utilizado OSPF todos los PEs de nuestra red podrán formar vecindad BGP con otros PEs e intercambiar las rutas de los clientes.

Figura 2.2 Intercambia rutas de vecinos no directamente conectados.



Fuente: Elaboración Propia

2.2 VPNs

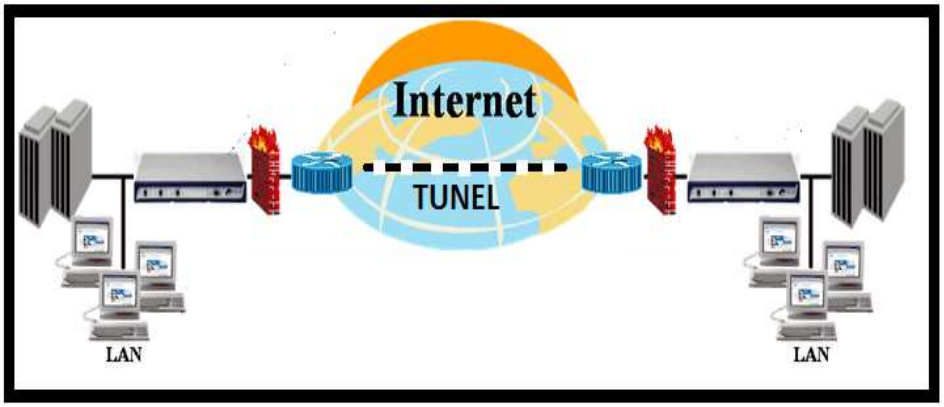
2.2.1 Definición

Una VPN es una estructura de red que emula una red privada sobre infraestructura pública existente. Brinda comunicación a nivel de las capas 2 ó 3 del modelo OSI. La VPN pertenece generalmente a una compañía y le permite tener diferentes locales interconectados a

través de la infraestructura de un proveedor de servicios. Esto es posible ya que la tecnología permite crear un túnel de encriptación a través de la Internet u otra red pública de tal forma que permita a los usuarios que se encuentran en los extremos del túnel disfrutar de la seguridad, privacidad y funciones que antes estaban disponibles sólo en redes privadas (ver Figura 2.3).

Es una red porque las VPNs son capaces de interconectar, extender y comunicar redes o segmentos de redes.

Figura 2.3 Estructura de una Red Privada Virtual



Fuente: Elaboración Propia

2.2.2 ¿Porque usar VPN?

Reducción de Costos

Para una implementación de red que abarque empresas distanciadas geográficamente ya no será indispensable en términos de seguridad realizar enlaces mediante líneas dedicadas (punto a punto). En su lugar, se puede emplear un acceso ADSL. Es de bajo

costo, brinda un ancho de banda alto y está disponible en la mayoría de zonas urbanas.

Alta Seguridad

Las redes VPN utilizan altos estándares de seguridad para la transmisión de datos, de una red punto a punto. Protocolos como 3DES (Triple data encryption standard) el cual cumple la función de encriptar la información a transferir y el protocolo IPSec (IP Security) para manejo de los túneles mediante software brindan un alto nivel de seguridad al sistema.

Escalabilidad

No se requiere inversiones adicionales para agregar usuarios a la red. El servicio se provee con dispositivos y equipos configurables y manejables. La desarrollada infraestructura de los proveedores de Internet hace innecesario realizar un enlace físico que puede significar una gran inversión de dinero y de tiempo.

Mayor Productividad

Una red VPN da un nivel de acceso durante mayor tiempo, que significa una mayor productividad de los usuarios de la RED. Además, con la consecutiva reducción en las necesidades de espacio físico.

2.2.3 VPNs de Capa 3

En las VPNs de capa 3, los proveedores de servicio entregan una conexión de línea arrendada entre un cliente y el POP (punto de presencia) más cercano en la red del proveedor de servicio.

Actualmente las tecnologías VPN mas desplegadas, basadas en IP, son las VPN basadas en MPLS BGP (Border Gateway Protocol). Estas tecnologías pueden acomodar intranet, extranet y aplicaciones de acceso a internet, satisfaciendo la necesidad del cliente e interconectar sitios dispersos geográficamente de manera segura y privada.

Las imperfecciones más importantes de VPNs basadas en IP son que soportan solamente IP y requieren una infraestructura de capa 3.

Propiedades:

- **Encapsulación:** Las VPNs encapsulan datos privados con un encabezado que les permite atravesar la red pública.

- **Cifrado de datos:** Esta propiedad permite convertir texto legible en un texto ilegible, logrando de esta manera que solo la persona a la que se le envía lo convierta en un texto legible.

  Existen varias técnicas de cifrado de datos que funcionan en distintos niveles del modelo OSI, de esta manera se puede encontrar algoritmos de cifrado de enlace de datos y algoritmos de cifrado a nivel de red.

- **Beneficios:** Los beneficios de una Red Privada Virtual son solo un término general, que se utiliza para describir todas las

utilidades potenciales cuando se implementa la tecnología VPN, entre estos podemos señalar: Seguridad, transparencia, flexibilidad, facilidad de instalación y uso, cobertura, ahorro de costos.

2.2.4 Redes VPN-MPLS

Una red privada requiere que todos los locales del cliente puedan interconectarse y sean completamente separadas de otras VPNs. Ese es el mínimo requisito de interconectividad que debe cumplirse. Sin embargo, algunos modelos de VPN de Capa 3 pueden requerir más que eso. Deben ser capaces de brindar conectividad entre diferentes VPNs e incluso proveer conexión a Internet.

El estándar más extendido para proporcionar soluciones de VPN sobre MPLS es definido por el IETF en la RFC 2547bis. Se conoce también como BGP/MPLS ya que utiliza BGP para distribuir la información de routing de la VPN a través del Backbone del proveedor de servicios y el MPLS para el reenvío del tráfico entre emplazamiento de la VPN.

El modelo de VPN definido consta de varios elementos:

- P (Provider Routers). Son los routers internos de la red del proveedor, que se comunican con los PE y con otros P pero no están conectados directamente a los routers de cliente. No necesitan mantener información específica de las rutas de la VPN y a nivel MPLS funcionan como LSRs conmutando

etiquetas. La comunicación para el establecimiento de rutas entre PEs y Ps se realiza mediante el protocolo MP-BGP (Multiprotocol BGP).

- PE (Provider Edge Routers). Es el router de entrada a la red del proveedor de servicios, al que se conectan los router de cliente, el PE mantiene las tablas de enrutamiento específicas de las VPN y a nivel MPLS actúa como LER y tiene capacidad para conmutar etiquetas.

- CPE (Customer Edge Router). Es el router de cliente que proporciona acceso a la red del proveedor sobre un enlace de datos que se establece con uno o varios routers del proveedor. Una de las características más importantes es que puede utilizarse cualquier tecnología de acceso a cualquier protocolo de encaminamiento entre el equipo del cliente y el del proveedor.

- VRF (VPN Routing and Forwarding Table). Tabla de rutas única que se crea en el PE para cada VPN conectada al mismo, de forma que el PE se comporta como si hubiera varios routers virtuales, uno por cada VPN con su propia tabla de enrutamiento.

Este es el método utilizado para proporcionar seguridad, aislando el tráfico entre distintas VPNs. Cuando el PE recibe un paquete del

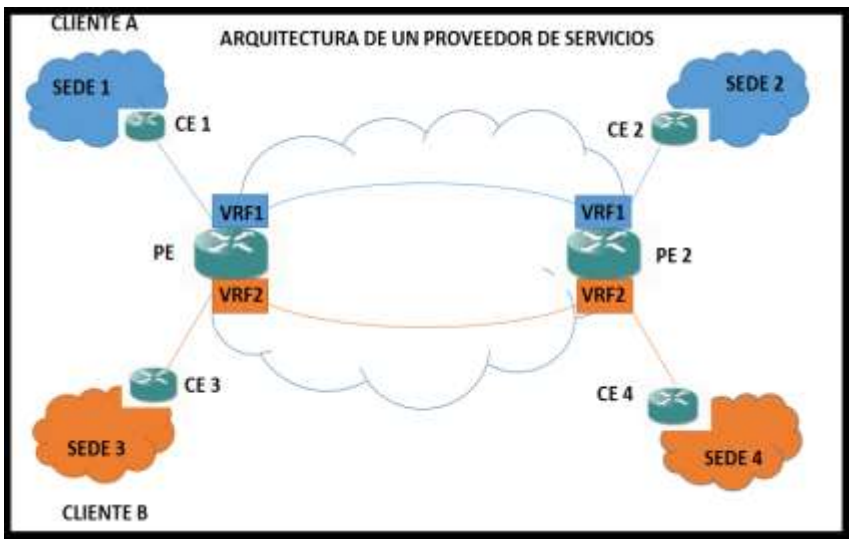
CPE se utiliza la tabla de encaminamiento VRF que está asignada a ese emplazamiento para determinar el enrutado de los datos.

La asociación con el VRF establece a nivel de puerto, de forma que si el PE tiene varias conexiones (varios enlaces en distintos puertos) con el mismo emplazamiento todas ellas se pueden asociar con el mismo VRF.

Por otro lado dos interfaces solo pueden mapearse con el mismo VRF a menos que se pretenda que compartan información de rutas, y la dirección de destino de los paquetes para un VRF se determina en función del interfaz de entrada.

La siguiente imagen (ver Figura 2.4) muestra un ejemplo de la arquitectura de una red VPN/MPLS con dos VPN distintas:

Figura 2.4 Arquitectura VPN - MPLS



Fuente: Elaboración Propia

2.2.4.1 Ventajas

Las redes VPN-MPLS presentan numerosas ventajas tanto desde el punto de vista del operador como del cliente:

- Desde el punto de vista del operador la tecnología MPLS ya está desplegada en el núcleo de la red IP, dando servicio a múltiples clientes, lo que permite ofrecer el servicio sin tener que hacer inversiones adicionales en el backbone y aun coste competitivo para el cliente.
- Desde el punto de vista del cliente el utilizar el backbone del operador supone un elevado ahorro de costes frente a la solución basada en el establecimiento de enlaces punto a punto (ver Figura 2.5). La construcción de enlaces se reduce el establecimiento del enlace entre la sede del cliente y el punto de entrada a la red MPLS del operador, lo que facilita y abarata la incorporación de nuevas sedes.
- Accesibilidad. La VPN-MPLS permite utilizar cualquier tecnología de acceso para interconectar las sedes con la red del operador, lo que también proporciona una gran flexibilidad.
- Por un lado permite al operador seleccionar la tecnología de acceso según el despliegue de red

que tenga en cada zona, pudiendo proporcionar una mayor cobertura geográfica, y abaratar los costes de establecimiento del enlace para el cliente.

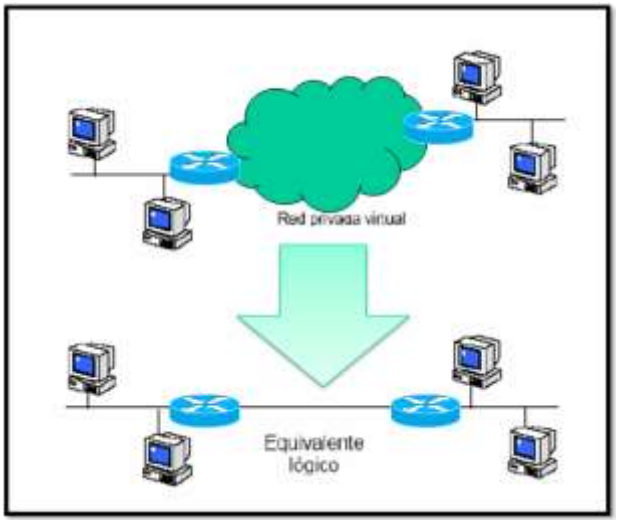
- Flexibilidad. La VPN-MPLS proporciona la interconexión de todas las sedes entre si lo que permite adaptarse a la topología requerida por las aplicaciones del cliente, pudiendo configurar fácilmente estructuras Full Mesh, Hub&Spoke, mixtas, etc. según las necesidades del cliente.
- Por otra parte la tecnología permite el solapamiento de espacios de direcciones entre distintos clientes, con lo que el cliente puede utilizar su propio espacio de direcciones, público o privado, adaptándose completamiento a sus necesidades y minimizando la configuración de su red interna.
- QoS. La utilización de la red MPLS ofrece la posibilidad de definir clases de servicio dentro de cada VPN que se adapten a las diferentes aplicaciones que pueda necesitar el cliente, proporcionando distintos mecanismos que garanticen la calidad de servicio.
- Administración. Desde la perspectiva del cliente toda la administración y gestión del backbone la realiza el operador lo que simplifica todas las tareas asociadas al mantenimiento de su propia red.

- Los routers de cliente de cada sede no tienen que intercambiar información de enrutamiento con otros routers de la VPN, por lo que todos los problemas de enrutamiento dentro del backbone son responsabilidad del operador, y el cliente tampoco tiene que gestionar los accesos a los routers PE o P.
- En el lado del operador la misma red de backbone puede proporcionar servicio a las VPNs de múltiples clientes sin necesidad de administrar cada una de ellas por separado.
- Seguridad. La VPN proporciona la separación de flujos de tráfico entre los distintos clientes que utilizan el backbone del operador ofreciendo niveles de seguridad equivalentes a los de los circuitos virtuales ATM o Frame Relay sin necesidad de implementar técnicas de encriptado adicional.
- Aun así en caso de ser necesarias medidas de protección adicionales se puede recurrir a soluciones combinadas como la utilización de IPSEC sobre VPN-MPLS.
- Disponibilidad. La red de backbone del proveedor de servicios generalmente ofrece unos niveles de redundancia y alta disponibilidad que es aprovechado por el cliente al utilizar esta red como

punto de unión entre todas las sedes.

- Por otra parte la red VPN-MPLS permite conectar todas las redes en una topología totalmente mallada entre las diferentes sedes, lo que supone que ante la caída de una de las sedes el resto permanecen comunicadas entre sí.
- Coste. Como resumen de varios puntos comentamos anteriormente una solución de este tipo proporciona al cliente una red de altas prestaciones a un coste muy reducido.

Figura 2.5 Arquitectura MPLS transparente para el cliente.



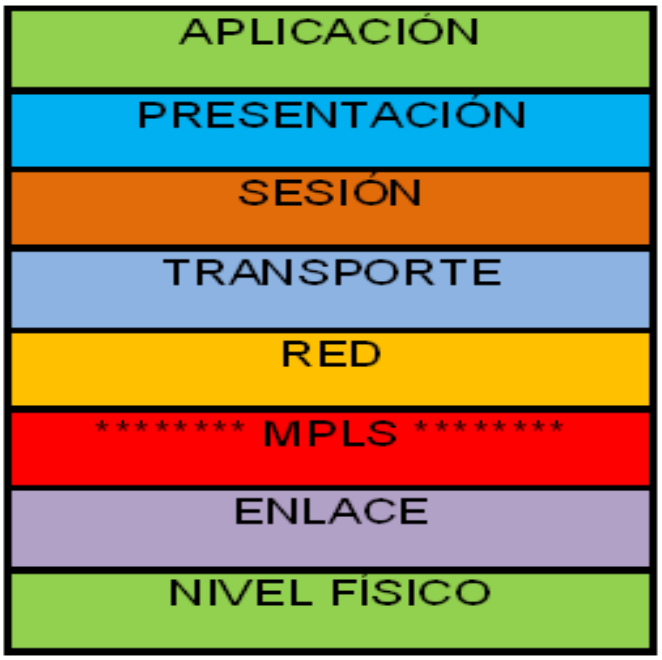
Fuente: Elaboración Propia

2.3 MPLS

2.3.1 Definición

MPLS es una tecnología de transmisión de paquetes de alto rendimiento que integra la gestión del rendimiento y el tráfico capacidades de capa de enlace de datos de conmutación con la escalabilidad, flexibilidad y rendimiento de la capa de red de enrutamiento. Permite a los proveedores de servicios para responder a los desafíos provocados por crecimiento explosivo y proporciona la oportunidad para que los servicios diferenciados sin necesitar la sacrificio de la infraestructura existente. La arquitectura MPLS es notable por su flexibilidad en los datos se pueden transferir a través de cualquier combinación de las tecnologías de capa 2, el apoyo que se ofrece para todos los protocolos de nivel 3 (ver Figura 2.6).

Figura 2.6 MPLS protocolo que opera entre la capa 2 y 3 del modelo OSI.



Fuente: Elaboración Propia

2.3.2 Principales ventajas de MPLS

Entre las ventajas de MPLS se destacan lo siguiente:

- Conmutación rápida de paquetes basado en etiquetas y no direcciones IP destino.
- Redes de clientes totalmente independientes (MPLS-VPN).
- Es multi-protocolo tanto hacia arriba (L3) como hacia abajo.
- Trabaja con QoS (Calidad de Servicio) basado en marcación de paquetes.
- La creación de una nueva VPN sólo implica la creación del circuito de acceso y del enrutamiento.
- Permite aplicar Ingeniería de Tráfico (TE).
- Uso eficiente del ancho de banda en accesos (full-mesh virtual).

2.3.3 Arquitectura de red MPLS

Una red MPLS consta fundamentalmente de los siguientes elementos:

- LSR (Label Switching Router). Elemento encargado de conmutar las etiquetas de los paquetes e intercambiar información con otros LSR de la red para establecer las asociaciones entre flujos y etiquetas.
- LER (Label Edge Router). Constituye el elemento de entrada y salida de la red MPLS, y se encuentra en la frontera de la misma. Se suele distinguir entre el equipo de entrada (ingress) y el de salida (egress).

- A la entrada de la red se realiza la función de procesar los paquetes, seleccionarlos y aplicar la etiqueta que les corresponda.
- En la salida de la red se encarga de suprimir las etiquetas y reenviar los paquetes hacia el destino utilizando el reenvío de la capa 3.
- FEC (Forwarding Equivalent Class). Conjunto de paquetes que son tratados de la misma forma en el proceso de reenvío, siguiendo la misma ruta con independencia de los destinos finales.
- LSP (Label Switched Path). Camino que se establece dentro de la red MPLS para todo tráfico de una misma FEC. Todos los paquetes identificados por esa FEC tendrán el mismo encaminamiento a través de la red.
- LIB. Forma parte del Plano de control cuya base de datos es usada por el LDP para distribución de etiquetas. Cuando esto ocurre los prefijos IP son asociados con sus entradas de etiquetas locales y el próximo salto con la información aprendida anteriormente.

Como en toda nueva tecnología, los elementos que definen la arquitectura de la misma deben ser estudiados intensamente ya que cumplen ciertas funciones y roles dentro de un dominio nuevo como es el caso de MPLS.

Elementos como LSRs y LERs son los principales dispositivos que ocupan una parte muy importante al momento de definir la arquitectura MPLS. Estos dispositivos cumplen con la función de intercambiar etiquetas dentro de una red MPLS. Los LSRs y LER en su estructura interna constan de dos componentes que requieren de profundo entendimiento como lo son: El Plano de Control y el Plano de Datos o de Envío.

2.3.4 Plano de control

En el Plano de Control en un LSR y un LER se encuentran los protocolos de encaminamiento y las tablas de encaminamiento.

El protocolo de encaminamiento se encarga de mantener la información de las actualizaciones de rutas entre los LSRs que se encuentra dentro de la red MPLS. Los protocolos de encaminamiento crean la tabla de enrutamiento IP que es usada para construir la base de información de envío (LIB). Esta tabla de enrutamiento IP en el plano de control es empleada para determinar el intercambio de etiquetas, donde los nodos adyacentes las intercambian para todas las subredes que están contenidas dentro de su tabla. Este intercambio realizado por el protocolo de distribución de etiquetas (LDP) crea la base de información de etiquetas (LIB).

2.3.5 Plano de Datos

A diferencia del Plano de Control, el Plano de Envío en los LSRs y LERs difiere un poco ya que en el LER se extienden las funcionalidades debido a que no solo cuenta con la tabla de envío de etiquetas sino que también trabaja con una tabla de envío IP.

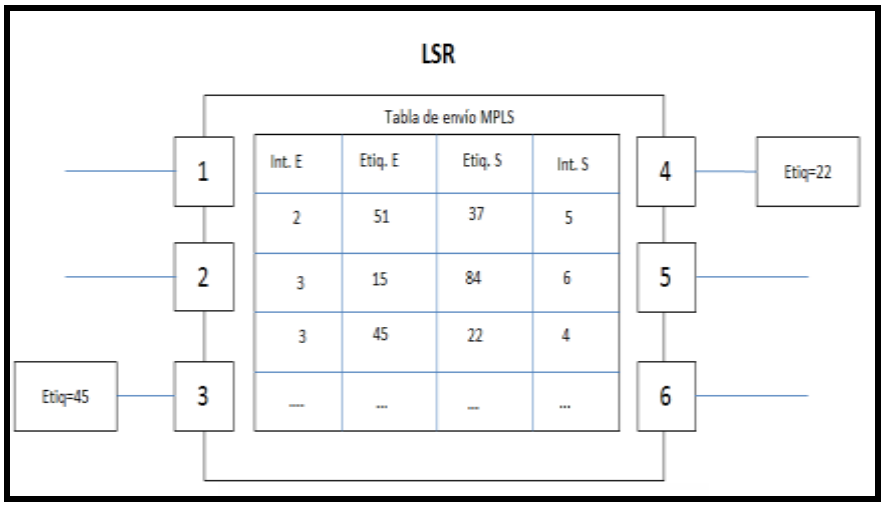
Por esta diferencia se describe separadamente las funcionalidades del Plano de Envío para el LSR y el LER.

LSR: En el proceso de enrutamiento IP-MPLS se utilizan las etiquetas que se intercambian entre LSRs adyacentes que ayudan a la creación de la tabla de envío de etiquetas en el Plano de Datos para enviar los paquetes etiquetados a través de una red MPLS.

LER: La tabla de envío IP estándar es construida en base a tabla de enrutamiento IP y es extendida con información de etiquetas. Esta extensión de componentes en el Plano de Datos se debe a que los paquetes IP entrantes a un LER pueden ser enviados como paquetes IP natos a un nodo no MPLS o pueden ser etiquetados y enviados a otros nodos MPLS. Además si los paquetes entrantes vienen etiquetados pueden ser enviados a otros nodos MPLS, o si su destino es un dominio no MPLS, su etiqueta puede ser removida y el chequeo de capa de red es realizado (envío IP) para encontrar el destino no MPLS.

En general, y para ambos casos, al crearse la tabla de envío de etiquetas cada entrada de la tabla contendrá una etiqueta de entrada y una etiqueta de salida, que corresponden a cada interfaz de entrada a un nodo MPLS. En el siguiente ejemplo (ver Figura 2.7) se ilustra el funcionamiento de un LSR del núcleo MPLS. En este caso un paquete que llega a un LSR por la interfaz 3 y con etiqueta 45, se le remueve esa etiqueta y se le asigna la etiqueta 22 que le indica que el paquete debe salir por la interfaz 4 hacia el siguiente LSR, de acuerdo con la información de la tabla.

Figura 2.7 Tabla de envío MPLS.



Fuente: Elaboración Propia

2.3.6 Etiquetas MPLS

La etiqueta MPLS es un identificador dentro de la cabecera de los paquetes que permite clasificar un paquete con respecto a la FEC a la que pertenece. Esta asociación FEC-etiqueta puede no ser unívoca, y puede utilizarse la misma etiqueta para diferentes FECs (por ejemplo para darle el mismo tratamiento a diferentes FEC

dentro de un segmento de la red), o pueden asociarse varias para la misma FEC (para realizar reparto de carga, por ejemplo).

MPLS añade una sobrecarga adicional para la comunicación entre routers adyacentes, sumada a la propagación de los prefijos de enrutamiento se agregan las funcionalidades de mantenimiento de las LIB junto con las tablas de adyacencia, generando un consumo de recursos extra. CEF, LDP y otros procesos contribuyen también al aumento de consumo de dichos recursos.

La distribución de etiquetas se lleva a cabo a través de un protocolo de distribución de etiquetas, como LDP particularmente MPLS LDP.
Hay que tener en cuenta que la arquitectura de MPLS permite dos formas de propagar la información necesaria:

1. Extender la funcionalidad de los protocolos existentes.
2. Crear nuevos protocolos dedicados a la tarea de intercambios de etiquetas.

Extender la funcionalidad de un protocolo existente requiere bastante tiempo y esfuerzo, especialmente en BGP y OSPF.

En una arquitectura MPLS la decisión de asignar una etiqueta en particular a un FEC es propiedad del LSR en cada host a lo largo del camino. El LSR anterior informa al siguiente LSR sobre etiquetas

decididas para esa FEC, esto implica esencialmente que las etiquetas se asignan en sentido ascendente hacia el destino.

La distribución de etiquetas puede ocurrir de dos formas:

- Unsolicited downstream
- Downstream-ondemand

Cualquiera de los dos casos ocurre ante un evento de convergencia, un vecino MPLS puede enviar (Unsolicited downstream) para solicitar que le envíen alguna actualización (Downstream-ondemand). Un ejemplo es cuando una etiqueta no está asociada a un FEC determinado.

2.3.7 LDP

LDP (Label Distribution Protocol) constituye un protocolo de control para distribuir la asociación de etiquetas a los LSRs. Se emplea para mapear las FECs a las etiquetas, a partir de las cuales se establecen los LSPs.

Las sesiones LDP se establecen siempre entre las parejas LSRs, conocidas como LDP Peers, no necesariamente adyacentes. Para el establecimiento de sesiones utiliza TCP, e incluye mecanismos para el descubrimiento de LDP Peers potenciales.

Es un protocolo escalable, de forma que la distribución de etiquetas es incremental. Cuando hay pocas etiquetas utiliza asignación

basada en downstream-on-demand y métodos de retención conservativos. Por el contrario cuando hay muchas etiquetas la asignación es unsolicited-downstream y la retención liberal.

Se definen cuatro tipos de mensajes LDP:

- Descubrimiento (Discovery messages). Utilizados para señalizar la presencia de LSRs en la red. Los mensajes se envían por difusión sobre UDP.
- Sesión (Session messages). Empleados para el establecimiento, mantenimiento y liberación de sesiones LDP (sesiones entre LDP Peers). Los mensajes se envía sobre TCP.
- Anuncio (Advertisement messages). Para crear, cambiar o borrar las asociaciones FEC-etiqueta.
- Notificación (Notification messages). Proporcionan información de avisos y señalización de errores.

2.3.8 Modo de operación MPLS

Para transportar los paquetes de datos a través de una red MPLS es necesario llevar a cabo una serie de pasos:

1. Descubrimiento de la topología de la red.
2. Creación y distribución de etiquetas.
3. Creación de los LSPs a partir del intercambio de etiquetas.
4. Reenvío de paquetes.
5. Eliminación de etiquetas a la salida de la red.

Descubrimiento de la topología.

El descubrimiento de la topología de la red se hace utilizando la propia información encaminamiento que manejan los protocolos estándar como OSPF, RIP, BGP, etc.

A partir de la información proporcionada por estos protocolos se construyen las tablas de encaminamiento en los LSRs.

Creación y distribución de etiquetas.

Los LSRs establecen las asociaciones FEC-etiqueta y construyen sus tablas (LIBs) antes de que comience el envío de tráfico. Para ello intercambian información de las asociaciones e información de las características de tráfico o capacidades MPLS mediante protocolos de distribución de etiquetas como LDP.

El contenido de las tablas establece el mapeo entre una etiqueta y un FEC, de forma que en función del interfaz y la etiqueta de entrada se puede obtener el interfaz, la etiqueta de salida y el siguiente salto. Las entradas de la tabla son actualizadas cada vez que se establece una nueva asociación FEC-etiqueta.

Creación de los LSPs

Los LSPs son creados en dirección inversa a la creación de entradas LIBs. El LER de entrada a la red MPLS utiliza la información de las tablas para encontrar cual es el próximo salto y con ello la etiqueta asociada a un determinado FEC.

La obtención de dicha asociación dependerá del método de distribución de etiquetas utilizando:

- Con downstream on demand el LER solicitará al siguiente salto la información de la etiqueta asociada a la FEC.
- Con unsolicited downstream puede disponer y de dicha información de los anuncios de asociación FEC-etiqueta recibidos de otros LSRs.
- En los saltos siguientes si el LSR no tuviera información de la etiqueta de salida asociada a un FEC la solicitaría al LSR del siguiente salto, y así sucesivamente hasta llegar al LER de salida de la red MPLS.

Reenvío de paquetes

Cuando un paquete entra en la red el LER de entrada podría no tener ninguna etiqueta para ese paquete. En ese caso tendrá que crear un LSP para el FEC al que corresponde el paquete, siguiendo el procedimiento indicado en el punto de creación de LSPs.

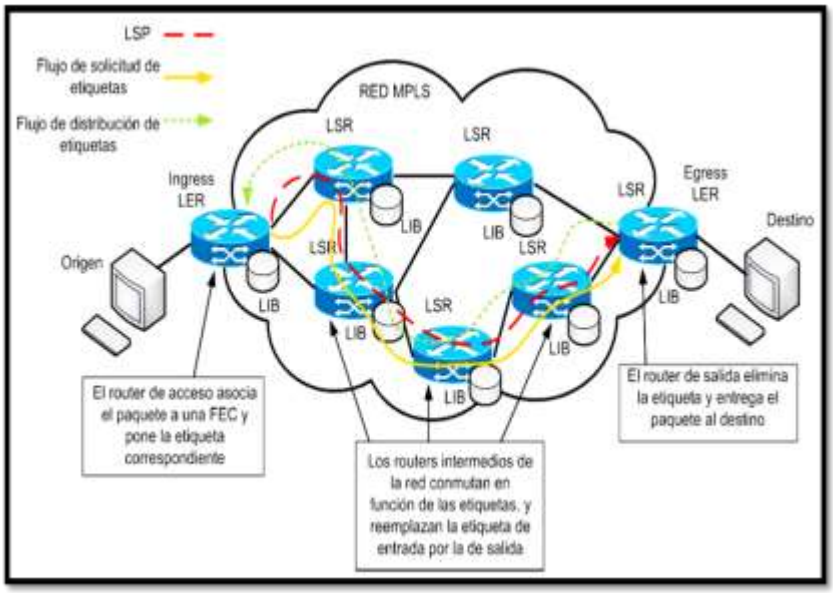
Se dispone de la etiqueta el LER de entrada la inserta en el paquete y la reenvía al LSR del primer salto. A partir de ese punto cada LSR examina la etiqueta del paquete recibido, la sustituye por la etiqueta de salida y la reenvía hacia el LSR del siguiente salto por el interfaz de salida especificado en la LIB.

Eliminación de etiquetas a la salida

Una vez que el paquete llega al LER de salida este elimina la etiqueta ya que el paquete está saliendo de la red MPLS, y lo entrega al destino.

El siguiente grafico (ver Figura 2.8) muestra el esquema de funcionamiento de una red MPLS y los flujos de información:

Figura 2.8 Funcionamiento de la red MPLS.



Fuente: Elaboración Propia

2.4 PROTOCOLOS DE ENRUTAMIENTO DINÁMICO PARA MPLS USADO EN EL PROYECTO.

MPLS al igual que las tecnologías actuales de TCP/IP, utiliza los protocolos de enrutamiento dinámico tales como: protocolos de Gateway Interior y Exterior IGPs y EGPs respectivamente.

El enfoque principal en este trabajo está en los protocolos de enrutamiento dinámico que se utilizan en el diseño de la red MPLS que se describirá en

secciones posteriores, para lo cual se diseña la topología usando principalmente OSPF y BGP

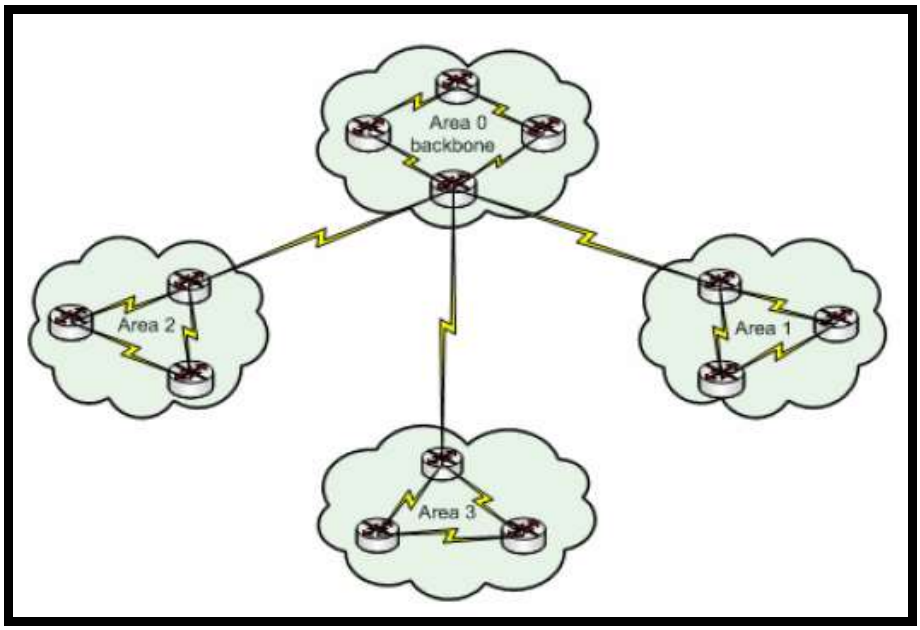
2.4.1 Protocolo OSPF

El protocolo de “solamente la ruta más corta primero” (OSPF), es un protocolo de estado de enlace. Se conoce que los protocolos de estado de enlace mantienen una base de datos de información de topología. El algoritmo de enrutamiento de estado de enlace mantiene información compleja sobre ruteadores lejanos y su interconexión. Los protocolos de estado de enlace generan una inundación (flooding) de información de ruta, que da a cada ruteador una visión completa de la topología de red. El método de actualización desencadenada por eventos permite el uso eficiente de un ancho de banda y una convergencia rápida. Los cambios de estado de un enlace se envían a todos los ruteadores en la red tan pronto como se produce.

El protocolo OSPF es uno de los protocolos de estado de enlace más importantes, y se basa en las normas de código abierto (Open Source), lo que significa que muchos fabricantes lo pueden desarrollar y mejorar. Es un protocolo complejo que se describe en varios estándares del IETF cuya implementación en redes más amplias presenta un verdadero desafío. Este es un protocolo de enrutamiento de Gateway Interior (IGP) que es preferido por todos ya que presenta soluciones de escalabilidad. OSPF puede ser usado

tanto en redes pequeñas como en redes grandes, en una sola área o en varias áreas (ver Figura 2.9).

Figura 2.9 Áreas OSPF



Fuente: Elaboración Propia

Las grandes redes OSPF utilizan diseño jerárquico, dado que varias áreas se conectan a un área de distribución o a una área cero, conocida como backbone. El enfoque del diseño para redes OSPF permite el control extenso de las actualizaciones de enrutamiento. La definición de área acelera la convergencia, limita la inestabilidad de la red y mejora el rendimiento.

OSPF utiliza un algoritmo de ruta más corta desarrollado por Dijkstra. Este algoritmo considera la red como un conjunto de nodos conectados con enlaces punto a punto. Cada enlace tiene un costo, un nombre y cuenta además con una base compleja de todos los enlaces y por lo tanto se conoce la información sobre la topología

física en su totalidad. Todas las bases de datos del estado de enlace, dentro de una determinada área, son idénticas. El algoritmo de ruta más corta calcula entonces la topología sin bucles con el nodo como punto de partida y examinando a su vez la información que posee sobre nodos adyacentes.

Para que los ruteadores OSPF puedan compartir la información de enrutamiento se requiere una relación de vecinos y se tiende a esto cuando un ruteador es adyacente con por lo menos uno en cada red IP a la cual está conectado. Los ruteadores OSPF determinan con que otros pueden intentar formar adyacencias tomando como base el tipo de red a las cuales están conectados, es decir, unos trataran de hacerse adyacentes con respecto a todos los ruteadores vecinos y otros tratan de hacerse adyacentes con respecto a solo uno de los ruteadores vecinos. Una vez formada la adyacencia, se intercambia la información del estado de enlace. Los equipos de enrutamiento con interfaces OSPF se reconocen tres tipos de redes:

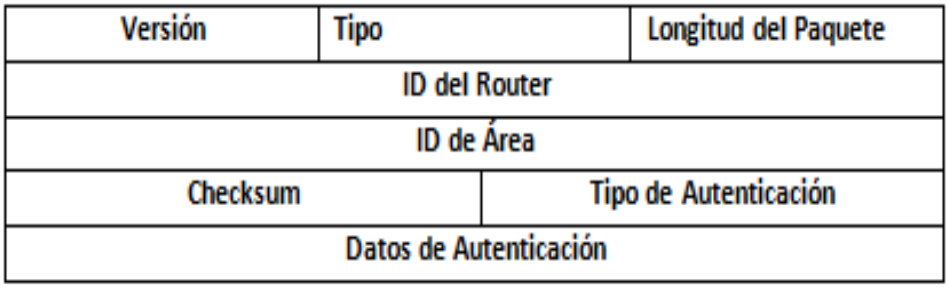
a) Multiacceso de Broadcast (ej. Ethernet)
b) Redes Punto a Punto
c) Multiacceso sin Broadcast (ej. Frame Relay)

Cuando un ruteador inicia un proceso de enrutamiento OSPF en una interfaz, envía paquetes de descubrimiento (Hellos) a intervalos regulares. En la capa de red los paquetes de descubrimiento se direccionan hacia la dirección Multicast 224.0.0.5 que equivale a

todos los ruteadores OSPF, los mismos que utilizan estos paquetes para iniciar nuevas adyacencias y asegurarse que entre los vecinos se mantenga el funcionamiento. Los mensajes de descubrimiento (Hellos) se envían cada 10 segundos por defecto en las redes multiacceso de broadcast y punto a punto. En las interfaces que se conectan a las redes como Frame Relay, el tiempo por defecto es de 30 segundos.

En las redes multiacceso el protocolo Hello elige un ruteador designado (DR) el cual se hace adyacente a todos los ruteadores del segmento broadcast y presenta un único punto de falla ya que todos los ruteadores del segmento envían el estado de enlace a este ruteador designado. Además de ello se elige un ruteador designado de respaldo (BDR). Aunque el paquete de descubrimiento es pequeño, consiste en un encabezado de paquete OSPF (Ver Figura 2.10), en donde para el paquete de descubrimiento, el campo de tipo se establece en 1.

Figura 2.10 Encabezado de Paquete OSPF.



Fuente: Elaboración Propia

El paquete de descubrimiento transmite información para la cual, todos los vecinos deben estar de acuerdo antes de que se forme una

adyacencia y que se pueda intercambiar información del estado de enlace.

Los ruteadores adyacentes pasan por una secuencia de estados, y deben estar en su estado completo antes de crear las tablas de enrutamiento y direccionar el tráfico. Cada elemento de actualización del estado de enlace (LSU). Esos LSAs describen todos los enlaces de los ruteadores quienes al recibirlas de sus vecinos las registran en la base de datos del estado de enlace.

Una vez completas las bases cada ruteador utiliza el algoritmo SPF para calcular la ruta con menor costo hacia un destino desconocido, luego la información de enrutamiento mantenida y cuando existe un cambio en el estado del enlace se produce la inundación notificándose así el cambio en la red.

2.4.2 Protocolo BGP

BGP (Border Gateway Protocol) es un protocolo de enrutamiento moderno diseñado para ser escalable y poder utilizarse en grandes redes creando rutas estables ente las organizaciones. BGP soporta VLSM, CIDR y summarización.

BGP es un protocolo de enrutamiento extremadamente completo, usado entre organizaciones multinacionales y en internet. El principal propósito de BGP es conectar grandes redes o sistemas autónomos. Las grandes organizaciones utilizan BGP como el vínculo entre

diferentes divisiones empresariales. BGP se utiliza en Internet para conectar diferentes organizaciones entre sí.

Es el único protocolo que actualmente soporta enrutamiento entre dominios, los dispositivos equipos y redes por una organización son llamados sistemas autónomos, AS. Esto significa independencia, es decir que cada organización es independiente de elegir la forma de conducir el tráfico y no se los puede forzar a cambiar dicho mecanismo. Por lo tanto BGP comunica los AS con independencia de los sistemas que utilice cada organización.

2.4.3 Manejo Básico de BGP

BGP asocia redes con sistemas autónomos de tal manera que otros router envían tráfico hacia el destino a través de un sistema autónomo. Cuando el tráfico llega a los routers frontera de BGP, es trabajo de los routers del IGP encontrar el mejor camino interno.

BGP es un protocolo path-vector, aunque mantiene muchas características comunes con los de vector-distancia. Las rutas son registradas de acuerdo con los sistemas autónomos por donde está pasando y los bucles son enviados rechazando aquellas rutas que tienen el mismo número de sistema autónomo al cual están llegando.

Los vecinos BGP son llamados peers, estos no son automáticamente descubiertos sino que deben estar predefinidos. Existen cuatro tipos de mensajes en BGP para que la relación sea construida y posteriormente mantenida:

- Open
- Keeplive
- Update
- Notification

Cuando el proceso de BGP comienza se crean y mantienen las conexiones entre los peers utilizando el puerto TCP 179 a través de mensajes BGP open, posteriormente las sesiones son mantenidas enviando constantemente mensajes keepalive y la información de peer se mantiene en una tabla de vecinos separada. Si un peer es reseteado, este envía un mensaje de notification para indicar la finalización de la relación. Cuando se establece por primera vez la relación de vecindad, los routers BGP intercambian sus tablas de enrutamiento por completo utilizando mensajes update. Finalmente solo se enviaran actualizaciones incrementales cuando existan cambios en la red.

2.4.4 Jerarquías BGP

Otros protocolos de enrutamiento han sido creados de tal manera que soporten sumarizaciones y para que se pueda organizar la red de manera jerárquica. Las organizaciones no están distribuidas

jerárquicamente, por lo tanto BGP debe trabajar con cualquier topología que le sea dada. BGP se beneficia de la sumarización de la misma manera que los demás protocolos de enrutamiento, es decir, menos consumo de recursos de memoria y CPU, y tablas de enrutamiento más pequeñas.

Una red BGP optimizada será altamente sumarizada pero no necesariamente de manera jerárquica. BGP por naturaleza proporciona un resumen de las rutas claves identificando los posibles caminos entre sistemas autónomos. Debido a que los AS no están bien organizados, las redes BGP reflejan esa falta de organización. BGP puede ser implementado entre redes o dentro de una red. BGP detecta los bucles mirando las rutas de las AS-path.

2.4.5 Tablas de BGP

El enrutamiento a través de BGP involucra tres tipos de tablas:

- Tabla de vecinos
- Tabla de BGP
- Tabla de enrutamiento IP

Las rutas de BGP son mantenidas en una tabla de BGP separada y las mejores rutas son pasadas a la tabla de enrutamiento. A diferencia de otros protocolos de enrutamiento, BGP no utiliza una métrica. En su lugar BGP emplea un proceso de 10 pasos para seleccionar las rutas dependiendo de una serie de propiedades.

BGP soporta herramientas como route-maps y listas de distribución que permiten al administrador cambiar el flujo de tráfico basado en los atributos de este protocolo.

2.4.6 MP – BGP (BGPv4)

Anteriormente BGPv4 era capaz de llevar solamente información para trafico IPv4. Sin embargo como se define en el RFC 2283, ya existen extensiones que permiten que BGPv4 lleve información de enrutamiento para múltiples protocolos de capa de red (IPv6 IPX, etc.). Las extensiones son compatibles con versiones anteriores, es decir, un ruteador que soporte las extensiones puede operar con otro ruteador que no soporte las extensiones.

Esta extensión del protocolo BGPv4 existente se utiliza para anunciar rutas VPN cliente entre los routers de tipo PE que se aprendieron de los routers de tipo CPE conectados. Estas rutas de los clientes pueden ser aprendidas a través de las rutas normalizadas de BGPv4, RIPv2, estáticas u OSPF.

MP-BGP solo se requiere dentro de la columna vertebral del proveedor de servicios. Por lo tanto, todas las sesiones de MP-BGP son sesiones internas de BGP, interna porque la sesión se da entre dos routers que pertenecen al mismo sistema autónomo.

MP-BGP se requiere dentro de la arquitectura MPLS-VPN por que la actualización BGP necesita llevar más información que solo una dirección IPv4 como por ejemplo: dirección VPN-IPv4, información de etiquetas MPLS, comunidades BGP extendidas y comunidades posiblemente estándar BGP.

2.5 MARCO CONCEPTUAL

En este capítulo II citaremos a continuación una breve descripción de los términos técnicos que se usan a lo largo de este proyecto, para tener mayor conocimiento de los mismos.

ADSL: Consiste en una transmisión analógica de datos digitales apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o abonado.

AS: Se define como un grupo de redes IP que poseen una política de rutas propia e independiente.

ATM: El Modo de Transferencia Asíncrona o Asynchronous Transfer Mode (ATM) es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones.

BACKBONE: Son las principales conexiones troncales de Internet. Está compuesta de un gran número de routers comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo mediante cables de fibra óptica.

BGP: Border Gateway Protocol, es un protocolo mediante el cual se intercambia información de encaminamiento o ruteo entre sistemas

autónomos. Por ejemplo, los proveedores de servicio registrados en internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

BROADCAST: Es una forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

CEF: Cisco Express Forwarding. El uso de CEF es un prerrequisito para que el router pueda soportar MPLS, sin embargo un router puede utilizar CEF sin tener habilitado MPLS.

CERC: CE Routing Communities

CIDR: Permite una mayor flexibilidad al dividir rangos de direcciones IP en redes separadas

CoS: Clases de servicio, sirve para redistribuir el ancho de banda de un enlace y clasificarlo de acuerdo al tipo de dato.

CPE: Equipo Local del cliente, es un equipo de telecomunicaciones usado tanto en interiores como en exteriores para originar, encaminar o terminar una comunicación

EBGP: exterior Border Gateway Protocol

EGP: El Exterior Gateway Protocol (EGP) es un protocolo estándar usado para intercambiar información de enrutamiento entre sistemas autónomos.

FEC: Forwarding Equivalent Class, conjunto de paquetes que son tratados de la misma forma en el proceso de reenvío, siguiendo la misma ruta con independencia de los destinos finales.

FRAME RELAY: Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de

tramas o marcos (“frames”) para datos, perfecto para la transmisión de grandes cantidades de datos.

FULL MESH: Topología de red en el que se puede aplicar el término todos contra todos.

GATEWAY: Una pasarela, puerta de enlace o gateway es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

HUB: Dispositivo concentrador para compartir una red de datos.

IBGP: Internal Border Gateway Protocol

IETF: Es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad.

IGP: Protocolo de pasarela interno, hace referencia a los protocolos usados dentro de un sistema autónomo.

IP: Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del Modelo OSI

IPsec: Conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando o cifrando cada paquete IP en el flujo de datos.

IPX: Es una familia de protocolos de red desarrollados por Novell y utilizados por su sistema operativo de red NetWare.

ISP: proveedor de servicios de Internet, es una empresa que brinda conexión a Internet a sus clientes.

LAN: Red de área local.

LDP: Protocolo de distribución de etiquetas (LDP) es un protocolo en el que los routers son capaces de conmutación de etiquetas multiprotocolo (MPLS) información de asignación de etiquetas de cambio.

LER: Label Edge Router, elemento que inicia o termina el túnel (pone y quita cabeceras). Es decir, el elemento de entrada/salida a la red MPLS. Un router de entrada se conoce como Ingress Router y uno de salida como Egress Router. Ambos se suelen denominar Edge Label Switch Router ya que se encuentran en los extremos de la red MPLS.

LIB: Base de información de etiquetas (LIB) es la tabla de software mantenido por IP / MPLS con capacidad routers para almacenar los detalles de puerto y la etiqueta del router MPLS correspondiente al hacer estallar / empujó paquetes MPLS entrantes / salientes.

LSP: Label Switched Path, Camino que se establece dentro de la red MPLS para todo tráfico de una misma FEC. Todos los paquetes identificados por esa FEC tendrán el mismo encaminamiento a través de la red.

LSR: LSR (Label Switching Router): elemento que conmuta etiquetas.

MPLS: (Multiprotocol Label Switching) es un mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031.

OSI: Sistemas de interconexión abiertos, es el modelo de red descriptivo, que fue creado por la Organización Internacional para la Estandarización (ISO) en el año 1980.

OSPF: Es un protocolo de enrutamiento jerárquico de pasarela interior.

P (Provider): Router que estaría totalmente dentro de la red MPLS. No tendría ningún enlace conectado directamente a un CPE.

PE (Provider Edge): Equipo que comparte al menos un enlace con un CPE y otro dentro de la red MPLS. Se encarga de introducir las VRFs y realizar la función de POP.

POP: Punto de presencia, es un punto de interconexión entre las instalaciones de comunicación suministradas por la empresa telefónica y la instalación de distribución principal del edificio.

PSTN: Red telefónica conmutada, se define como el conjunto de elementos constituido por todos los medios de transmisión y conmutación necesarios para enlazar a voluntad dos equipos terminales mediante un circuito físico que se establece específicamente para la comunicación y que desaparece una vez que se ha completado la misma.

QoS: Calidad de Servicio, es el rendimiento promedio de una red de telefonía o de computadoras, particularmente el rendimiento visto por los usuarios de la red.

RIP: Routing Information Protocol, es un protocolo de puerta de enlace interna o IGP (Interior Gateway Protocol) utilizado por los routers (encaminadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

RPV: Red privada virtual, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet.

TCP: Protocolo de control de transmisión.

UDP: Protocolo de datagrama de usuario.

UNICAST: Es el envío de información desde un único emisor a un único receptor.

VLSM: Mascara de subred de tamaño variable.

VPN: Tiene la misma definición de la RPV.

VRF: Virtual routing and forwarding.

WAN: Red de área amplia.

CAPÍTULO III

DESARROLLO DE LA METODOLOGÍA

3.1 DESCRIPCIÓN DEL PROYECTO

Este proyecto está enfocado básicamente en la interconexión a nivel WAN que van a tener las sedes remotas y la principal de la empresa, aprovechando la red pública de un proveedor de servicios. La empresa solo requiere el acceso WAN hacia un proveedor de servicios, en la actualidad no requiere de otras tecnologías que se pueden adicionar como lo es la Calidad de Servicio, es por esto que solo se está enfocando este proyecto en el acceso de la empresa como cliente final

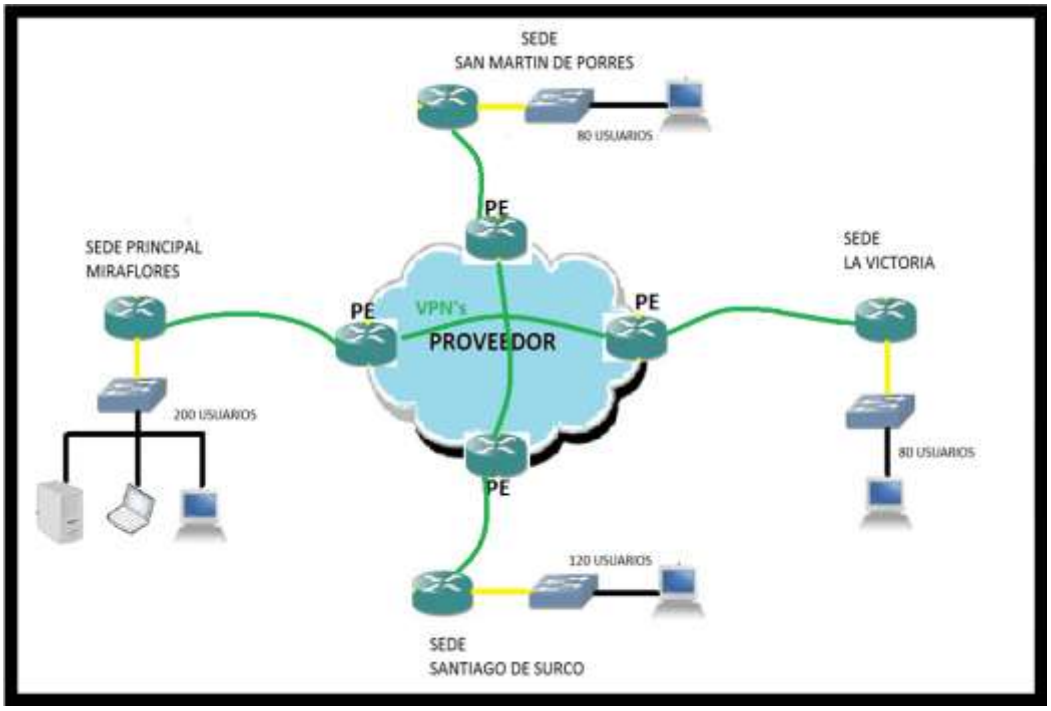
Para la solución a la problemática actual que presenta la empresa se implementa una red bajo una plataforma VPN-MPLS con la cual integraremos sus servicios e interconectaremos sus sedes remotas, aprovechando sus bondades de MPLS como: modelo acoplado e inteligente, ya que MPLS reconoce la existencia de VPNs (Redes Privadas Virtuales), se minimizará la complejidad de los túneles, fácil provisión de servicios ya que cada conexión afecta a un solo router, mayor escalabilidad, garantías en la seguridad, acceso al requerimiento del cliente, y alta disponibilidad de esta forma se disminuirá los costos.

En la siguiente gráfica (ver Figura 3.1) se puede ver la interconexión centralizada que va a existir entre las sedes remotas y la principal, esta comunicación se implementará mediante o a través de la red MPLS de un proveedor de servicios, esta red MPLS es transparente para el cliente final ya

que va a actuar como si fuese una conexión punto a punto (enlace lógico) (ver Figura 2.5). Las conexiones punto a punto (Principal → sedes remotas) se va a realizar mediante una VRF (Virtual Routing Forwarding) que se crea en la Nube MPLS específicamente en los routers de tipo PE, la cual garantiza una conexión segura y libre de tráfico que no corresponde a la Data del cliente.

Para cada empresa se maneja una distinta VRF, ya que cada empresa maneja un enrutamiento distinto al otro, esto te da la seguridad que el tráfico de una empresa no se mezcle con la de otra empresa y sea perjudicial para los mismos.

Figura 3.1 Topología futura de Red de la empresa



Fuente: Elaboración Propia

3.2 DISEÑO DE LA TOPOLOGÍA DE RED WAN

En este capítulo se realizará un diseño de la parte WAN del cliente desde el punto de vista del proveedor de servicios, esta es la mejor manera de poder descubrir, fundamentar y explicar bien las bondades en la parte del acceso

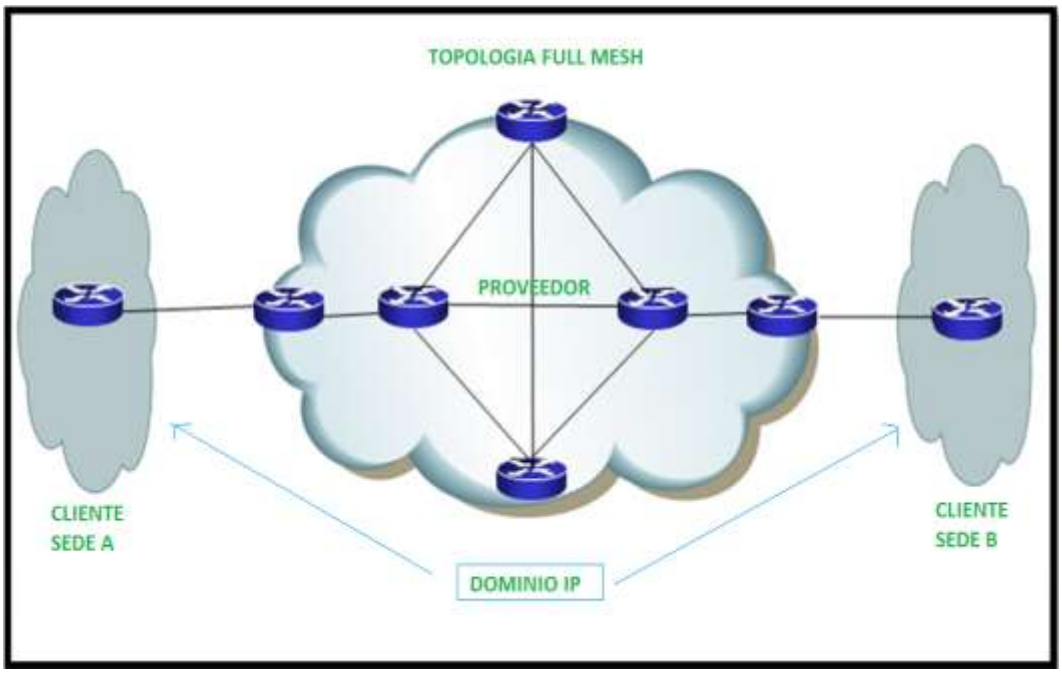
que puede ofrecer una red MPLS de un proveedor de servicios a un cliente. En este caso el cliente es una empresa de consumos que se le propone contar con una Red Privada Virtual mediante el Dominio de un Proveedor de Servicios.

Cuando se trata de diseñar una red WAN desde el punto de vista del proveedor de servicios, se deben considerar aspectos importantes ya que al momento de implementar es necesario asegurarse que el diseño escogido fue la topología más adecuada con los equipos de buen desempeño que puedan ofrecer, confiabilidad y robustez, a las empresas que deseen utilizar la red de un proveedor para el transporte de su información. Las consideraciones de diseño para la red presentada (ver Figura 3.2) se hacen pensando en una red mallada completa (Full Mesh), construida con equipos de la plataforma Cisco 7200, de tal forma que un proveedor con un diseño Full Mesh en su núcleo de red pueda ofrecer garantías de envío de información y que además cuente con caminos adicionales y redundantes según se dé el caso de que falle algún nodo en el núcleo de la nube.

En referencia al tipo de topología Full Mesh que se usará, se debe a que los grandes proveedores de servicios que existen en el Perú, utilizan dicha topología dentro de sus dominios MPLS y es lo que necesariamente se le ofrecerá a la empresa. Pues al hacer la comparación con otras topologías como Partial Mesh o Hub and Spoke, estos no brindan tanta confiabilidad y disponibilidad como lo tiene la topología Full Mesh.

Lo mismo ocurre con los routers Cisco que se usarán en este proyecto tanto en la parte del proveedor de servicios como en el cliente, por lo que el proveedor que se toma como referencia para el desarrollo del proyecto tiene en la nube únicamente routers Cisco. Por su parte Cisco es una empresa reconocida mundialmente en el campo de las redes, en el que brinda confiabilidad y seguridad en los equipos que están en el mercado.

Figura 3.2 Topología full mesh

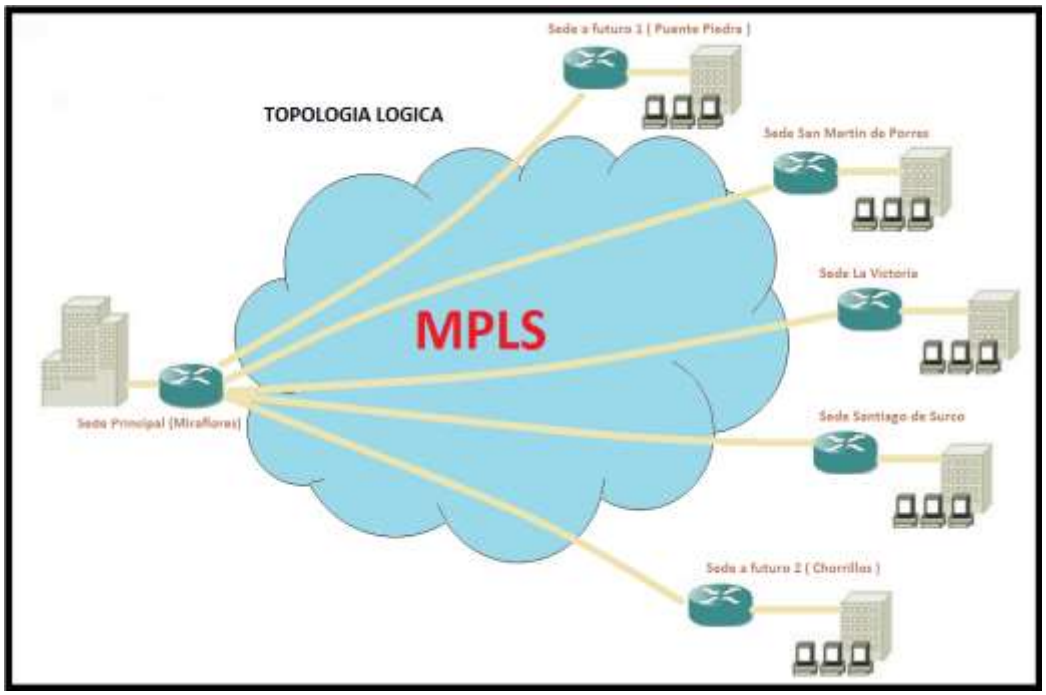


Fuente: Elaboración Propia

En el caso de la empresa para enviar información a través de la nube MPLS se debe ofrecer una topología lógica de tal manera que haga parecer que se cuenta con enlaces dedicados desde un sitio matriz / principal hacia cada una de las agencias con las que pueda contar. Una red diseñada con MPLS que será utilizada para el envío de información debe ser transparente para la empresa (cliente) dado que, al contar con una topología definida se puede alcanzar los destinos por diferentes caminos y así hacer del transporte de la

información confiable. La siguiente figura (ver Figura 3.3) de una referencia de cómo se conectan las agencias de la empresa y las posibles sedes a implementar con su matriz para ser servidos de las distintas aplicaciones que van a utilizarse tales como: correo, transferencia de archivos, voz, mensajería, aplicaciones transaccionales, etc.

Figura 3.3 Topología que define la conectividad de la empresa con sus Agencias-Sucursales



Fuente: Elaboración Propia

Según la Figura se puede notar que la matriz de la empresa (Matriz Miraflores) puede ofrecer aplicaciones a sus agencias por medio de un dominio público MPLS que un proveedor de servicios ofrece, buscando como solución más económica la implementación de VPNs de capa 3 de tal manera que se piense que estos canales VPN son enlaces dedicados.

3.2.1 Topología Full Mesh

Como se puede observar (ver Figura 3.2), el arreglo de los equipos de red de un proveedor es una topología de malla completa en el Core. Este tipo de arreglo (full mesh) se caracteriza por tener todos sus nodos conectados entre sí para el intercambio de información. Dada su gran cantidad de redundancias en lo que se refiere a enlaces, este tipo de topologías es usual en los Backbones de los proveedores. Al existir redundancia de enlaces se garantiza una estructura de Backbone confiable, capaz de manejar grandes cantidades de información.

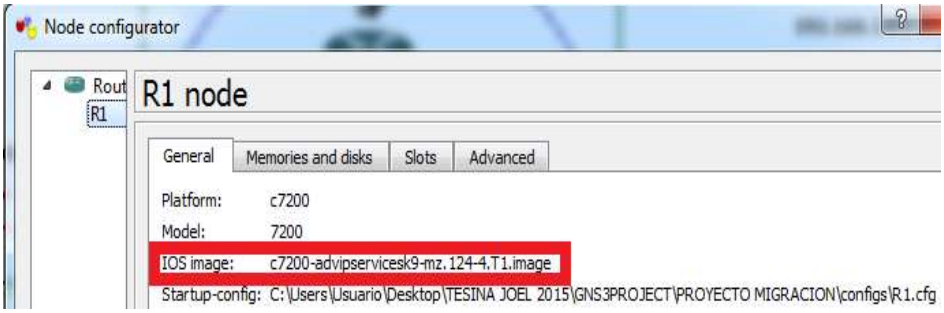
Para el diseño de una red MPLS de un proveedor, es necesario siempre estudiar la posibilidad de crear un núcleo mallado completo (full mesh), dado que pueden existir situaciones en las que se presenten problemas en algún enlace y es necesario contar con respaldos que reemplacen a la ruta principal. Además se considera este tipo de topologías para atender los requerimientos de usuarios que demandan gran uso de ancho de banda mediante el uso de aplicativos que así lo requieran (Voz, Video, Datos).

3.2.2 Herramientas representativas en el diseño de la Red MPLS

Una red MPLS está constituida por elemento de núcleo (P – Routers o LSRs) y elementos de frontera (PE – Routers o LERs). En el diseño utilizare router Cisco 7200 en los P y PE los cuales realizaran la distribución y enrutamiento de la red, adicionalmente estos routers

servirán para realizar el proceso MPLS, tiene un sistema operativo IOS c7200-advipservicesk9-mz.124-4.T.bin (ver Figura 3.4) muestra en para uso de proveedores de servicio, el mismo que cuenta con las funcionalidades necesarias, cualidades de procesamiento y gestión de recursos adecuadas a usarse en una red MPLS.

Figura 3.4 IOS que utilizara en los Router



Fuente: Elaboración Propia

3.2.3 Configuración de los protocolos en el aplicativo GNS3

En la topología elegida como modelo de la red MPLS será necesario el uso de herramientas de aplicación que simulen el comportamiento de la red interaccionando con entidades o protocolos de tal manera que se pueda estudiar el comportamiento del tráfico que circulará por la nube MPLS. Las características que deben presentar las herramientas de simulación, deben acoplarse a los requerimientos que demande una Red, para que de esa forma las condiciones y problemas que se presenten, se tomen en cuenta en ambientes de implementación con equipamiento real. La herramienta que se utiliza para este diseño de red VPN-MPLS el cual destaca por ser:

Configurable: De tal manera que se pueden alterar parámetros de red y de tráfico que circula a través de ella.

Analizable: Porque los resultados revelan el comportamiento de la red y los posibles problemas que puedan surgir.

Portable: Es de código abierto y fácil de ejecutar en varios sistemas operativos.

3.3 SOFTWARE GNS3

Gns3 es un software simulador libre creado para diseñar topologías de redes desde las más básicas hasta las complejas, simula router Cisco y sus diferentes conexiones.

Gns3 usa Dynamips los cuales proporciona los IOS de los equipos Cisco directamente en los routers simulados lo que permite realizar las configuraciones exactamente igual como en los equipos físicos conectado a un cable consola y usando un cable terminal.

Gns3 es una herramienta muy útil para estudiantes que deseen aprender y entender las diferentes topologías de redes y sus protocolos, además es de mucha importancia para todos los futuros profesionales que desean realizar laboratorios y rendir exámenes como CCNA y CCNP.

3.3.1 Ventajas de GNS3 sobre Packet Tracert

Gns3 trabaja en tiempo real en la computadora gracias a las imágenes de los IOS, sin embargo packet tracert emula los IOS en su forma básica, además que no puede usar procotolos como MPLS, BGP y entre otras.

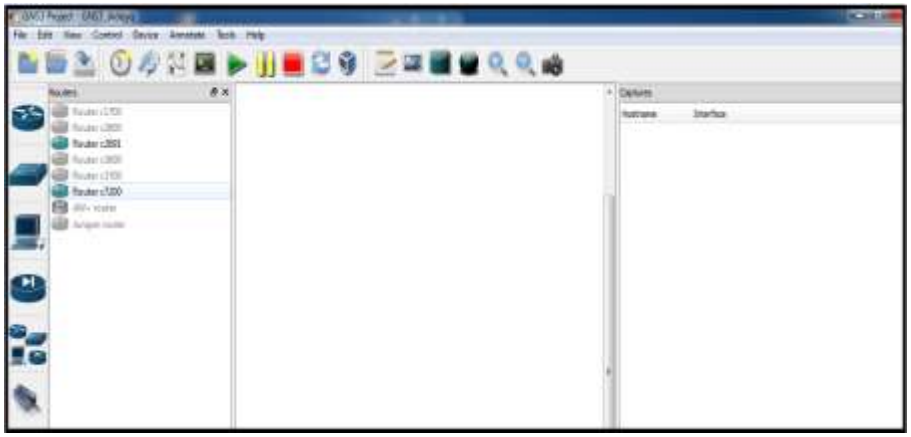
3.3.2 Desventajas de GNS3

Gns3 no puede usar una gran cantidad de router debido a su alto consumo en la memoria RAM, esto hace que el procesamiento de la computadora se vuelva lenta.

3.3.3 Introducción a la simulación

El presente proyecto muestra de manera sencilla la simulación de la tecnología MPLS, se enseñara las topologías básicas de MPLS, y la configuración básica de la misma (ver Figura 3.5).

Figura 3.5 Interfaz gráfica de aplicativo GNS3



Fuente: Elaboración Propia

3.3.4 Barra de Herramientas del GNS3

Dentro del aplicativo GNS3 tenemos algunas barras de herramientas, entre las cuales podemos mencionar las siguientes:

Barra general

En esta barra de herramienta podemos tener muchas opciones de trabajo como (ver Figura 3.6):

- Crear nuevos diseños

- Abrir nuevos proyectos
- Guardar proyectos
- Guardar topologías
- Mostrar etiquetas a las interfaces
- Conexión a interfaces LAN/WAN

Figura 3.6 Barra de herramientas General

Fuente: Elaboración Propia

Barra simulación

Esta barra nos permite ver opciones de inicio y parada de emulación así como también el acceso a consola para la administración de los equipos (ver Figura 3.7)

Figura 3.7 Barra de herramientas de simulación

Fuente: Elaboración Propia

Barra de dibujo

Esta barra nos permite agregar notas en el diseño topológico así como también insertar imágenes prediseñadas como figuras geométricas como cuadrado y círculos para agrupar algunos equipos que identifiquen alguna área específica (ver Figura 3.8).

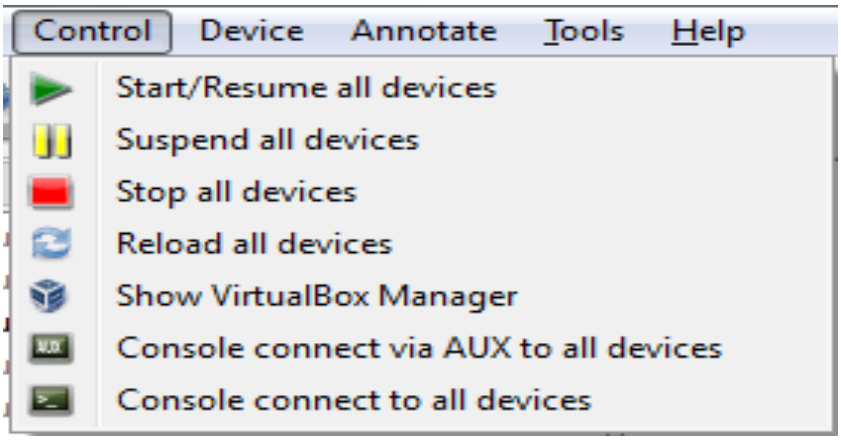
Figura 3.8 Barra de herramientas de dibujo

Fuente: Elaboración Propia

Barras de menús de GNS3

Al igual que la mayoría de aplicaciones dentro del menú principal encontramos muchas de las opciones que se realiza en las barras de herramientas, destacándose las de edición como la de control (ver Figura 3.9).

Figura 3.9 Barra de herramientas de Menús



Fuente: Elaboración Propia

3.4 DESARROLLO DEL DISEÑO

Para cumplir con el objetivo establecido de la red VPN MPLS, se brindará niveles de seguridad entre los enlaces; el diseño a simular se mostrará a continuación con sus respectivas configuraciones en todos los equipos Backbone y el cliente.

3.4.1 Etapas a simular

Las etapas a simular son aquellos elementos partícipes de la topología MPLS y los elementos del dominio IP que forman parte de la red de las empresas. Estos dispositivos son simulados con la herramienta GNS3 para lo cual se crea un archivo que representa todas las conexiones necesarias entre los elementos pertenecientes a la red MPLS.

Tanto los ruteadores de frontera como los ruteadores del núcleo de la red cuentan con funcionalidades de envío MPLS necesarias para ofrecer la seguridad al momento de transmitir la información proveniente de los dispositivos localizados en el lado de los cliente que hacen uso de esta red para comunicarse con sus sitios remotos. Virtualmente se simula los ruteadores de serie Cisco 7200 para la nube MPLS y los ruteadores de la serie Cisco 2800 para representar a los clientes. Aunque la herramienta de simulación permite ejecutar muchas plataformas más livianas para el caso de los clientes, las elegidas se las ha escogido por el desempeño que poseen al momento de la gestión de información.

3.4.2 Configuración de los routers de la red

Se tiene que seguir un orden sistemático para los pasos que se tomaran para que estos dispositivos realicen las funciones de enrutamiento de información, gestionando además recursos dentro del dominio en el que trabajan y mostrando robustez en sus funcionalidades al momento de recibir grandes volúmenes de datos.

En la presente sección se da a conocer los mecanismos para la configuración de enrutamiento y manejo de etiquetas que se dan en una Red IP – MPLS que utiliza herramientas de buen desempeño como lo son: protocolos de enrutamiento de estado de enlace (IGPs), protocolos de Frontera y Exteriores (EGPs) y protocolos de distribución de etiquetas.

3.4.3 Configuración de los P – Routers

Los dispositivos ubicados en el núcleo de la red MPLS como lo son los P – Routers (LSRs), son aquellos en los que se gestiona la información y se decide cual es la mejor ruta para alcanzar un destino. En el núcleo de una red deben existir redundancias y los dispositivos que conforman esta parte de la topología deben contar con entidades que le permitan mantener un mapa de las conexiones adyacentes (estado de enlace), a cada uno de ellos.

Estos protocolos de estado de enlace muy conocidos como protocolos de la ruta más corta (SPF) son eficaces a la hora de mantener la información necesaria de cambios en los sistemas y son muy usuales en los Backbones de los grandes proveedores de servicio. Al implementar estas herramientas en los dispositivos de red se asegura la estabilidad, flexibilidad y seguridad a la hora de mantener operativos los enlaces principales y de respaldo que pueda poseer una red.

En esta configuración se aplica a todos los router Cisco de nuestro CORE, en mi caso solo tomare 1 por motivos de capacidad de memoria de la Computadora donde se implementa, protocolo que usare es el OSPF.

3.4.3.1 Los Protocolos de Enrutamiento

En MPLS para lo correspondiente a protocolos de enrutamiento en el núcleo de la red, es muy usual aplicar el Protocolo de solamente la ruta más corta primero (Only Shortest Path First - OSPF), ya que el mismo obliga a que los dispositivos de red mantengan una coordinación entre ellos mientras se encuentren en una misma área. En la sección de configuración de OSPF se detalla los pasos necesarios para la configuración de esta herramienta de enrutamiento, que es además muy poderosa y eficiente a la hora de establecer un enlace que pudo haberse perdido en algún momento.

- **Protocolo OSPF**

El enrutamiento OSPF utiliza la definición de áreas. Cada ruteador contiene una base de datos completa de los estados de enlace de un área específica, a la misma se le puede asignar un número comprendido entre 0 y 65535. Sin embargo, al área correspondiente

al Backbone se le suele numerar con el cero por que en caso de que existan numerosas áreas utilizando OSPF, estas deben conectarse a la principal.

La configuración de este protocolo requiere que se active el proceso en un ruteador con las direcciones de red y la información de área especificada. Las direcciones de red se configuran con una máscara conocida como wildcard, más no, con una máscara de subred como se ejecuta en otros tipos de enrutamiento. La máscara wildcard representa las direcciones de enlaces o de dispositivos terminales que pueden estar presentes en un segmento específico.

El ID de proceso es un número que se utiliza para identificar un proceso de enrutamiento OSPF en un ruteador, en el cual pueden coexistir múltiples procesos que utilicen este protocolo. Es necesario que cada red, subred o dirección de interfaz, al ser añadida a una tabla de enrutamiento OSPF, se le identifique el área al que pertenece. En la Tabla 3.1 se especifican los comandos de configuración de OSPF y se describe la utilidad de los mismos.

Tabla 3.1. Configuración de Enrutamiento OSPF

Comandos	Propósito
Router(config)# **router ospf** <*process-id*>	Habilita en enrutamiento OSPF.
Router(config - router)# **network** <*ip-address*> <*wildcard-mask*> **area** <*area-id*>	Define una interfaz en la cual se ejecuta OSPF y señala el área para aquella interfaz.

Fuente: Elaboración Propia

- **Habilitando MPLS**

Una vez configurado el encaminamiento de paquetes IP y teniendo presente que se tiene una Red MPLS, es necesario habilitar las funcionalidades multiprotocolo las cuales permitan que a los paquetes IP se les añada etiquetas para el envío MPLS.

Se configura también el protocolo de distribución de etiquetas sobra las interfaces conectadas al núcleo MPLS con el fin de habilitar el intercambio de etiquetas entre el router, esto se hace a través del comando mpls ip.

Con esta configuración el ISP apenas está iniciando su operación y como no tiene usuarios conectados, el tráfico es interno.

Mediante la Tabla 3.2 se indican los comandos para la configuración de MPLS en un ruteador Cisco 7200.

Tabla 3.2. Configuración MPLS

Comandos	Propósito
Router(config)# **ip cef**	Habilita de manera global una funcionalidad de envió y conmutación propietaria de cisco (Requerida).
Router(config)# **mpls ip**	Habilita el envió MPLS de paquetes de longitud IPv4, normalmente caminos enrutados por la plataforma (Requerida).
Router(config)# **interface** <type> <slot/port>	Permite ingreso al modo de configuración de interfaz (Requerida).
Router(config-if)# **mpls ip**	Habilita el envió MPLS de paquetes de longitud IPv4, normalmente caminos enrutados para una interfaz en particular (Requerida).

Fuente: Elaboración Propia

- **Intercambio de Etiquetas – LDP**

Para la distribución de etiquetas en las interfaces es necesario especificar el protocolo que se utilizara y que de esa manera los dispositivos vecinos realicen el intercambio correspondiente y la negociación para luego crear las respectivas tablas que indican las etiquetas correspondientes a los paquetes entrantes. El comando presentado mediante la Tabla 3.3 detalla la sencilla configuración para la distribución de etiquetas en una interfaz.

Tabla 3.3. Configuración de señalización LDP

Comandos	Propósito
Router(config-if)# **mpls label protocol** <ldp|tdp|both>	Configura el protocolo de distribución de etiquetas en una interfaz.

Fuente: Elaboración Propia

3.4.4 Configurando los PE – Routers

Los dispositivos de red ubicados en la frontera MPLS, son aquellos que se encargan de recibir los paquetes y añadir la etiqueta correspondiente a su FEC para que pueda ser enviado a través del dominio. Estos dispositivos trabajan por lo general con varios protocolos de enrutamiento ya que los mismos cumplen funciones como: enrutar paquetes desde y hacia los clientes, enrutar paquetes hacia los ruteadores del núcleo de red o hacia otros dominios por medio de otros dispositivos de frontera.

En este caso el protocolo que se usara es BGP y tablas VRF con el propósito de que las rutas de los CPE alcancen a las rutas de los PE.

3.4.4.1 Los Protocolos de Enrutamiento

Dado que los dispositivos de frontera trabajan en dos ambientes diferentes (IP y MPLS), es necesario que estos trabajen con enrutamiento para los dos entornos. Al ser los encargados de recibir un paquete desde un dominio IP ellos deben utilizar un protocolo que les permita la interconexión con un mundo exterior

diferente del dominio al que pertenecen. Cuando se etiqueta el paquete IP el siguiente paso es encaminarlo dentro del dominio MPLS, para lo cual debe utilizar una entidad que le permita la comunicación con sus vecinos dentro de la misma red los cuales son los ruteadores del núcleo.

- **Protocolo OSPF**

Este protocolo de estado de enlace es el encargado de establecer la comunicación entre los dispositivos de frontera (PE) y los dispositivos del núcleo de red (P). Su configuración es idéntica a la mostrada en la Tabla 3.1 ya que estos ruteadores también forman parte de un área compartida con los ruteadores del núcleo, al tener interfaces conectadas hacia el interior de la red.

- **Protocolo BGP**

El protocolo BGP nos va permitir la comunicación entre dominios por lo que su implementación debe ser únicamente en las fronteras de una Red. Para la conexión de sitios locales con sitios remotos mediante VPNs, este protocolo es muy usual ya que además permite ser trabajado como protocolo de interiores y se utiliza para la comunicación específica entre dispositivos de frontera. Su implementación se refiere

al uso de sistemas autónomos y dado que en esta implementación se utiliza como BGP interior, el sistema autónomo será único y servirá para identificar a la nube MPLS como sistemas bajo una administración común. La Tabla 3.4 muestra en detalle los pasos a seguir a la hora de implementar la comunicación BGP entre dispositivos de frontera que pertenecen a un mismo sistema autónomo (iBGP).

Tabla 3.4 Configuración de Enrutamiento BGP

Comandos	Propósito
Router(config)# **router bgp** <AS number>	Configura el proceso de enrutamiento IBGP con el número de sistema autónomo que será pasado a otros vecinos IBGP.
Router(config-router)# **neighbor** <ip-address | peer-group-name> **remote-as** <AS-number>	Especifica la dirección IP de un vecino con el cual se establecerá en enrutamiento BGP identificado el sistema autónomo al que pertenece.
Router(config-router)# **neighbor** <ip-address | peer-group-name> **update-source** <loopback-interface>	Configura a BGP para que utilice cualquier interface operacional en conexiones TCP.
Router(config-router)# **neighbor** <ip-address | peer-group-name> **activate**	Establece el emparejamiento con un vecino específico.

Fuente: Elaboración Propia

- **Habilitando MPLS**

Una vez configurado los protocolos de encaminamiento se debe habilitar MPLS al igual que en los ruteadores

participantes del núcleo de red, para tener funcionalidades multiprotocolo se añada las etiquetas a los paquetes entrantes al dominio MPLS. Los comandos para la configuración MPLS de los ruteadores mencionados, son mostrados en la Tabla 3.2.

- **Intercambio de etiquetas – LDP**

Para configurar el manejo de etiquetas en los dispositivos de frontera hace referencia al comando detallado anteriormente (Tabla 3.3) en la sección de Configuración de Intercambio de etiquetas en los P – Routers.

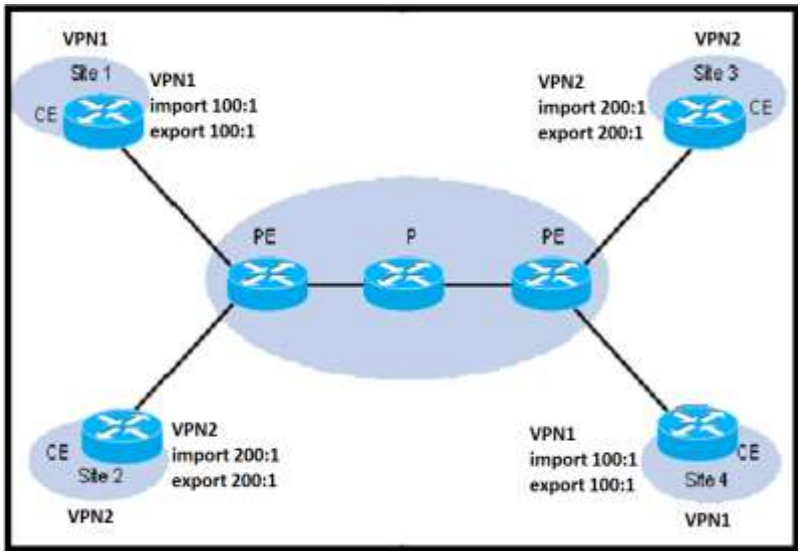
- **Configurando y habilitando VPNs en los PE**

Para habilitar las redes privadas virtuales de capa de red, es necesario saber que, entre los dispositivos de frontera se realiza el intercambio de información de las intranets de los clientes conectados físicamente a aquellos LERs los cuales le harán parecer a los dispositivos CPEs que están unidos a sus sitios remotos como si se tratara de un enlace dedicado.

Al tratar de entender el funcionamiento de las VPNs de capa de red se debe saber que cada una de ellas se asocia con una o más instancias de enrutamiento a la

cual se las denomina VRF (Virtual Routing and Forwarding instances). Una VRF determina la membresía que tiene un cliente conectado a un ruteador de frontera del proveedor de servicio. Cada VRF está compuesta por una tabla de enrutamiento IP, una tabla CEF, un grupo de interface que utilizan dichas tablas, un conjunto de reglas y parámetros del protocolo de enrutamiento que controlan la información que se incluye en la tabla de ruteo, las VRF contienen las rutas disponibles en la VPN que pueden ser accedidas por los sitios de los clientes. Cada sitio puede estar suscrito a varias VPN, pero solamente a un VRF (ver Figura 3.10). Para prevenir que no salga ni ingrese tráfico fuera de la VPN, cada VRF tiene guardada información de envío en las tablas IP y CEF.

Figura 3.10 Redes Privadas Virtuales – VPNs,



Fuente: Elaboración Propia

La distribución de información de la conexión VPN de capa de red se controla mediante el uso de comunidades de ruta objetivo VPN. Las comunidades BGP extendidas se encargan de dicha distribución, mediante lo que se detalla a continuación:

Cuando una nueva ruta VPN entra desde un ruteador CPE, esta ingresa al protocolo BGP y añade sus atributos a la lista de comunidades extendidas de ruta objetivo. Los valores de esta lista se obtienen de la lista de exportación de rutas objetivo relacionadas con la VRF de donde se obtuvo la nueva ruta.

Adicionalmente, cada VRF incluye también una lista de importación de comunidades extendidas de ruta objetivo, la misma que define los atributos que una

comunidad extendida de ruta objetivo debe tener para que la ruta pueda ser importada a la VRF.

Mediante una sesión entre el ruteador de frontera y el ruteador del cliente (PE - CPE), el dispositivo ubicado en el borde del dominio MPLS obtiene el prefijo IPv4 del cliente para luego convertirlo en un nuevo prefijo VPN – Ipv4 al añadirle 8 bytes de Distintivo de Ruta (RD), que como su nombre lo indica, sirve para distinguir la ruta. Este nuevo prefijo sirve para identificar la dirección del cliente sin importar donde se encuentre y si su dirección es global o local, única o común. El RD se obtiene del VRF del ruteador PE en cuestión.

Para las VPNs en MPLS, BGP es el encargado de distribuir la información de capacidad de alcance a los prefijos VPN – IPv4. Cuando la distribución se lleva a cabo dentro del dominio IP – MPLS tenemos BGP interior por medio de sesiones entre dispositivos de frontera (PE – PE).

Para el envío de paquetes en una conexión VPN con MPLS se hace uso de la información de ruteo almacenada en las tablas CEF y VRF. Los dispositivos

de frontera añaden una etiqueta a cada prefijo que se obtiene de los ruteadores del cliente; el prefijo incluye información alcanzable de los demás ruteadores de frontera.

Los paquetes que atraviesan el Backbone MPLS llevan dos etiquetas, la primera tiene la dirección del ruteador de frontera que es el siguiente salto y la segunda que le indica como el ruteador PE alcanzado debe reenviar ese paquete al ruteador CPE. Cuando el ruteador PE recibe el paquete etiquetado, lee la etiqueta, la quita y reenvía el paquete al destino marcado en la segunda etiqueta.

La creación y configuración de VPNs en MPLS es muy sencilla con el uso de BGP y se deben tener en cuenta pasos como: definición de VPNs configuración de iBGP entre dispositivos de frontera, y configuración de enrutamiento hacia cliente en los ruteadores de frontera (Tablas 3.5, 3.6 y 3.7).

Tabla 3.5 Creación y definición de VRF

Definición de VPNs de capa de red	
Comandos	**Propósito**
Router(config)# **ip vrf** <vrf-name>	Define la instancia en enrutamiento virtual con su nombre.
Router(config-vrf)# **rd <route-distinguisher>**	Crea tablas de enrutamiento y envió.
Router(config-vrf)# **route-target import** <route-target-ext-community>	Crea una lista de importación de comunidades extendidas de ruta objetivo para la VRF especificada.
Router(config-vrf)# **route-target export** <route-target-ext-community>	Crea una lista de exportación de comunidades extendidas de ruta objetivo para la VRF especificada.
Router(config-vrf)# **interface** <type> <slot/port>	Ingresa al modo de configuración de interfaz.
Router(config-if)# **ip vrf forwarding** <vrf-name>	Asocia una VRF con una interfaz.

Fuente: Elaboración Propia

Tabla 3.6 Configuración de Multiprotocolo BGP

Configuración de MP – IBGP entre sesiones PE - PE	
Comandos	**Propósito**
Router(config)# **router bgp** <AS number>	Ingresa al proceso de enrutamiento IBGP con el número de sistema autónomo que está configurado.
Router(config-router)# **address-family vpnv4**	Ingresa al modo para configuración de MP – IBGP para VPNv4.
Router(config-router-af)# **neighbor** <ip-address | peer-group-name> **activate**	Establece el emparejamiento con un vecino especificado.
Router(config-router-af)# **neighbor** <ip-address | peer-group-name> **send-community both**	Los vecinos renegocian sus capacidades.

Fuente: Elaboración Propia

Tabla 3.7 Configuración del enrutamiento BGP sobre la VRF del cliente

Configuración de MP – BGP entre sesiones PE - PE	
Comandos	**Propósito**
Router(config)# **address-family ipv4 vrf** <name-vrf>	Configurar por VRF el enrutamiento por BGP.
Router(config)# **neighbor** <ip-address> **remote-as** <AS-number>	Especifica la dirección ip del vecino que se establecerá el enrutamiento BGP.
Router(config)# **neighbor** <ip-address> **activate**	Especifica la dirección IP del router vecino y la activa.
Router(config)# **neighbor** <ip-address> **as-override**	Activa la función de cambio de AS de los router de origen por lo de destino.

Fuente: Elaboración Propia

3.4.5 Configurando los CPE – Routers

La configuración de los dispositivos localizados en las oficinas del cliente es muy sencilla y puede ser vista como un enrutamiento sencillo del trafico IP hacia un destino final, es decir de un punto a otro. Para el cliente la información de etiquetamiento MPLS es transparente ya que los mismos no pertenecen al dominio en el cual se asignan y se conmutan las etiquetas a los paquetes que los envían hacia la red MPLS. La información de enrutamiento de los dispositivos que se conectan a la nube MPLS es enviada de extremo a extremo dentro de la red mediante los protocolos de enrutamiento ya mencionado BGP.

3.4.5.1 Configuración del Router del cliente

Para los sitios del cliente que se van a conectar la sede principal (Matriz) con su sede remota (Sucursal) por medio de una red MPLS que les brinde seguridad al momento de transmitir información es necesario conocer los diferentes dominios que se pueden presentar al momento de entablar las redes de datos. Para el diseño se presentan el dominio IP de los sitios de los clientes y un dominio MPLS por medio del cual se enlazaran los puntos locales con los sitios remotos.

- **Conectividad hacia la red MPLS**

La información desde los cliente puede ser enviada mediante protocolos de enrutamiento dinámico (BGP exterior, OSPF ente áreas, RIP etc.), o mediante el enrutamiento estático, pero en este caso emplearemos el enrutamiento dinámico con el protocolo BGP, los mismos se encargaran de enrutar el tráfico hacia los equipos del núcleo MPLS con un trato específico acorde a la calidad de servicio que se le puede brindar al enlace.

- **Configurando el Enrutamiento**

Dado que se ha decidido enrutar dinámicamente el tráfico de la red de los clientes, el comando de configuración presentado en la Tabla 3.8 ayuda a direccionar los paquetes hacia la red MPLS, para que luego el equipamiento dentro de la misma se encargue de direccionarlo a su destino.

Tabla 3.8 Configuración del protocolo BGP en el CPE hacia la nube MPLS

Comandos
Router(config)# **router bgp** <AS-number>
Router(config)# **network** <ip-address>
Router(config)# **neighbor** <ip-address> **remote-as** <AS-number>
Router(config)# **no synchronization** Router(config)# **no auto-summary**

Fuente: Elaboración Propia

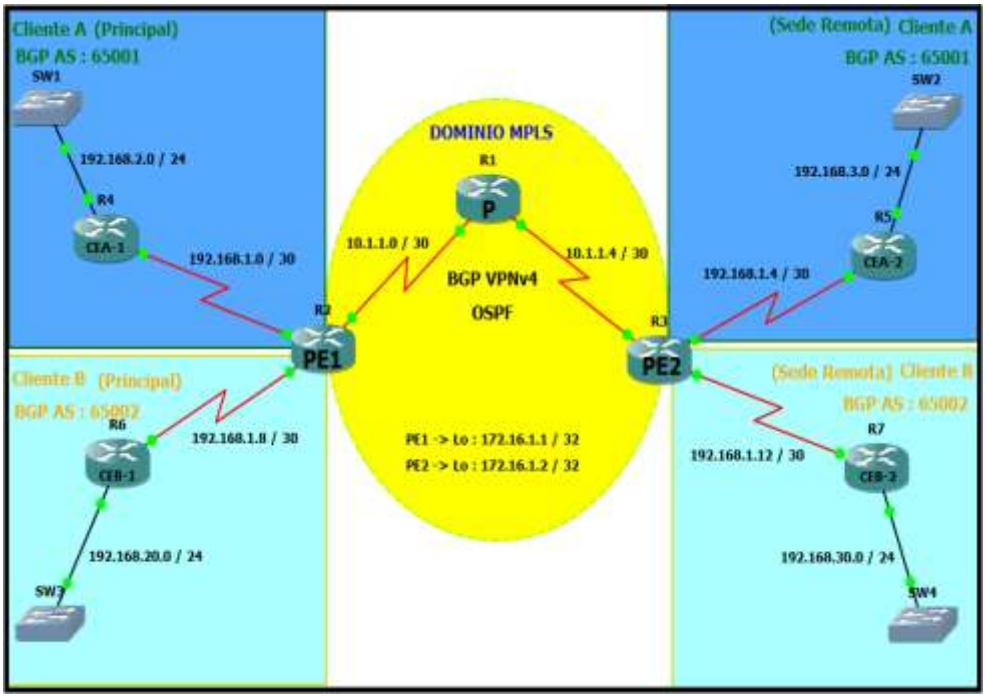
De las implementaciones de los servicios que puede brindar la red MPLS de un proveedor se pueden obtener muchos resultados. El hecho de que el cliente piense que su sede principal y sucursales poseen enlaces dedicados para conectarse entre sí, es uno de los objetivos principales de la implementación de conexiones VPNs entre la matriz y las agencias. Las sucursales de la empresa pueden acceder a los distintos aplicativos que su sede Principal les pueda ofrecer por medio de conexiones VPN en MPLS.

3.5 REVISIÓN Y CONSOLIDACIÓN DE RESULTADOS

3.5.1 Resultado final de la topología.

Como resultado final tenemos la siguiente topología emulada en el programa GNS3 (ver Figura 3.11).

Figura 3.11 Red WAN de la empresa



Fuente: Elaboración Propia

Se emuló un escenario real la cual está compuesta por 2 clientes (A y B) cada uno con una sede remota.

El motivo por el cual se emuló dos clientes, es para poder demostrar que a pesar que las empresas (independientes una de otra) están interconectadas a la misma nube MPLS, no van a compartir la información que pase sobre ellas.

Se llega a la conclusión que cuando la empresa migre su red WAN hacia una red VPN-MPLS, habrán otras empresas ya interconectadas que provisionen del mismo PE, pero cada empresa tendrá la seguridad que los datos que vayan a transferir entre sus sedes no serán interceptadas o serán vistas por otras empresas ajenas a las mismas.

En esta topología a la empresa que he implementado se le denota como cliente A, y el cliente B será otra cualquier empresa.

Cada cliente manejara una VRF diferente para la interconexión entre sus sedes, esto quiere decir que cada cliente manejara su propia tabla de enrutamiento.

3.5.1.1 Revisión del OSPF en la nube MPLS

Recordamos que configuramos OSPF como protocolo de enrutamiento dinámico en la nube MPLS (P).

OSPF es un protocolo de routing interno (IGP) del tipo estado de enlace. Los equipos anuncian toda la información al arrancar el protocolo. Se enviaran entre si paquetes link state cuando se detectan fallos en algún enlace. Entonces, todos los routers actualizan la base de datos topológica, se copian los link state e inundan a los vecinos. Por lo tanto, solo se van

enviando las nuevas actualizaciones de las rutas (y no la tabla completa).

En la siguiente figura (ver Figura 3.12) se hacen uso de los comandos puestos anteriormente para verificar el enrutamiento OSPF y las adyacencias:

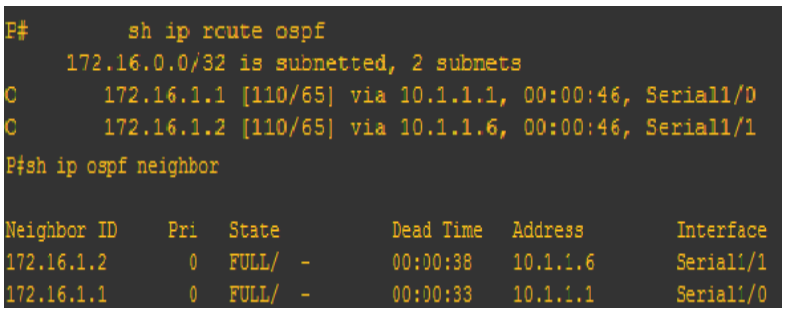
Estos comandos fueron ejecutados en el Router de tipo ‘’P’’.

Show ip route ospf

Show ip ospf neighbors

Los comandos para comprobar las adyacencias OSPF es:

Figura 3.12 Adyacencias OSPF



Fuente: Elaboración Propia

3.5.1.2 Revisión del funcionamiento MPLS

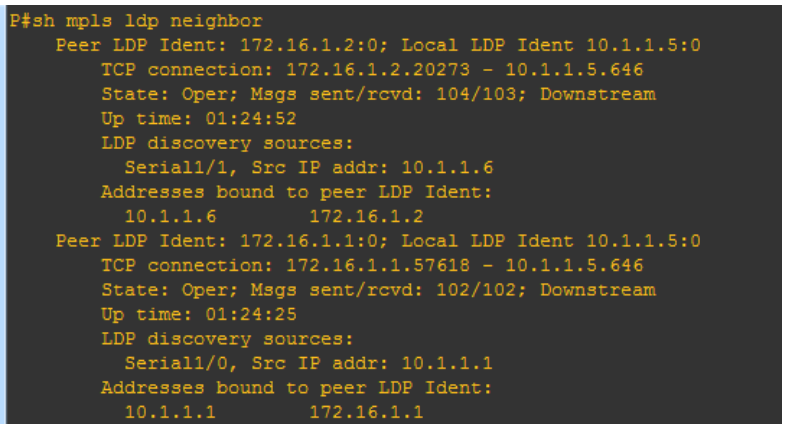
Para el funcionamiento del MPLS, para verificar se usara el siguiente comando.

Show mpls ldp neighbor

Este comando se puede ejecutar en todo el dominio MPLS, tanto en los routers de borde (Router – PE) como los routers núcleo (Router – P).

En la siguiente figura (Figura 3.13) se pueden ver los vecinos que forman el dominio MPLS:

Figura 3.13 Revisión de los vecinos MPLS



Fuente: Elaboración Propia

3.5.1.3 Revisión del BGP en la nube MPLS

El uso del protocolo de enrutamiento BGP es importante para dejar preparado el dominio MPLS para crear servicios de Redes Privadas Virtuales, y este si es el caso ya que configuraremos las RPV para la interconexión entre las sedes.

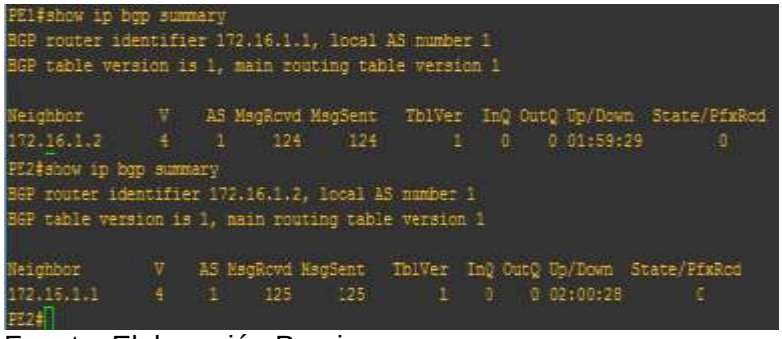
Para la verificación del estado BGP en la nube MPLS, citaremos el siguiente comando:

Show ip bgp summary

Recordemos que el protocolo BGP dentro del dominio MPLS solo se utilizara en los router de borde (PE - Routers).

La siguiente figura (ver Figura 3.14) muestran el correcto funcionamiento del protocolo BGP.

Figura 3.14 Resultado de los vecinos BGP.



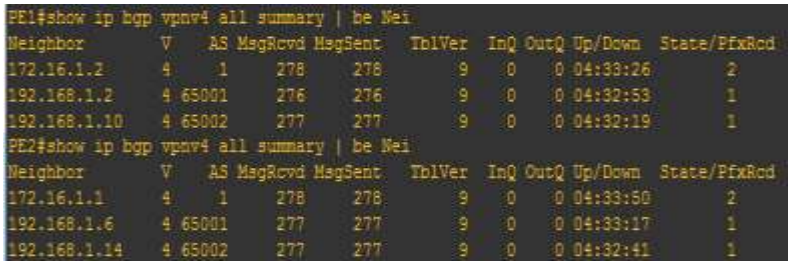
Fuente: Elaboración Propia

3.5.1.4 Revisión de la VPN en la nube MPLS

Para establecer las VPN que se realizan entre los routers de borde se necesita del protocolo de enrutamiento BGP; recordemos que el protocolo BGP en el dominio MPLS se utiliza solamente en los routers de borde (Router – PE).

La siguiente figura (ver Figura 3.15) se puede verificar el establecimiento de la VPN entre los routers de borde.

Figura 3.15 Establecimiento de la VPN en los PE – Routers



Fuente: Elaboración Propia

3.5.1.5 Verificación de las VRFs

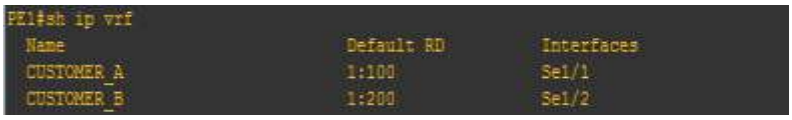
Cada empresa se le asigna una VRF distinta, para este caso a la empresa se le asignara la VRF CUSTOMER_A y para la otra empresa la VRF CUSTOMER_B por cuestiones didácticas.

Para poder verificar en los Router – PE la tabla de enrutamiento para cada VRF se realizara con el siguiente comando:

Show ip route vrf <nombre VRF>

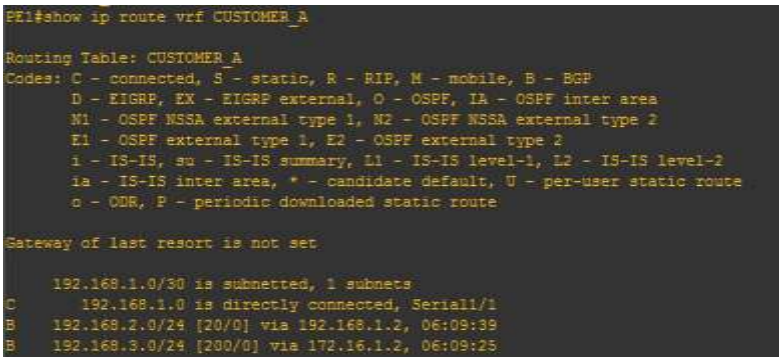
En las siguientes figuras (Figura 3.16, 3.17 y 3.18) se pueden observar las tablas de enrutamiento que tiene cada empresa en los routers de borde.

Figura 3.16 Nombres de las VRF configuradas



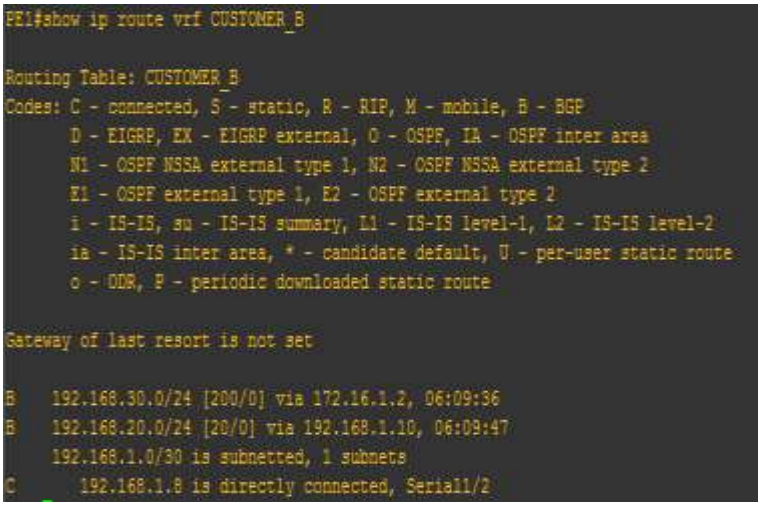
Fuente: Elaboración Propia

Figura 3.17 Tabla de enrutamiento de la empresa A



Fuente: Elaboración Propia

Figura 3.18 Tabla de enrutamiento de la empresa B



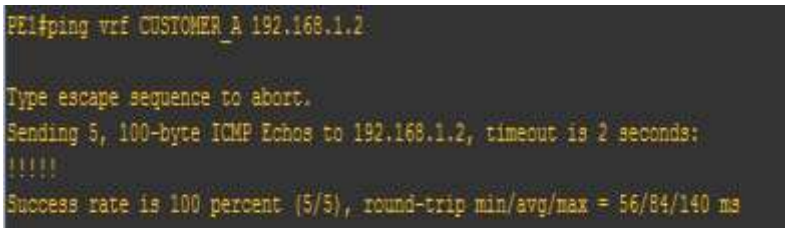
Fuente: Elaboración Propia

3.5.1.6 Verificación de la conectividad entre CPE – PE

En este escenario la conectividad que se va a dar entre CPE y el PE conectado, es mediante la VRF. Si no se pusiera sobre una VRF esto perjudicaría gravemente a las empresas que están conectadas a un mismo router de tipo PE, por lo que la transferencia de datos independiente de cada empresa se podría intercambiar con las de otras y ser riesgoso (ver Figura 3.19 y Figura 3.20).

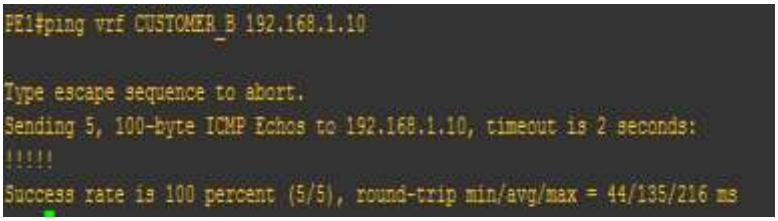
Las siguientes graficas muestran la conectividad VRF que existe entre el PE – CPE de cada empresa.

Figura 3.19 Conectividad mediante VRF entre el PE y la empresa cliente A



Fuente: Elaboración Propia

Figura 3.20 Conectividad mediante VRF entre el PE y la empresa cliente B



Fuente: Elaboración Propia

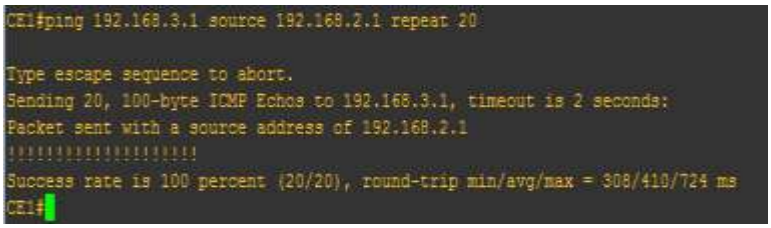
3.5.1.7 Conectividad entre la Sede Principal y la Sede Remota

Finalmente a lo que se quiere llegar en un principio es que se establezca la conectividad entre la sede Principal y la sede Remota de la empresa denotada por cliente A.

Al obtener conectividad entre sus sedes, esto va a tener que pasar por la nube MPLS, y la importante va ser que la nube MPLS por donde se van a transferir los datos va ser transparente para el cliente.

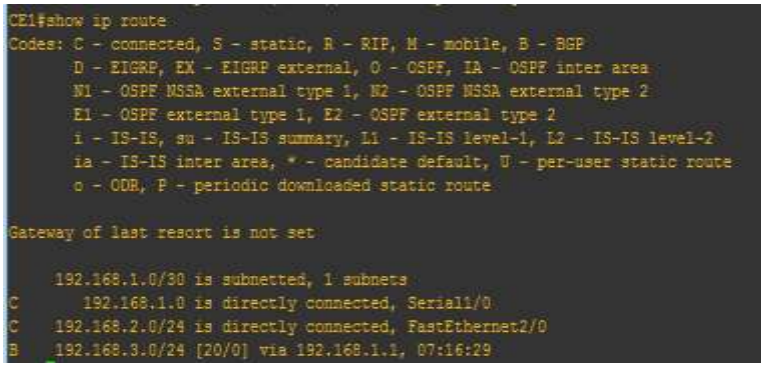
En la siguiente figura (ver Figura 3.21 y Figura 3.22) se puede verificar la conectividad que se da entre la Sede principal y la sede remota de la empresa (cliente A).

Figura 3.21 Pruebas de PING entre la Sede Principal y Remota cliente A



Fuente: Elaboración Propia

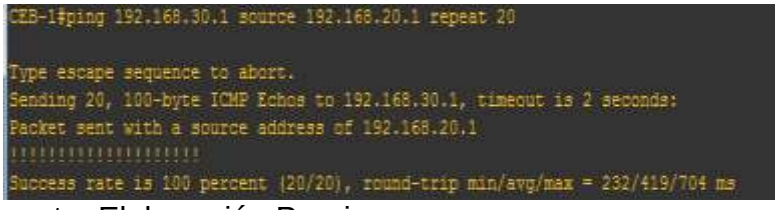
Figura 3.22 Tabla de enrutamiento de la Sede Principal del cliente A



Fuente: Elaboración Propia

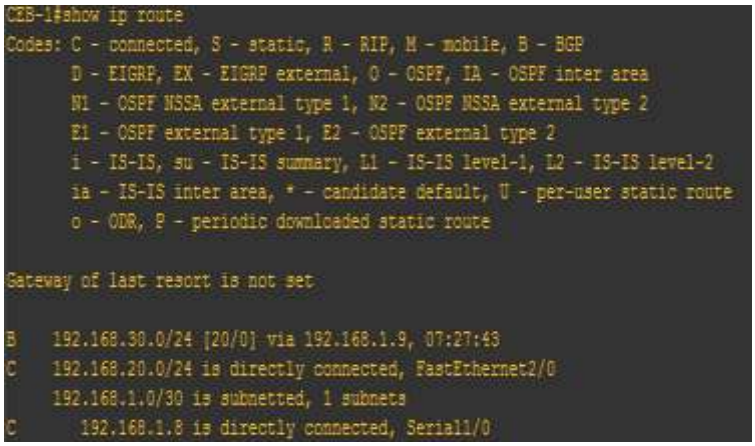
En la siguiente figura (ver Figura 3.23 y Figura 3.24) se puede verificar la conectividad que se da entre la Sede principal y la Sede Remota de la empresa B (cliente B).

Figura 3.23 Pruebas de PING entre la Sede Principal y Remota cliente B



Fuente: Elaboración Propia

Figura 3.24 Tabla de enrutamiento de la Sede Principal del cliente B



Fuente: Elaboración Propia

CAPÍTULO IV

COSTOS Y BENEFICIOS

Después de estudiar varios productos de las Redes Privadas Virtuales existentes en el mercado, se ha determinado que los requerimientos a tomarse en cuenta para la comunicación de la empresa son relativos de acuerdo al número de sucursales con los que cuenta.

Para realizar el análisis costo/beneficio es necesario recopilar datos relevantes durante el desarrollo del proyecto y en base a ello tomar la mejor decisión para determinar si se procede o no con la implementación de la Red Privada Virtual para satisfacer los requerimiento de seguridad en la transferencia de datos de la empresa.

Este estudio evalúa aspectos fundamentales para la migración de la red WAN a una MPLS de la empresa, quien tendrá la facultad de decidir si desea implementar la Red Privada Virtual, a partir de los costos establecidos en este estudio.

Para el análisis de los costos se considera lo siguiente:

4.1 ESCENARIO INICIAL

La empresa realiza cuantiosos gastos cuando se trata de poder recolectar la información de cada sucursal que opera de la empresa. Esta información que se traslada hacia la sede Principal se realiza diariamente, en la cual

transportan: Ventas del día (facturas y boletas), inventarios de los productos vendidos, productos que demandan, pago de los trabajadores mensuales, gastos de alquiler del local y pago de servicios básicos. Toda esta información es transportada por cada sucursal que se encuentran en los distritos de San Martin de Porres, La Victoria y Santiago de Surco hacia la Sede Principal que está ubicada en Miraflores en la Tabla 4.1 y Tabla 4.2.

El transporte de la información se realiza a diario, ya que la empresa necesita saber las ventas (Boletas y Facturas) que se realizaron en el día como también los productos que le faltan para las ventas del día siguiente.

Gastos de la empresa antes de la Migración:

Tabla 4.1 Gastos de la empresa antes de la Migración

Variables por cada Sede	Cantidad	Costo Mensual S/.
Movilidad de la información (ida y vuelta).	50	700.00
Mano de obra (Personal encargado para el transporte)	2 Personas	2500.00
Gasto en llamadas mediante telefonía móvil	1200 min	600.00
Servicio de internet convencional para cada sucursal	1	120.00
Tiempo empleado	1	1300.00
Total		5220.00

Fuente: Elaboración Propia

Tabla 4.2 Gastos de la empresa antes de la Migración total de sedes

Gastos por cada Sede x4 S/.	Mensual S/.	Anual S/.
5220.00 x4	20880.00	250560.00

Fuente: Elaboración Propia

En caso la información que se transporta hacia la sede principal se llegara a perder los costos y aumentarían significativamente, ya que tendría una pérdida aproximada a la producción del día por parte de la sucursal.

4.2 ESCENARIO FUTURO

Se realiza un estudio de factibilidad en el caso de que la empresa realice la migración de las redes WAN de sus sedes hacia una RPV con recursos públicos (VPN-MPLS).

Se tomarán en cuenta las tarifas que proporciona el proveedor de servicios América Móvil (Claro), como también las siguientes consideraciones que afectan los precios en lo que corresponde a los gastos de instalación del servicio para cada sede:

Los gastos de instalación varían de acuerdo a la ubicación de las sedes, estando estas en los distritos de: Miraflores, San Martin de Porres, La Victoria y Santiago de Surco. Se toman en consideración las ubicaciones por lo que estas sedes deben estar a una distancia lo más cercana posible al POP

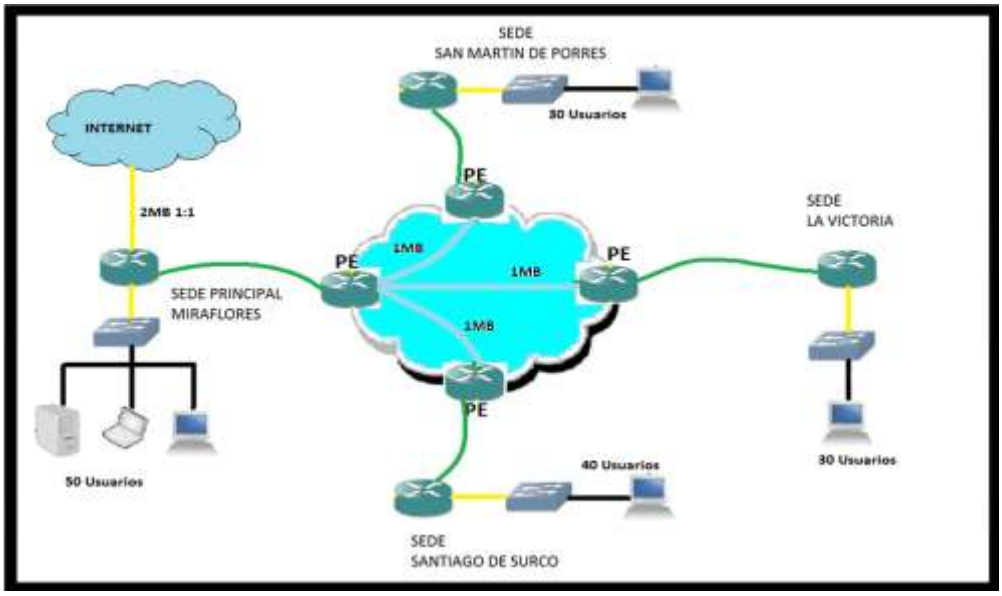
(punto de presencia del proveedor). Esto se debe a que los gastos en el tendido de fibra óptica se incrementarían a mayores distancias.

En este caso como las sedes se encuentran en distritos con sectores industriales, hay troncales del proveedor que pasan muy cerca lo cual implicaría que el tendido de la fibra óptica sea de muy poca distancia, esto ocasionaría una disminución de los gastos favorable para la empresa.

Se toma como referencia la mejor oferta comercial del proveedor, teniendo en cuenta lo que se necesita de ancho de banda para la cantidad usuarios que trabajan para cada sede. En total se necesitaran 3 enlaces de RPV para conectar la Sede Principal con las 3 sucursales de las cuales cada uno tendrá un ancho de banda de 1Mb dedicado y adicionalmente se propondrá un servicio de Internet por fibra óptica de 2Mb con overbooking de 1:1 que estará ubicado en la sede principal (ver Figura 4.1).

Por último se hizo la comparación entre lo que le costaría a la empresa comprar los equipos o alquilarlos para el servicio, se llega a la conclusión en este caso que lo más factible es el alquiler de equipos.

Figura 4.1 Topología final de la empresa



Fuente: Elaboración Propia

Gastos de la empresa después de la Migración:

En el siguiente cuadro Tabla 4.3, solo se colocará los gastos iniciales de instalación, esto solo corresponde a un único pago, los montos varían de acuerdo a la lejanía de la sede al POP (punto de presencia del proveedor).

Tabla 4.3 Costo de Instalación luego de la migración

Servicio	Ancho de Banda	Descripción	Monto (Único Pago) S/.
RPV Sede: Miraflores	1Mb	Instalación: Tendido de fibra óptica, ponchado hacia el Media Converter, conexión del Router Cisco con UPS y un cable de red para conectar Switch del cliente.	3892.00
RPV Sede: San Martin de Porres	1Mb	Instalación: Tendido de fibra óptica, ponchado hacia el Media Converter, conexión del Router Cisco con UPS y un cable de red para conectar Switch del cliente.	2958.00
RPV Sede: La Victoria	1Mb	Instalación: Tendido de fibra óptica, ponchado hacia el Media Converter, conexión del Router Cisco con UPS y un cable de red para conectar Switch del cliente.	3265.00
RPV Sede: Santiago de Surco	1Mb	Instalación: Tendido de fibra óptica, ponchado hacia el Media Converter, conexión del Router Cisco con UPS y un cable de red para conectar Switch del cliente.	2893.00
Internet	2Mb	Instalación: Tendido de fibra óptica, ponchado hacia el Media Converter, conexión del Router Cisco con UPS y un cable de red para conectar Switch del cliente.	3758.00
TOTAL			16766.00

Fuente: Elaboración Propia

En el siguiente cuadro Tabla 4.4 se colocará los gastos mensuales que tendrá la empresa por cada sucursal

Tabla 4.4 Costo Mensual luego de la migración

Servicio	Ancho de Banda	Descripción	Pago Mensual S/.	Total Mensual S/.
RPV Sede: Miraflores	1Mb	Ancho de banda	2574.50	3129.50
		Acceso	345.00	
		Alquiler de equipos	210.00	
RPV Sede: San Martin de Porres	1Mb	Ancho de banda	2574.50	3129.50
		Acceso	345.00	
		Alquiler de equipos	210.00	
RPV Sede: La Victoria	1Mb	Ancho de banda	2574.50	3129.50
		Acceso	345.00	
		Alquiler de equipos	210.00	
RPV Sede: Santiago de Surco	1Mb	Ancho de banda	2574.50	3129.50
		Acceso	345.00	
		Alquiler de equipos	210.00	
Internet Sede: Miraflores	2Mb	Ancho de banda	3125.50	3871.50
		Acceso	451.00	
		Alquiler de equipos	295.00	
TOTAL				16389.50

Fuente: Elaboración Propia

En el siguiente cuadro Tabla 4.5 se muestra el gasto anual luego de la migración.

Tabla 4.5 Costo anual luego de la migración

Gasto por instalación S/.	Gasto mensual S/.	Gasto anual + Instalación S/.
16766.00	16389.50 **x12**	213440.00

Fuente: Elaboración Propia

4.3 BENEFICIO DE LA PROPUESTA

El siguiente recuadro Tabla 4.6 detalla la comparación de los gastos que realizaría en La empresa el primer año donde está incluido los gastos de instalación.

Se llega a la conclusión: A pesar que en el primer año están incluidos los pagos únicos de instalación se logra observar la disminución de los gastos en un año de S/. 213440.00.

Tabla 4.6 Costo de comparación de beneficio al año

Antes de la migración S/.	Después de la migración (1er Año) S/.
250560.00	213440.00

Fuente: Elaboración Propia

En el segundo año se lograría observar el notable ahorro que tendría la empresa al realizar la migración, sin contar los costos de instalación que se dieron en el primer año como se muestra en la Tabla 4.7.

Tabla 4.7 Costo de comparación de beneficio al Segundo año

Antes de la migración S/.	Después de la migración (2do Año) S/.
250560.00	196674.00

Fuente: Elaboración Propia

Según los cuadros comparativos se logra verificar la factibilidad de la migración de la red WAN de la empresa hacia una red VPN-MPLS generándole menores gastos que antes de la migración.

CONCLUSIONES

1. Se logra concluir que al usar una red VPN-MPLS de un proveedor de servicios la empresa tiene menores gastos después de la migración.

2. Luego de un análisis de las Redes Privadas Virtuales se ha podido determinar que la implementación de estas es una de las mejores opciones de comunicación, ya que resultan muy beneficiosas tanto en aspectos económicos como en la fiabilidad de la transmisión de la información.

3. Se propone una solución para la empresa para que pueda migrar hacia una red MPLS de un proveedor de servicios para poder entablar enlaces de datos, voz, video, etc. entre sus sucursales.

4. Con la implementación de la VPN se logra el objetivo principal de este estudio, el mismo que es permitir que los datos de la empresa sean transmitidos a través de la red pública desde cada una de las sucursales, proporcionando mayor rapidez, seguridad y confiabilidad.

RECOMENDACIONES

1. Se recomienda a la empresa adquirir de una red VPN-MPLS para su red WAN ya que estarían ahorrando grandes sumas de dinero que beneficiarían a la empresa.

2. Es recomendable que el tráfico que se vaya a enviar en un futuro por los usuarios de la empresa sea gestionado en el Backbone distribuyendo el mismo en clases de diferenciado servicio (MPLS soporta Clases de Servicio) las mismas por sus niveles de prioridad logrando que tengan ventajas las aplicaciones más críticas.

3. Para comprender una tecnología de nueva generación, es recomendable conocer y tener en claro las funciones de los elementos que son participes y que definen la topología de una red teniendo en cuenta además la ubicación que deben tener los mismos.

4. Se recomienda en un futuro cuando el número de trabajadores aumente en la empresa evaluar la posibilidad de aumentar el ancho de banda de los enlaces, ya que el consumo de recursos del enlace del propio personal puede aumentar y como consecuencia puede afectar el rendimiento del enlace.

5. Se recomienda a la empresa que el futuro administrador de red de la VPN, deber tener un plan de contingencia, que permita dar una breve solución a los diversos problemas que se puedan presentar en esta, en el caso de producirse desastres físicos o eléctricos.

BIBLIOGRAFÍA

Libros consultados:

1. Hugo, Z. (2002). Implementación de Redes MPLS – VPN Casos de estudio, de http://www.cudi.edu.mx/primavera2002/presentaciones/MPLSVPN.pdfBrown.
2. STEVE, B. (2001). IMPLEMENTACION DE REDES PRIVADAS VIRTUALES (RPV). MEXICO: MCGRAW-HILL / INTERAMERICANA DE MEXICO.
3. TOD, LAMMLE. (2005) CCNA CISCO CERTIFIED NETWORK ASSOCIATE, Estados Unidos: SYBEX INC.
4. Ernesto, A. (2010). GUIA DE ESTUDIO PARA LA CERTIFICACION CCNP. RA-MA.
5. Juan, Z. (2013). Yo sé networking - BGP, de http://networksjuan.blogspot.pe/2013/01/yo-se-networking-bgp.html.
6. GNS3. (2013, Diciembre 2). Retrieved from http://www.gns3.net.

Enlaces Webs:

7. http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a0080093f23.shtml
8. https://learningnetwork.cisco.com/thread/25187
9. http://www.slideshare.net/thiland/BGPPub
10. http://www.ietf.org/rfc/rfc4364.txt
11. http://www.ramonmillan.com/tutoriales/mpls.php
12. https://prezi.com/acr_j2s2ofmt/mpls-multi-protocol-label-switching/

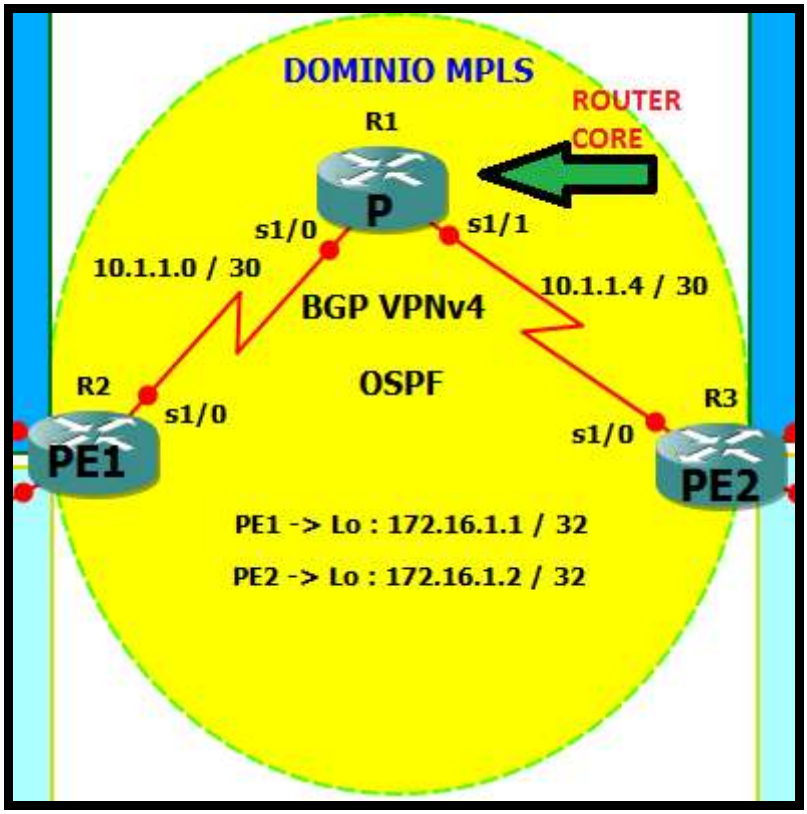
ANEXOS

CONFIGURACIONES ESPECÍFICAS POR EL TIPO DE ROUTER

A continuación se citaran las configuraciones empleadas en la simulación del GNS3 para el caso de implementación de una VPN usando una red pública de un proveedor de servicios.

Anexo 01 Configuración del router CORE

En este tipo de router se configurará el multiprotocolo MPLS, y solamente el protocolo de enrutamiento dinámico OSPF, para la distribución de las etiquetas.



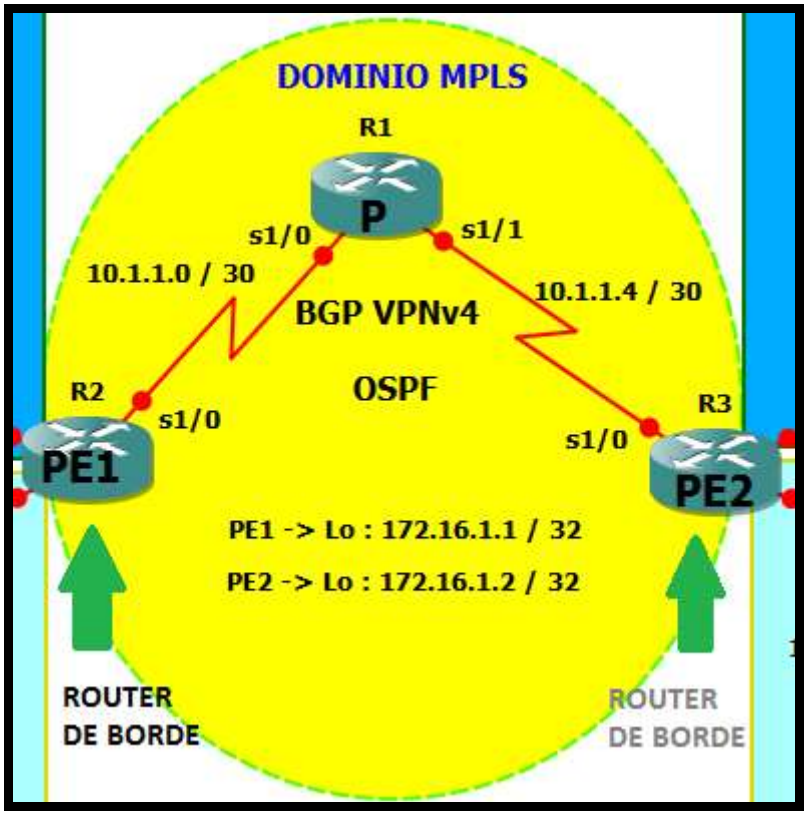
P#show run
Building configuration...
Current configuration : 1672 bytes
!
version 12.4

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip subnet-zero
ip cef
!
no ip domain lookup
ip domain name lab.local
!
!
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Serial1/0
 ip address 10.1.1.2 255.255.255.252
 mpls ip
!
interface Serial1/1
 ip address 10.1.1.5 255.255.255.252
 mpls ip
!
!
router ospf 100
 log-adjacency-changes
 network 10.1.1.0 0.0.0.7 area 0
!
ip classless
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
!
control-plane
```

```
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
P#
```

Anexo 02 Configuración del router de BORDE

En este tipo de router se configurará el multiprotocolo MPLS, y los protocolos de enrutamiento dinámico OSPF para la distribución de etiquetas, y BGP para el establecimiento del MP-BGP para las VPN.



PE1#sh run
Building configuration...

Current configuration : 2717 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!

```
resource policy
!
ip subnet-zero
ip cef
!
!
ip vrf CUSTOMER_A
 description cliente A
 rd 1:100
 route-target export 1:100
 route-target import 1:100
!
ip vrf CUSTOMER_B
 description cliente B
 rd 1:200
 route-target export 1:200
 route-target import 1:200
!
no ip domain lookup
ip domain name lab.local
!
!
!
interface Loopback0
 ip address 172.16.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Serial1/0
 ip address 10.1.1.1 255.255.255.252
 mpls ip
!
interface Serial1/1
 ip vrf forwarding CUSTOMER_A
 ip address 192.168.1.1 255.255.255.252
!
interface Serial1/2
 ip vrf forwarding CUSTOMER_B
 ip address 192.168.1.9 255.255.255.252
!
!
!
router ospf 100
 log-adjacency-changes
 network 10.1.1.1 0.0.0.0 area 0
 network 172.16.1.1 0.0.0.0 area 0
!
```

```
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.16.1.2 remote-as 1
 no auto-summary
 !
 address-family vpnv4
 neighbor 172.16.1.2 activate
 neighbor 172.16.1.2 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf CUSTOMER_B
 neighbor 192.168.1.10 remote-as 65002
 neighbor 192.168.1.10 activate
 neighbor 192.168.1.10 as-override
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family ipv4 vrf CUSTOMER_A
 neighbor 192.168.1.2 remote-as 65001
 neighbor 192.168.1.2 activate
 neighbor 192.168.1.2 as-override
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
no ip http server
no ip http secure-server
!
!
!
logging alarm informational
!
!
mpls ldp router-id Loopback0
!
control-plane
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
```

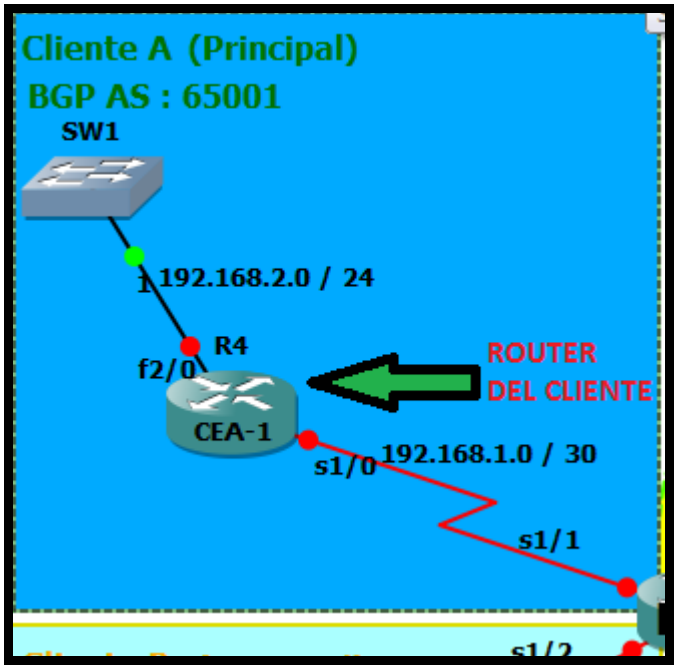
```
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end

PE2#sh run
Building configuration...

Current configuration : 2763 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip subnet-zero
ip cef
!
!
!
!
ip vrf CUSTOMER_A
 description cliente A
 rd 1:100
 route-target export 1:100
 route-target import 1:100
!
ip vrf CUSTOMER_B
 description cliente B
 rd 1:200
 route-target export 1:200
 route-target import 1:200
!
no ip domain lookup
```

```
ip domain name lab.local
!
!
!
!
!
interface Loopback0
 ip address 172.16.1.2 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Serial1/0
 ip address 10.1.1.6 255.255.255.252
 mpls ip
!
interface Serial1/1
 ip vrf forwarding CUSTOMER_A
 ip address 192.168.1.5 255.255.255.252
!
interface Serial1/2
 ip vrf forwarding CUSTOMER_B
 ip address 192.168.1.13 255.255.255.252
!
router ospf 100
 log-adjacency-changes
 network 10.1.1.6 0.0.0.0 area 0
 network 172.16.1.2 0.0.0.0 area 0
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 172.16.1.1 remote-as 1
 neighbor 172.16.1.1 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 172.16.1.1 activate
 neighbor 172.16.1.1 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf CUSTOMER_B
 neighbor 192.168.1.14 remote-as 65002
 neighbor 192.168.1.14 activate
 neighbor 192.168.1.14 as-override
 no auto-summary
 no synchronization
 exit-address-family
```

```
 !
 address-family ipv4 vrf CUSTOMER_A
 neighbor 192.168.1.6 remote-as 65001
 neighbor 192.168.1.6 activate
 neighbor 192.168.1.6 as-override
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
no ip http server
no ip http secure-server
!
!
logging alarm informational
!
!
mpls ldp router-id Loopback0
!
control-plane
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

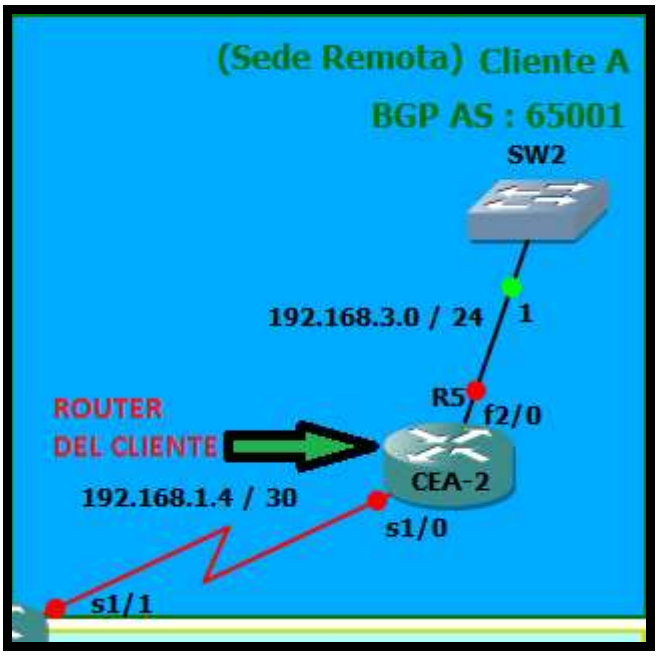
Anexo 03 Configuración del router de CLIENTE

En este tipo de router únicamente se configurará el protocolo BGP para la conectividad entre las sedes del cliente, y la transmisión de datos.



CEA-1#sh run
Building configuration...
Current configuration : 1879 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip subnet-zero
ip cef
!
!
!
!
no ip domain lookup

```
ip domain name lab.local
!
!
!
interface Serial1/0
 ip address 192.168.1.2 255.255.255.252
!
interface FastEthernet2/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
!
router bgp 65001
 no synchronization
 bgp log-neighbor-changes
 network 192.168.2.0
 neighbor 192.168.1.1 remote-as 1
 no auto-summary
!
ip classless
no ip http server
no ip http secure-server
!
!
logging alarm informational
!
!
control-plane
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```



CEA-2#sh run
Building configuration...

Current configuration : 1879 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name lab.local
!
!
!
!

```
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Serial1/0
 ip address 192.168.1.6 255.255.255.252
!
!
interface FastEthernet2/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router bgp 65001
 no synchronization
 bgp log-neighbor-changes
 network 192.168.3.0
 neighbor 192.168.1.5 remote-as 1
 no auto-summary
!
ip classless
no ip http server
no ip http secure-server
!
!
logging alarm informational
!
!
!
control-plane
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
```

line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login
!
!
End