UNIVERSIDAD NACIONAL AUTONOMA DE NICARAGUA

RECINTO RUBEN DARIO

DEPARTAMENTO DE TECNOLOGIA

CARRERA DE INGENIERIA ELECTRONICA

SEMINARIO DE GRADUACIÓN

TEMA

Diseño de una red de transporte de datos implementando MPLS, utilizando el simulador GNS 3 para la interconexión de sitios remotos con su sitio central a través de redes privadas virtuales (VPN).

INTEGRANTES: JUAN RAFAEL RUIZ ESPINOZA

JENNIFER LUCIA CENTENO MORALES

TUTOR: MSC. ALVARO SEGOVIA

ASESOR TECNOLÓGICO: ING. JAIRO GONZALEZ MORENO

05 de Febrero 2013.

DEDICATORIA

Este fruto de la vida universitaria, se lo ofrecemos a Dios que de no ser por él, no sería posible, también sin el apoyo de cada uno de nuestros maestros que nos fueron motivando con esos granitos de conocimientos tan valiosos, tan cruciales para alimentarnos las mentes adecuadamente para llegar a este punto cumbre y poder finalizar los estudios superiores con éxito.

A mi mamá Patricia, a mi abuelita a mi hermano, a mis tíos en especial a mi tío Leonardo y a mi tío Henry que me han apoyado económicamente y emocionalmente durante toda esta larga trayectoria.

Jennifer Centeno.

A Dios por darme la vida, el conocimiento y perseverancia para alcanzar la realización de este trabajo final.

A mis padres Juan Ruiz Aguirre y Otilia de la Cruz Espinoza por darme todo su apoyo y haberme sabido comprender de distintas formas en el transcurso del proceso de elaboración del presente trabajo de graduación.

Juan Rafael Ruiz

AGRADECIMIENTO

Le agradecemos a Dios, de igual forma estamos en gratitud con nuestros padres y amigos porque cuando estuvimos desmotivados por pasar alguna adversidad en nuestras vidas ellos nos supieron comprender y aconsejar dándonos nuevamente ánimos de seguir adelante hasta llegar así a esta nueva etapa final.

De manera especial a nuestro asesor tecnológico Ingeniero Jairo González Moreno y al tutor Álvaro Segovia quienes con mucha paciencia nos han tomado de su mano para enseñarnos como desarrollar este trabajo y llegar a su culminación con su valioso aporte y colaboración.

A todas aquellas personas que de una u otra forma han mantenido su esperanza en nosotros y han entendido el esfuerzo realizado extendiéndonos su mano amiga.

VALORACION DEL DOCENTE

Resumen

El trabajo lo realizamos sobre el Sistema Operativo Ubunto con una simulación aplicada en el programa GNS3 (Simulador grafico de redes) elegido por sus propiedades gráficas y capacidad para soportar el IOS (Internetwork Operating System) real de los router, gracias a las bases que tiene en Dynamips, PEMU (incluyendo el encapsulador) y en parte en Dynagen. GNS 3 también utiliza la tecnología SVG para proveer símbolos de alta calidad para la realización de los mágicos diseños de topologías de red. La tecnología MPLS se basa en el análisis del envío de paquetes de una red, usando conmutación de etiquetas, lo cual es la base principal de este protocolo, el manejo que MPLS da a las redes privadas virtuales (VPNs) para la interconexión de sitios remotos con sus sitios centrales al adoptar una VPN MPLS será capaz de reducir complejidad en la administración de la red, aminorar los costos, mejorando el desempeño de la red y obteniendo conectividad universal. La red privada virtual (VPN) es una tecnología de red que permite la extención de una red privada sobre una red de uso pública como lo es el internet. Las VPN basadas en MPLS superan la mayor parte de los inconvenientes de las otras tecnologías de VPN. MPLS opera entre la capa de enlace de datos (capa 2) y la capa de red (capa 3) del modelo OSI, juntando ambas capas y haciendo uso de la velocidad del envío (forwarding) y del control del enrutador (routing), de esta forma logramos la creación de nuestra topología con redes flexibles y escalables, es decir que gracias a este conjunto de herramientas y sus características logramos con éxito nuestra meta.

INDICE PAG

INTRODUCCIÓN

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

Esto ha provocado la creación de nuevas aplicaciones y servicios así como el aumento en usuarios. Una VPN MPLS (redes privadas virtuales basadas en multiprotocolo de conmutación de etiquetas) es una arquitectura que provee envío de datos seguros a través de una red compartida que conecta sitios geográficamente distribuidos.

Las redes privadas virtuales MPLS o MPLS VPN es una de las aplicaciones e implementaciones más populares de la tecnología MPLS. En la actualidad proveedores de servicios han optado por la migración de sus tradicionales redes Frame Relay y ATM (modo de transferencia asíncrono) a redes MPLS VPN. La implementación y uso de estas redes puede proporcionar a los proveedores de servicios escalabilidad y facilitar a la vez el funcionamiento y administración de la red.

Para la elaboración de este trabajo contaremos con la ayuda de un simulador que es el GNS (Jeremy, GNS3, 2012) Graphical Network Simulator, este permitirá diseñar fácilmente topologías de red y luego ejecutar simulaciones en él. Soporta el IOS de routers, ATM (modo de transferencia asíncrono), Frame Relay /switchs Ethernet (redes de área local) y PIX (Private Internet Exchange).firewalls(autentificación), y así podemos extender nuestra propia red privada conectándola a la topología virtual, demostrando su correcto funcionamiento en la red VPN basada en MPLS (Rosen, 2001), observaremos a traves del diseño de la topología como llega el paquete IP al usuario destino con una dirección IP que pertenezca a la misma red del proveedor de servicio.

JUSTIFICACIÓN

El reto en la actualidad es el envío de paquetes IP, las empresas y los proveedores de servicios buscan la necesidad de crear redes seguras para enviar y recibir datos (voz, video e imagen).

Para resolver esta necesidad la tecnología VPN MPLS es una buena opción, una conexión MPLS VPN permite a un proveedor de servicios crear algo similar a una conexión de línea dedicada entre dos puntos a través de Internet, sin necesidad de adquirir una conexión fija. Utilizando redes VPN, el tráfico es dirigido rápidamente a lo largo de la ruta de A a B, de manera que pueden crearse intranets y extranets a través de infraestructura privada o compartida. Se obtiene mayor flexibilidad al tener sólo una conexión a la red del operador. Sólo los routers situados en el borde de la red del proveedor de servicios necesitan "tener conocimiento de VPN", ya que aquellos que se encuentran dentro del núcleo, sólo necesitan transmitir el tráfico de red, de manera que sus tablas de encaminamiento no resultan imposibles de manejar.

La tecnología MPLS de Cisco Systems, a través del software Cisco IOS, hace a las redes VPN más fáciles de desplegar gracias a la utilización de una plataforma que combina la inteligencia de encaminamiento con el rendimiento de la conmutación.

Estas redes MPLS VPN ofrecen mayor escalabilidad para atender a las necesidades de cientos de miles de usuarios, y son lo bastante flexibles para métodos o esquemas de tráfico del tipo de cualquiera-a-cualquiera, para aceptar rápidamente nuevas instalaciones. Además, ofrecen un rendimiento predecible y fiable a través de diferentes clases de servicio, permiten a los usuarios conectarse a través de diferentes medios y cumplen con los requerimientos de transporte y ancho de banda de nuevas aplicaciones. Cabe destacar que la tecnología MPLS de Cisco posibilita a los proveedores de servicios optimizar el ancho de banda de

red, aplicando selectivamente clases de servicio basadas en etiquetas o “labels” MPLS.

Las redes MPLS VPN escalan fácilmente al aumentar la cantidad de rutas y clientes, y ofrecen el mismo nivel de privacidad que las tecnologías de conmutación. Además, los clientes pueden utilizar direcciones IP privadas sin necesidad de conversión y puede alcanzarse la máxima privacidad y seguridad sin necesidad de túneles ni encriptación. Además no se corre el riesgo de infiltraciones o extraer algún dato.

Al ser un servicio Network-based (red básica), la implementación de la VPN no requiere un hardware específico ni costoso para ser instalado en las oficinas del cliente. De este modo, empresas que al día de hoy mantienen distintos y costosos servicios para soportar sus necesidades de voz, datos y video; pueden unificar estos requerimientos concluyendo en un ahorro significativo y manteniendo relación con un único proveedor de servicios.

OBJETIVOS

OBJETIVO GENERAL

Diseñar una red MPLS utilizando la simulación para la interconexión de clientes (sitios remotos con sus centrales) a través de VPN.

OBJETIVOS ESPECÍFICOS

- Definir el protocolo de enrutamiento para la aplicación de red MPLS.
- Establecer la topología lógica para la red de transporte MPLS.
- Implementación de redes privadas virtuales, definidas en la tecnología MPLS.
- Verificar el funcionamiento de la red MPLS utilizando los comandos adecuados. para su interpretación.

4. DESARROLLO

Antes de empezar ejecutamos el simulador GNS3 en Ubuntu (sistema operativo), este tipo de simulador hace uso intensivo de memoria RAM y CPU (unidad central de proceso) en orden de lograr la emulación, éste ejecuta una imagen de IOS (Sistema Operativo de Interconexión de Redes.) que requiere 256 MB de RAM en un router real, y dedica 256 MB de RAM a la instancia de su router virtual, este utilizará 256 MB de memoria para funcionar. Luego de lo anterior vamos a trabajar solamente con 12 routers por la capacidad que tiene nuestro CPU que es de 2.4 GB y 4GB de RAM.

Al diseñar una red de transporte de datos implementando MPLS en redes privadas virtuales (VPN) utilizando el simulador GNs3, nos decidimos por una topología que interconecte 2 sitios remotos Ces (cliente A2, cliente B2) con sus sitios centrales (cliente A1,cliente B1), refiriéndonos a remotos: que significa establecer una configuración de modo que un router configurado debidamente sea capaz de comunicarse directamente con un servidor en internet por eso se llama remoto "*Que se encuentra apartado o distante*" (Wiktionary, 2012), y así de esta forma poder trabajar al mismo tiempo con los archivos en el sitio local, es decir la copia que hay en el ordenador, y en el sitio remoto, colgados en el servidor, en Internet. Una red remota "*es una red que no está directamente conectada al router*". En otras palabras, una red remota es con la que sólo se puede llegar mediante el envío del paquete a otro router; pero será una red en la que no todos se podrán comunicar entre si, ya que cada proveedor de servicio tendrá configurado únicamente en su router las VRF de los clientes (cliente A1 con cliente A2) y (cliente B1 con cliente B2) ver figura 1:

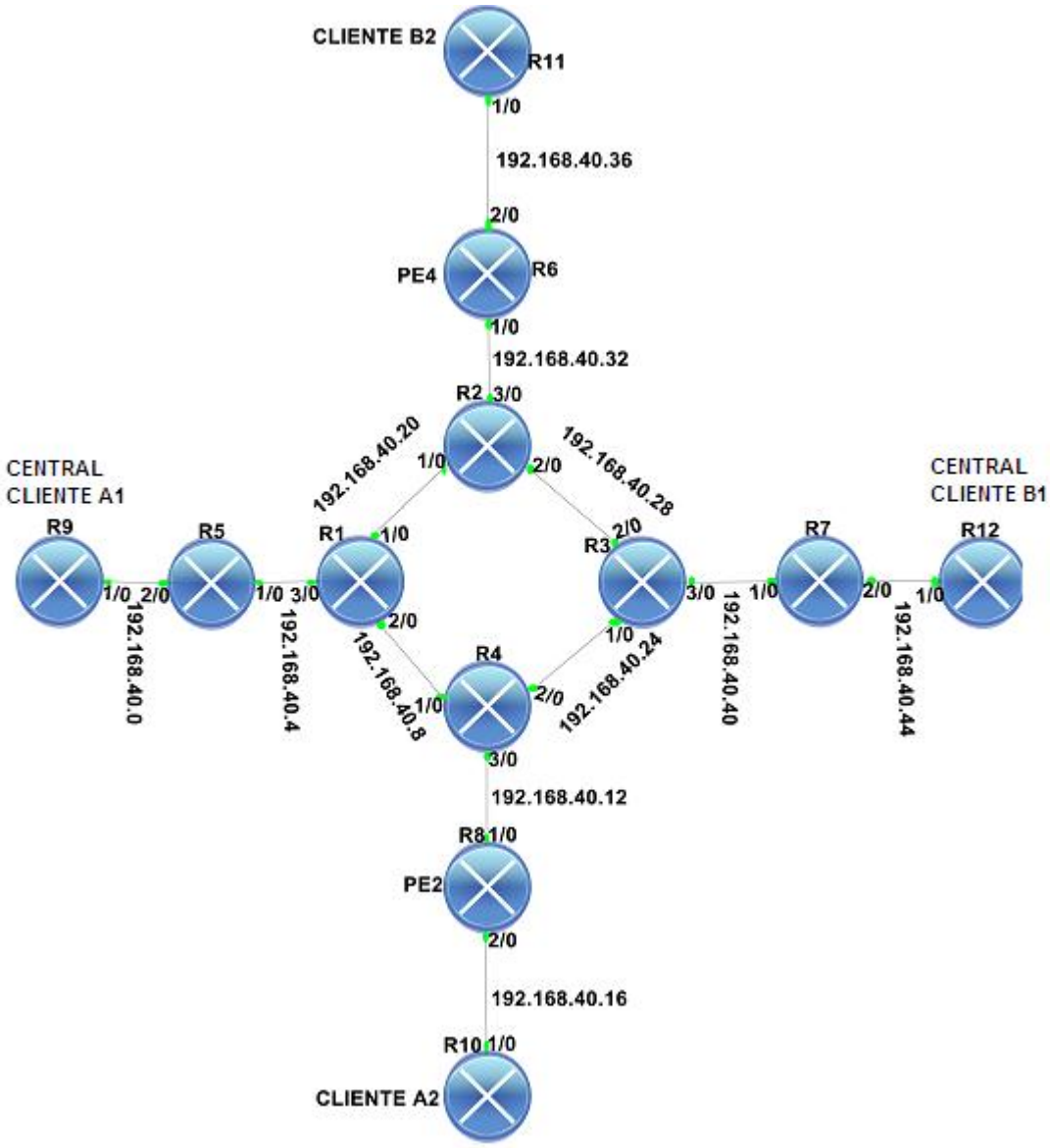

Fig. 1 Topología de interconexión de sitios remotos con su sitio central

Tabla 1. Dirección IP para el CLIENTE A

CLIENTE A1	PE1		P1			P2			PE2		CLIENTE A2
Int.G 1/0	Int.G 1/0	Int.G 2/0	Int. G1/0	Int G 2/0	Int.G 3/0	Int.G 1/0	Int.G 2/0	Int G 3/0	Int.G 1/0	Int. G 2/0	Int.G 1/0
192.168.40.1/30	192.168.40.4/30	192.168.40.2/30	192.168.40.21/30	192.168.40.9/30	192.168.40.6/30	192.168.40.10/30	192.168.40.25/30	192.168.40.13/30	192.168.40.14/30	192.168.40.17/30	192.168.40.18/30

Tabla 2. Dirección IP para el CLIENTE B

CLIENTE B1	PE3		P3			P4			PE4		CLIENTE B2
Int.G 1/0	Int.G 1/0	Int.G 2/0	Int. G1/0	Int G 2/0	Int.G 3/0	Int.G 1/0	Int.G 2/0	Int G 3/0	Int.G 1/0	Int. G 2/0	Int.G 1/0
192.168.40.46/30	192.168.40.42/30	192.168.40.45/30	192.168.40.26/30	192.168.40.30/30	192.168.40.41/30	192.168.40.22/30	192.168.40.29/30	192.168.40.33/30	192.168.40.34/30	192.168.40.37/30	192.168.40.38/30

En cuanto a las conexiones para nuestra topología elegimos Gigabit Ethernet ya que es una tecnología escalable, permite implementación sobre redes operativas existentes, conservando el método de acceso al medio CSMDA/CD (acceso multiple con deteccion de portadora y deteccion de colisiones), y dependiendo de los requerimientos de la red puede operar en modo Full Dúplex(comunicación bidireccional, enviando y recibiendo mensajes de forma simultánea) o Half Dúplex (cada extremo de la conexión transmite uno después del otro).

Gigabit Ethernet tiene ventajas como son: bajos costos en su implementación y altas velocidades de transmisión.

Esta ventaja que presenta Gigabit Ethernet es muy aprovechadas por las empresas portadoras, ya que es una inversión relativamente baja, sencilla y eficaz. Es una tecnología con la que se puede conseguir grandes velocidades en la transmisión de datos, sin tener que realizar mayores cambios en la infraestructura de la redes.

Los routers que utilizaremos para este diseño son los de Cisco 7200 ver figura 2 ya que aportan una relación de rendimiento excepcional en una potente plataforma Cisco. “Los routers Cisco 7200 son los routers de procesador único más rápidos de Cisco” (Cisco 7200 , 2007) , ideales para empresas y proveedores de servicios que implementan MPLS, agregación de ancho de banda, periféricos WAN, seguridad IP, VPN e integración vídeo/voz/datos. La serie 7200 integra diseño modular, opciones de conectividad y funciones de gestión. Entre las características mas importantes destacan:

- Hasta 16.000 sesiones PPP por chasis
- Escalable a 5.000 túneles por chasis
- Punto de interfaz red a red para señalar interworking (interfuncionamiento), media interworking, traducciones de direcciones y de puertos (privacidad y ocultación de topología), facturación y normalización CDR y gestión de ancho de banda (marcas de calidad de servicio con TOS)
- Chasis VXR con TDM activado y adaptadores de puertos de voz
- 3RU con una gama de interfaces modulares (de DS0 a OC-3)
- Compatible con Fast Ethernet, Gigabit Ethernet, Paquete sobre SONET, etc.

Figura 2. Router Cisco 7200

Para el diseño de una red vpn basada en MPLS, se tendrán que correr únicamente protocolos de enrutamiento OSPF o IS-IS ya que son los únicos que soportan MPLS (tráfico de ingeniería).

En este diseño desde el punto de vista del cliente (cliente A o cliente B), ven a sus routers internos para comunicarse con sus clientes routers de borde(CES) de un sitio a otro a través de una VPN gestionados por el proveedor de servicios (ver Figura 3), del Cliente de la red. Este punto de vista simple de la red del cliente es la ventaja de VPN, el cliente experimenta la comunicación directa a sus sitios como si tuvieran su propia red privada, a pesar de que su tráfico está atravesando una infraestructura de red pública y que están compartiendo la infraestructura con otras empresas.

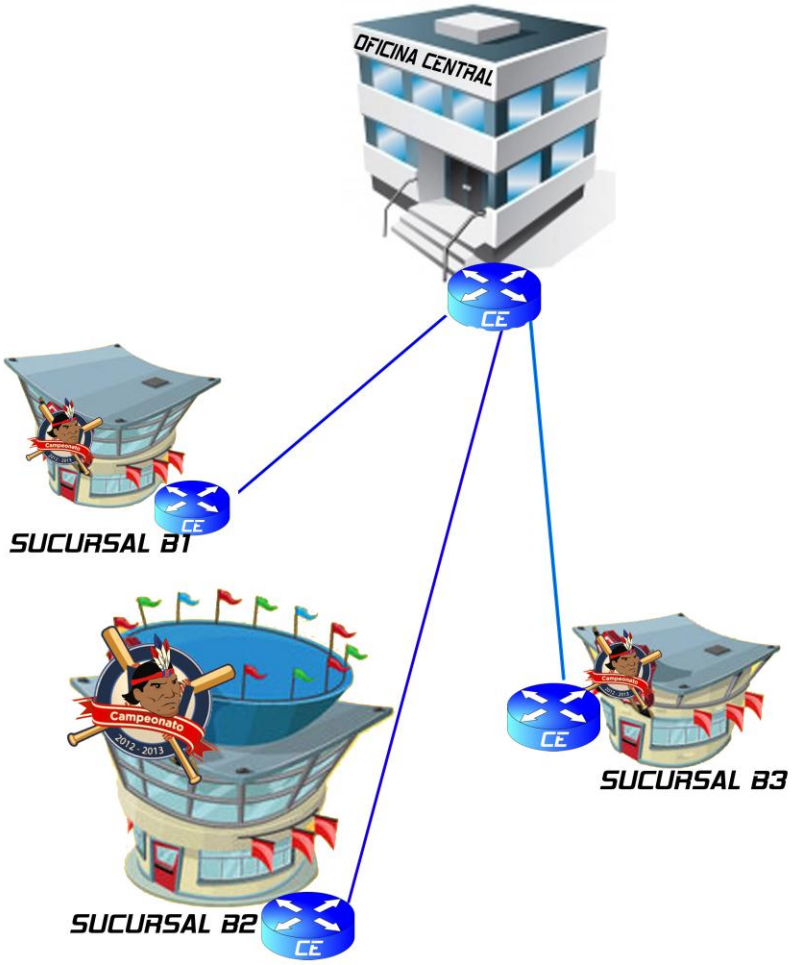

Figura 3. Punto de vista del cliente de la red (CE)

El punto de vista del proveedor de servicios de la red es naturalmente muy diferente, como se muestra en la Figura 4. Esta ilustración muestra dos clientes diferente, donde cada cliente tiene un único VPN (VPN1 para el cliente A y VPN2 para el cliente B), que contiene la LIB (base de información de etiquetas) y FLIB (base de información de reenvío de etiquetas)

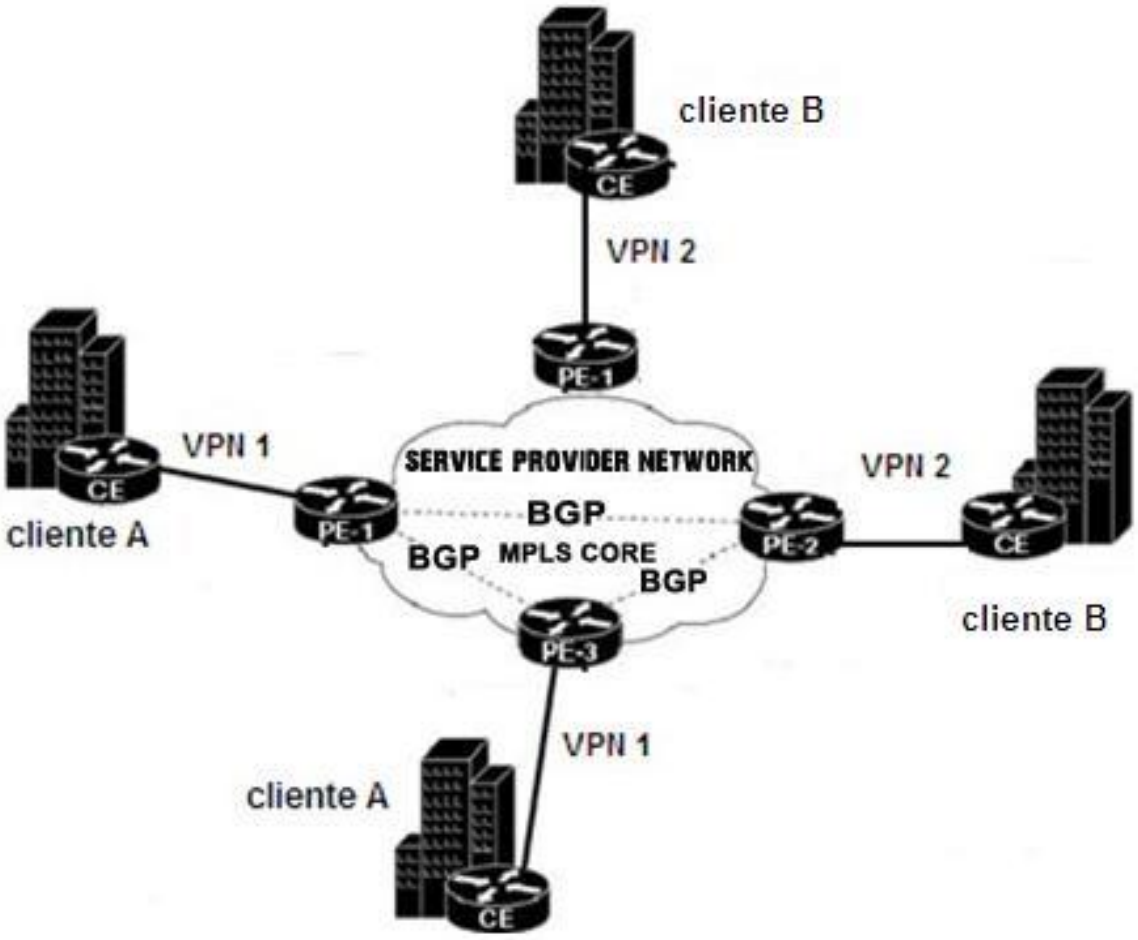

Figura 4. Punto de vista del proveedor de servicio (PE) de la red

Comparativa X25, Frame relay, ATM Y MPLS

	X.25	Frame-relay	ATM	MPLS
Establecimiento de la Conexión	En el nivel de red	No	Desde la capa ATM	En el nivel de red
Control de flujo en cada salto y corrección de errores	En el nivel de enlace	No(debe implementarlo un protocolo de nivel superior)	No, (opera en modo orientado a conexión).	SI
Control de flujo extremo a extremo	En el nivel de red	No	Si garantizadas y fiables	Si
Velocidad	Constante (hasta 64 Kbps)	Control de velocidad variable (ráfagas) desde 56Kbps hasta 50Mbps	Velocidad alcanzada hasta 2.5 Gbps	Hasta 10 Gbps
Multiplexacción	En el nivel de red	En el nivel de enlace	En el nivel de red	Con GMPLS
Control de congestion	No necesario	Necesario	Necesario	No necesario
Tamaño de paquete	Hasta 512 bytes	Hasta 4096 bytes	1518 bytes	Hasta 1500 bytes
Manejo de Información	Por Paquetes	Por Ráfagas de paquetes	Por celdas	Por etiquetado de

				paquetes

La Métrica: "*Es un valor utilizado por los protocolos de enrutamiento para asignar costos a fin de alcanzar cualquier red remota*." (Zinin, 2012); cada protocolo utiliza su propia métrica, por ejemplo RIP utiliza el conteo de saltos, EIGRP utiliza una combinación de ancho de banda y retardo, por su parte OSPF usa el ancho de banda. La métrica entra en función cuando el router aprende más de una ruta hacia el mismo destino, para tal fin el protocolo de enrutamiento debe evaluar y diferenciar entre las rutas disponibles y seleccionar la ruta con la métrica más baja. Aunque en realidad el router puede aprender sobre una ruta hacia la misma red a través de más de un origen (en ruta estática) como lo dicen los tres principios relacionados con las tablas de enrutamiento extraídos del libro de Alex Zinin, Cisco IP Routing:

1. *"(…) Cada router toma su decisión en forma independiente, según la información de su propia tabla de enrutamiento.*
2. *El hecho de que un router tenga cierta información en su tabla de enrutamiento no significa que los otros routers tengan la misma información.*
3. *La información de enrutamiento sobre una ruta desde una red a otra no suministra información de enrutamiento sobre la ruta inversa o de regreso"* (Zinin, 2001).

Después de tener un conocimiento sobre lo que vamos a realizar empezaremos con la configuración.

Pasos para la Configuración de una red VPN MPLS que interconecta clientes con su sitio central.

1) Inicialmente ejecutamos el protocolo de enrutamiento OSPF (IGP) en una sola área (área 0) y se activa MPLS en cada interfaz entre enrutadores PE y P el cual no transportará tráfico de usuario. Con esto pretendemos que dicho ISP apenas

está iniciando su operación y que aún no tiene usuarios conectados, por ahora el tráfico es completamente interno, ver figura 5.

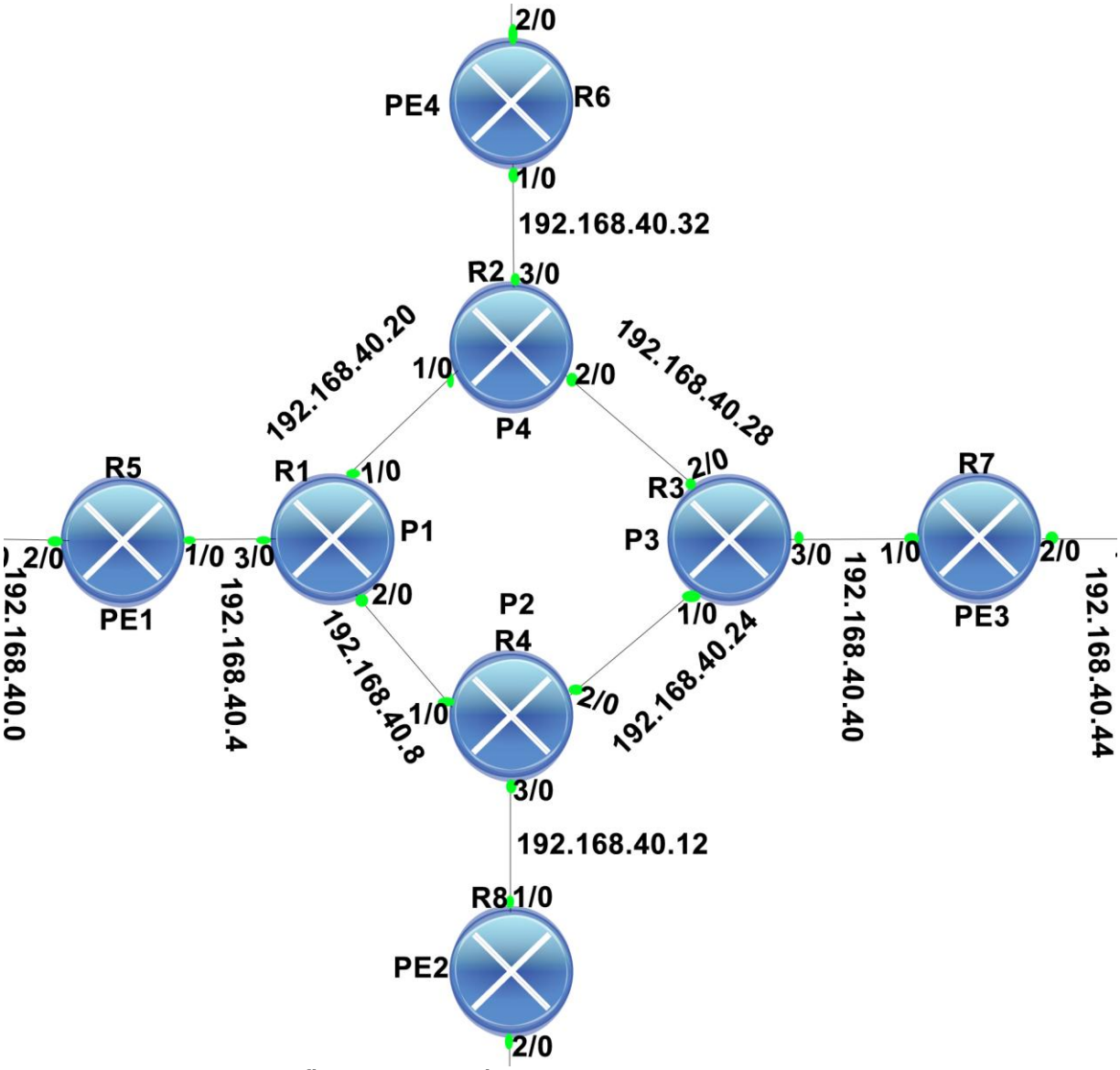

figura 5. Enrutamiento entre PEs y Ps

2) Configuración de los VRFs “Los VRF son básicamente enrutadores virtuales dentro de un enrutador físico” (VRF, 2009). Una instancia VRF contiene una tabla de enrutamiento que está completamente separada (y es independiente) tanto de otras tablas de enrutamiento correspondiente a otros VRF como de la tabla de enrutamiento principal del enrutador) en los enrutadores PE (R6, R5, R7 y R8) los

demás R1, R2, R3, R4 no requiere de una configuración adicional puesto que desempeña el papel de un equipo P (intercambio de etiquetas).

3) Ahora que se tienen configurados los VRFs en los enrutadores PE, estos VRFs se aplican a las interfaces de cada enrutador PE que esté recibiendo a un enrutador CE, pero teniendo en cuenta al respectivo usuario recibido por cada interface.

4) Después de tener los VRFs configurados y activos, es momento de realizar la configuración con una ruta por defecto. Empezaremos con la configuración básica en los enrutadores CE, es decir, en todos los equipos de borde del usuario (R1, R2, R3, R4).

El equipo del cliente no se le tendrá que configurar mas que una ruta que conozca a otros clientes de la misma VPN y al proveedor de servicio.

5) Lo siguiente es configurar en los enrutadores PE una ruta estática para que formen adyacencias con los enrutadores CE.

6) Para que las sucursales de cada usuario del ISP se puedan comunicar mutuamente. Se configura parejas VPNv4 a traves de BGP entre los enrutadores PE (Cuando BGP está funcionando de esta manera, con frecuencia se le refiere con el nombre MP-BGP) este protocolo es preferido por su flexibilidad y extensibilidad. Las rutas transportadas dentro de MP-BGP se conocen como rutas VPNv4. BGP se refiere a familias de direcciones (address families*). Esto* permite que BGP pueda distinguir cual tipo de rutas está viendo (enviando o recibiendo) con el fin de que entre ellos se intercambien rutas VPNv4.

Con esto concluye la configuración de VPN basadas en MPLS. Para entender mejor mas adelante en este documento se comprobara las configuraciones hechas anteriormente.

Envió de paquetes a través del Backbone MPLS VPN

Cuando un paquete IP ingresa al backbone MPLS VPN al enrutador PE proveniente del enrutador CE, se le introducen 2 etiquetas o labels una de ellas es la etiqueta vpn label (etiqueta mas interna) la cual determinará cual será el enrutador PE de salida que recibirá el paquete y la otra es la etiqueta externa label, dicha etiqueta determinara cual será el enrutador P que esta antes del enrutador PE de salida, luego un prefijo de 64 bits es añadido al paquete y eso lo hace único. Los P router realizan un switcheo (conmutación) de etiquetas y el paquete alcanza al PE router de salida. El PE router realiza un lookup sobre la etiqueta de VPN y envía el paquete al router CE. A través de esta función los routers no ven el paquete en sí sino su etiqueta, ver figura 6.

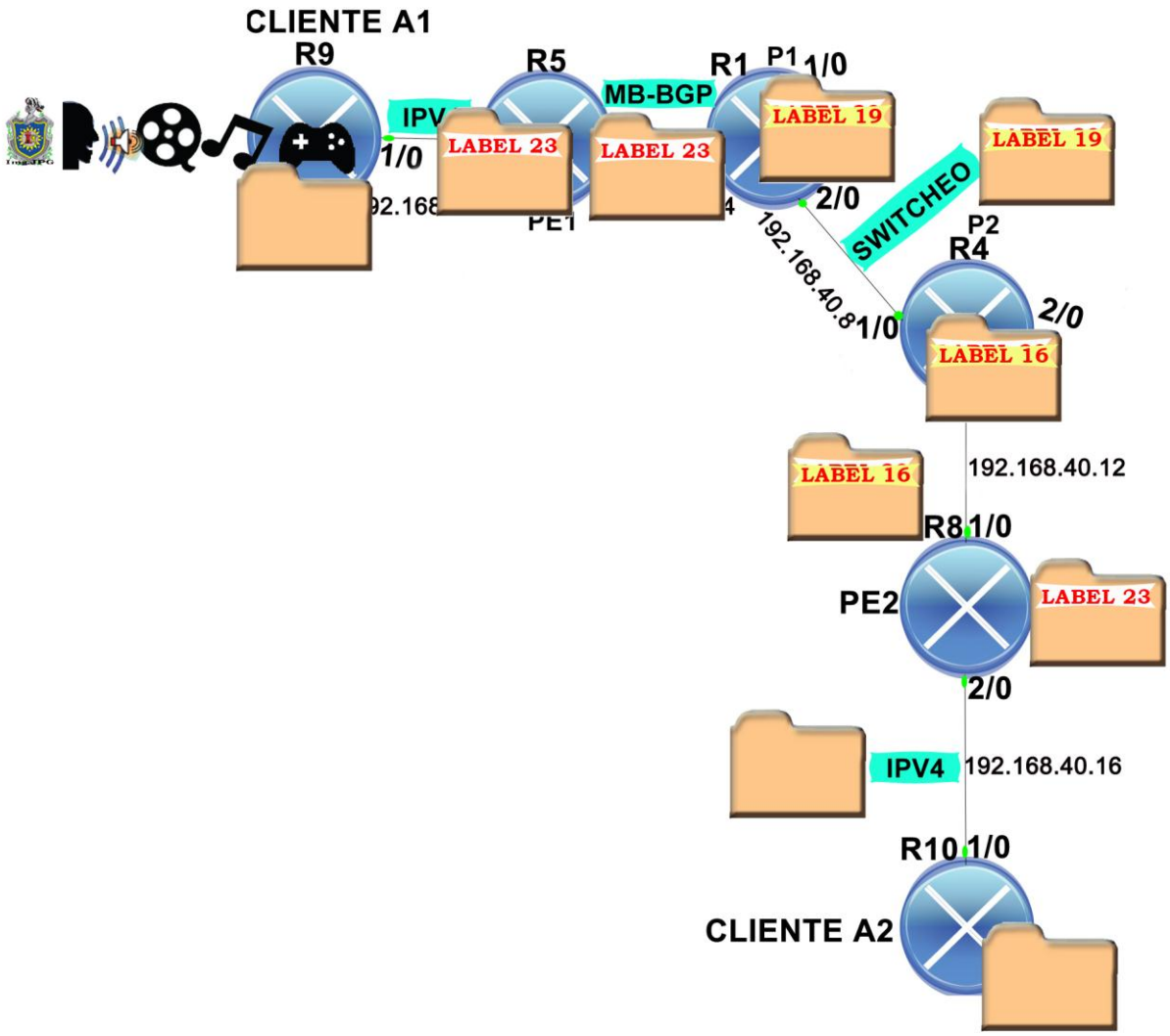

Figura 6. Envío de paquetes a través del Backbone.

4.1 DEFINICIÓN DEL PROTOCOLO DE ENRUTAMIENTO OSPF

"Open Shortest Path First (frecuentemente abreviado OSPF) es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - Link StateAlgorithm) para calcular la ruta más corta posible". OSPF es probablemente el tipo de protocolo IGP más utilizado en grandes redes. IS-IS, es más común en grandes proveedores de servicio (RFC de OSPF, 1998).

4.1.1 Difusión de la topología de la red

Se configurara el protocolo OSPF en la nube para lograr que exista conectividad MPLS entre las distintas terminales, teniendo previamente determinada la IP correspondiente a cada enrutador.

OSPF mantiene actualizada la capacidad de enrutamiento entre los nodos de una red mediante la difusión de la topología de la red y la información de estado-enlace de sus distintos nodos. Esta difusión se realiza a través de varios tipos de paquetes:

- Paquetes Hello (tipo 1). Cada router envía periódicamente a sus vecinos un paquete que contiene el listado de vecinos reconocidos por el router, indicando el tipo de relación que mantiene con cada uno.

- Paquetes de descripción de base de datos estado-enlace (DataBaseDescription, DBD) (tipo 2). Se emplean en el intercambio de base de datos enlace-estado entre dos nodos, y permiten informar al otro nodo implicado en la sincronización acerca de los registros contenidos en la LSDB propia, mediante un resumen de estos.

- Paquetes de estado-enlace o Link State Advertisements (LSA). Los cambios en el estado de los enlaces de un router son notificados a la red

mediante el envío de mensajes LSA. Dependiendo del estatus del router y el tipo de información transmitido en el LSA, se distinguen varios formatos (entre paréntesis, las versiones de OSPF en que se utilizan):

- (OSPFv2 y v3) Router-LSA o LSA de encaminador.
- (OSPFv2 y v3) Network-LSA o LSA de red.
- (OSPFv2 y v3) Summary-LSA o LSA de resumen. En OSPFv2 se distinguen dos tipos: tipo 3, dirigidos a un router fronterizo de red; y tipo 4, dirigidos a una subred interna. En OSPFv3, los Summary-LSA tipo 3 son renombrados como Inter-Area-Prefix-LSA, y los tipo 4 pasan a denominarse Intra-Area-Prefix-LSA.
- (OSPFv2 y v3) AS-External-LSA o LSA de rutas externas a la red.
- (OSPFv3) Link-LSA o LSA de enlace, que no se retransmite más allá del link del origen.

4.1.2 Áreas en las que trabaja OSPF

OSPF organiza un sistema autónomo (AS) en áreas. Estas áreas son grupos lógicos de routers cuya información se puede resumir para el resto de la red. Un área es una unidad de enrutamiento, es decir, todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (Link State Data base)

OSPF distingue los siguientes tipos de área:

Área Backbone: El backbone, también denominado área cero, forma el núcleo de una red OSPF. Es la única área que debe estar presente en cualquier red OSPF, y mantiene conexión, física o lógica, con todas las demás áreas en que esté particionada la red. La conexión entre un área y el backbone se realiza mediante los ABR, que son responsables de la gestión de las rutas no-internas del área (esto es, de las rutas entre el área y el resto de la red).

Área stub: Un área stub es aquella que no recibe rutas externas. Las rutas externas se definen como rutas que fueron inyectadas en OSPF desde otro protocolo de enrutamiento. Por lo tanto, las rutas de segmento necesitan normalmente apoyarse en las rutas predeterminadas para poder enviar tráfico a rutas fuera del segmento.

Área not-so-stubby: También conocidas como NSSA, constituyen un tipo de área stub que puede importar rutas externas de sistemas autónomos y enviarlas al backbone, pero no puede recibir rutas externas de sistemas autónomos desde el backbone u otras áreas.

4.1.3 Tipos de router en OSPF:

Un router OSPF clásico es capaz de enrutar cualquier paquete destinado a cualquier punto del área en el que se encuentra (enrutamiento intra-area). Para el enrutamiento entre distintas áreas del AS (enrutamiento inter-area) y desde el AS hacia el exterior (enrutamiento exterior), OSPF utiliza routers especiales que mantienen una información topológica más completa que la del área en la que se sitúan. Así, pueden distinguirse:

- Routers fronterizos de área o ABRs (AreaBorderRouters), que mantienen la información topológica de su área y conectan ésta con el resto de áreas, permitiendo enrutar paquetes a cualquier punto de la red (inter-arearouting).

- Routers fronterizos del AS o ASBRs (AutonomousSystemBorderRouters), que permiten encaminar paquetes fuera del AS en que se alojen, es decir, a otras redes conectadas al Sistema Autónomo o resto de Internet (externalrouting).

4.1.4 Interfaces en OSPF

Los nodos de una red basada en OSPF se conectan a ella a través de una o varias interfaces con las que se conectan a otros nodos de la red. El tipo de enlace (link) define la configuración que asume la interface correspondiente. OSPF soporta las siguientes tipos de enlace, y provee para cada uno de ellos una configuración de interfaz:

- Punto a punto (point-to-point, abreviadamente ptp), cuando la interfaz está conectada exclusivamente a otra interfaz.
- Punto a multipunto (point-to-multipoint, abreviadamente ptmp).
- Broadcast, para enlaces en los que todas las interfaces pueden conectarse directamente entre ellas. El ejemplo típico de enlace broadcast es el que corresponde a una red de tipo Ethernet.
- Enlace virtual (virtual link), cuando no responde a una topología física.
- Enlace de múltiple acceso no-broadcast (Non-broadcast Multiple Access, NBMA), para enlaces en los que el medio es compartido pero no todas las interfaces participantes pueden comunicarse directamente entre sí.

4.1.5 Estado de las interfaces

- Down (sin actividad).
- Waiting (estado de espera).
- Loopback.
- Point-to-point (interface punto a punto)
- DR, abreviatura de Designated Router (interface de enrutador designado).
- Backup, por Backup Designated Router (interface de enrutador designado auxiliar, BDR).
- DROther (interface en una red broadcast o NBMA sin estatus DR ni BDR).

4.2 TOPOLOGÍA LÓGICA PARA LA RED DE TRANSPORTE MPLS VPN

4.2.1 Topologia parcial mesh (VPN MPLS)

Los servicios de redes privadas virtuales están orientados claramente hacia el cliente, pero no en todos los casos se puede implementar cualquier tipo de topología de red por motivos estructurales de la empresa, distribución de sedes de la misma, tipo de aplicaciones y servidores utilizados y su disposición en las distintas sedes de la empresa, etc.

En resumen, por los elevados costes que puede significar la implementación o no de un tipo de topología de red determinado, como puede ser el caso de la topología Hub and Spoke o full mesh.

.

Por estos y otros motivos, en muchos casos, se buscan otras soluciones topológicas para implementar el servicio VPN en una empresa. Estas soluciones son topologías totalmente o parcialmente malladas.

La topología implementada en el diseño es la topología Partial-Mesh cuando solo algunos nodos de la red tienen conectividad directa con el resto de nodos de la red, es decir, algunos de los nodos tendrán conectividad directa con el resto de nodos y otros únicamente estarán conectados a uno o dos nodos en la red de forma directa. Una topología Partial Mesh normalmente se implementa en redes de acceso que a su vez están conectadas a redes con topología Full-Mesh. Podemos ver un ejemplo de red con topología Partial-Mesh en la figura 1 mostrada anteriormente.

4.3 IMPLEMENTACION MPLS VPN

4.3.1 Beneficios

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

- **Seguridad**

A través de la configuración de las tablas virtuales en el PE router es posible el aislamiento del tráfico entre VPNs donde el PE router es el único en tener conocimiento acerca de cada VPN que está configurada en el backbone Adicionalmente la utilización de etiquetas para distinguir los paquetes IP asegura que los paquetes serán entregados a la VPN correcta

- **Escalabilidad de la red**

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

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

- **Extranets e Intranets**

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

- **Otras**

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

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

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

4.4 VERIFICAR EL FUNCIONAMIENTO DE LA RED MPLS UTILIZANDO LOS COMANDOS ADECUADOS PARA SU INTERPRETACIÓN

4.4.1 Verificar el Estado OSPF de la red

Una vez configurado OSPF, podemos revisar la tabla de enrutamiento de R12 para tener una idea del estado de la red, para ello se usa el comando sh ip route.

R12# show ip route

```
Router>sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.40.45 to network 0.0.0.0

     192.168.40.0/30 is subnetted, 1 subnets
C       192.168.40.44 is directly connected, GigabitEthernet1/0
     150.1.0.0/32 is subnetted, 1 subnets
C       150.1.12.12 is directly connected, Loopback0
S*   0.0.0.0/0 [1/0] via 192.168.40.45
Router>
```

Para verificar los protocolos configurados en los router usamos el comando Show ip protocols en este caso sobre R5:

```
Router#sh ip protocols
Routing Protocol is "ospf 100"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 150.1.5.5
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    150.1.0.0 0.0.255.255 area 0
    192.168.40.0 0.0.0.255 area 0
 Reference bandwidth unit is 100 mbps
  Routing Information Sources:
    Gateway         Distance      Last Update
    150.1.1.1            110      00:02:55
    150.1.7.7            110      00:02:55
    150.1.8.8            110      00:02:55
    150.1.3.3            110      00:02:55
    150.1.6.6            110      00:02:55
    150.1.2.2            110      00:02:55
    150.1.4.4            110      00:02:55
  Distance: (default is 110)

Routing Protocol is "bgp 101"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Maximum path: 1
  Routing Information Sources:
    Gateway         Distance      Last Update
  Distance: external 20 internal 200 local 200
```

Podemos ver en la tabla de enrutamiento la verificación que los enrutadores han aprendido sobre la existencia de todas las redes conectadas al núcleo MPLS (incluyendo las direcciones de Loopback) por medio de OSPF, excepto para los enlaces que se conectaran a futuros usuarios.

R4#show ip ospf neighbors (Para verificar vecinos conectados)

```
Router#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
150.1.8.8         1   FULL/DR         00:00:36    192.168.40.14   GigabitEthernet3/0
150.1.3.3         1   FULL/BDR        00:00:36    192.168.40.26   GigabitEthernet2/0
150.1.1.1         1   FULL/BDR        00:00:35    192.168.40.9    GigabitEthernet1/0
Router#
Router#
```

4.4.2 Verificar el funcionamiento de MPLS en la red

Una vez completada la configuración de todos los enrutadores conectados al núcleo, podemos verificar que se han establecido las sesiones LDP y que se están comunicando.

show mpls interfaces**(** Muestra las interfaces en las que está funcionando MPLS-LDP).

R5# sh mpls interfaces

```
Router>sh mpls interface
Router>sh mpls interfaces
Interface              IP            Tunnel   Operational
GigabitEthernet1/0     Yes (ldp)     No       Yes
Router>
```

show mpls ldp neighbor (Muestra los routers que mantienen una relación de vecindad con el router en el que se ejecuta el comando).

R5# sh mpls ldp neighbor

```
Router>sh mpls ldp neighbor
    Peer LDP Ident: 150.1.1.1:0; Local LDP Ident 150.1.5.5:0
        TCP connection: 150.1.1.1.646 - 150.1.5.5.14443
        State: Oper; Msgs sent/rcvd: 36/36; Downstream
        Up time: 00:15:35
        LDP discovery sources:
          GigabitEthernet1/0, Src IP addr: 192.168.40.6
        Addresses bound to peer LDP Ident:
          192.168.40.21   150.1.1.1       192.168.40.9    192.168.40.6
Router>
```

show mpls ldp binding (Muestra la tabla de etiquetas que está utilizando el router donde se ejecuta el comando).

R5# sh mpls ip binding

```
Router>sh mpls ip binding
  150.1.1.1/32
        in label:     23
        out label:    imp-null  lsr: 150.1.1.1:0      inuse
  150.1.2.2/32
        in label:     24
        out label:    16        lsr: 150.1.1.1:0      inuse
  150.1.3.3/32
        in label:     25
        out label:    22        lsr: 150.1.1.1:0      inuse
  150.1.4.4/32
        in label:     26
        out label:    23        lsr: 150.1.1.1:0      inuse
  150.1.5.5/32
        in label:     imp-null
        out label:    24        lsr: 150.1.1.1:0
  150.1.6.6/32
        in label:     27
        out label:    25        lsr: 150.1.1.1:0      inuse
  150.1.7.7/32
        in label:     28
        out label:    26        lsr: 150.1.1.1:0      inuse
  150.1.8.8/32
        in label:     29
        out label:    27        lsr: 150.1.1.1:0      inuse
  192.168.40.4/30
        in label:     imp-null
        out label:    imp-null  lsr: 150.1.1.1:0
  192.168.40.8/30
        in label:     16
        out label:    imp-null  lsr: 150.1.1.1:0      inuse
  192.168.40.12/30
        in label:     21
        out label:    19        lsr: 150.1.1.1:0      inuse
  192.168.40.20/30
        in label:     17
        out label:    imp-null  lsr: 150.1.1.1:0      inuse
  192.168.40.24/30
        in label:     20
        out label:    20        lsr: 150.1.1.1:0      inuse
  192.168.40.28/30
        in label:     19
        out label:    17        lsr: 150.1.1.1:0      inuse
  192.168.40.32/30
        in label:     18
        out label:    18        lsr: 150.1.1.1:0      inuse
  192.168.40.40/30
        in label:     22
        out label:    21        lsr: 150.1.1.1:0      inuse
Router>
```

show mpls forwarding-table Muestra la tabla de forwarding del router donde se ejecuta el comnnando.

R5# sh mpls forwarding-table

```
Router>sh mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     192.168.40.8/30  0          Gi1/0      192.168.40.6
17     Pop tag     192.168.40.20/30 0          Gi1/0      192.168.40.6
18     18          192.168.40.32/30 0          Gi1/0      192.168.40.6
19     17          192.168.40.28/30 0          Gi1/0      192.168.40.6
20     20          192.168.40.24/30 0          Gi1/0      192.168.40.6
21     19          192.168.40.12/30 0          Gi1/0      192.168.40.6
22     21          192.168.40.40/30 0          Gi1/0      192.168.40.6
23     Pop tag     150.1.1.1/32     0          Gi1/0      192.168.40.6
24     16          150.1.2.2/32     0          Gi1/0      192.168.40.6
25     22          150.1.3.3/32     0          Gi1/0      192.168.40.6
26     23          150.1.4.4/32     0          Gi1/0      192.168.40.6
27     25          150.1.6.6/32     0          Gi1/0      192.168.40.6
28     26          150.1.7.7/32     0          Gi1/0      192.168.40.6
29     27          150.1.8.8/32     0          Gi1/0      192.168.40.6
30     Aggregate   192.168.40.0/30[V]   \
                                    0
31     Untagged    150.1.0.0/32[V]  0          Gi1/0      192.168.40.6
Router>
```

4.4.3 Verificación de un Proveedor de servicios (PE) con sus sucursales (CE)

Para verificar que un enrutador PE está recibiendo información de sus vecinos enrutadores CE a través de BGP, se usa el comando **sh ip bgp vpnv4 all**:

R5# sh ip bgp vpnv4 all

```
Router>sh ip bgp vpnv4 all
BGP table version is 10, local router ID is 150.1.5.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf clienteA)
*> 150.1.0.0/32     192.168.40.18            0         32768 ?
* i                 150.1.8.8                0    100      0 ?
*> 192.168.40.0/30  0.0.0.0                  0         32768 ?
*>i192.168.40.16/30 150.1.8.8                0    100      0 ?
Router>
```

En la salida vamos a observar que R1 está recibiendo rutas de los usuarios por medio del protocolo eBGP y que dichas rutas están siendo asociadas con los respectivos VRFs previamente configurados. Mediante el comando **sh ip route vrf clienteA** podemos observar las tablas VRF, usando al usuario A como ejemplo:

R5# sh ip route vrf clienteA

```
Router>sh ip route vrf clienteA

Routing Table: clienteA
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.40.0/30 is subnetted, 2 subnets
C       192.168.40.0 is directly connected, GigabitEthernet2/0
B       192.168.40.16 [200/0] via 150.1.8.8, 00:18:18
     150.1.0.0/32 is subnetted, 1 subnets
S       150.1.0.0 [1/0] via 192.168.40.18
Router>
```

Se observara, dentro del enrutador R1 las redes de cada usuario estarán separadas a nivel lógico de las redes de otros usuarios.

4.4.4 Verificar el intercambio de rutas VPNv4 entre los enrutadores PE

R5# sh ip bgp vpnv4 vrf cliente A 150.1.9.9

En este punto, se debe tener completa conectividad extremo-a-extremo (end-to-end) entre las redes de cada usuario del ISP

R5:

```
Router#SH IP BGp VPnv4 VRf clienteA 150.1.9.9
BGP routing table entry for 1:1:150.1.9.9/32, version 2
Paths: (1 available, best #1, table clienteA)
  Advertised to update-groups:
     2
  9
    192.168.40.1 from 192.168.40.1 (150.1.9.9)
      Origin incomplete, metric 0, localpref 100, valid, external, best
      Extended Community: RT:1:1
      mpls labels in/out 30/nolabel
Router#SH IP BGp VPnv4 VRf clienteA 150.1.10.10
BGP routing table entry for 1:1:150.1.10.10/32, version 7
Paths: (1 available, best #1, table clienteA)
  Advertised to update-groups:
     1
  10
    150.1.8.8 (metric 4) from 150.1.8.8 (150.1.8.8)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1
      mpls labels in/out 32/30
Router#
```

4.4.5 Verificación del funcionamiento de la VPN-MPLS

Con los siguientes comandos podremos verificar que la VPN que hemos configurado está funcionando según lo esperado:

1. show ip route vrf <nombre VRF> en

   R5

```
Router>sh ip route vrf clienteA

Routing Table: clienteA
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     192.168.40.0/30 is subnetted, 2 subnets
C       192.168.40.0 is directly connected, GigabitEthernet2/0
B       192.168.40.16 [200/0] via 150.1.8.8, 00:18:18
     150.1.0.0/32 is subnetted, 1 subnets
S       150.1.0.0 [1/0] via 192.168.40.18
Router>
```

Con este comando podremos comprobar los prefijos que se han exportado y los que se han importado en la tabla de routing de la VRF y por ende los prefijos que formarán parte de la VPN.

2. traceroute vrf <nombre VRF><Dirección a la que queremos llegar>

```
Router#traceroute vrf clienteA 192.168.40.1

Type escape sequence to abort.
Tracing the route to 192.168.40.1

  1 192.168.40.13 [MPLS: Labels 20/23 Exp 0] 28 msec 28 msec 28 msec
  2 192.168.40.9 [MPLS: Labels 19/23 Exp 0] 12 msec 12 msec 36 msec
  3 192.168.40.2 [MPLS: Label 23 Exp 0] 56 msec 52 msec 56 msec
  4 192.168.40.1 32 msec 32 msec *
Router#
```

El funcionamiento de este comando es exactamente el mismo que el de un traceroute normal, pero para comprobar el funcionamiento de la VPN y usando direcciones destino de la propia VPN, con origen un equipo que pertenezca a la misma VPN necesitamos añadir el parámetro vrf junto al nombre de la vrf que pertenece a nuestra VPN.

3.ping vrf <nombre VRF> <Dirección a la que queremos llegar

```
Router>ping vrf clienteA 192.168.40.18

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.40.18, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/13/32 ms
Router>
```

El funcionamiento es exactamente el mismo que el de un ping normal, la explicación del uso del parámetro vrf se aplica exactamente igual que en el comando anterior.

5. CONCLUSIÓN

A través de este diseño podemos decir que la tecnología MPLS VPN es la evolución natural de las redes existentes que quieren converger en sistemas de comunicaciones que puedan soportar las capacidades necesarias del crecimiento de Internet y al mismo tiempo, que permitan a los administradores de redes controlar el tráfico de una forma más sencilla, visual y especifica.

El hecho de simplemente intercambiar etiquetas, en vez de la interpretación y el procesamiento de todo un encabezado IP en cada salto de un paquete IP, provee una mejor manera de enviar paquetes, lo que al mismo tiempo ofrece la oportunidad de enviar flujos de tráfico a una mayor velocidad.

Después de haber hecho los pasos necesarios para la implementación y diseño, de la forma más concreta y precisa posible, de una red MPLS y sus servicios de VPN, se pudo observar la forma como se envían los paquetes de datos (voz, video e imagen), la manera como se da el intercambio de etiquetas cuando un cliente envía o recibe un paquete, de esta manera los router de otros clientes no ven el paquete en si sino su etiqueta y no se correrá el riesgo de extracción o manipulación de algún dato

MPLS supera ampliamente a tecnologías como ATM o Frame- Relay en el sentido que reduce costos a los SP y permite ocupar enlaces Ethernet a nivel de capa física para el transporte de datos en forma de paquetes. Esto hace que el escalamiento de ancho de banda para el SP sea menos costoso en comparación con otras tecnologías como ATM y Frame-Relay.

La conmutación aporta mayor escalabilidad de redes, mayor control en la QoS y lo que más importa a las empresas, mayor control sobre la Ingeniería del Tráfico.

6. BIBLIOGRAFÍA

GNS3, Dynamips, Dynamips Blog, Dynagen (front-end basado en texto al emulador): Software (20/08/12)

http://www.gns3.net

http://www.ipflow.utc.fr/index.php/Cisco_7200_Simulator
http://www.ipflow.utc.fr/blog
http//dyna-gen.sourceforge.net

Centro de Recursos MPLS (23/08/12)

http://www.mplsrc.com

Este es el enlace donde obtuvimos una guía de inicio rápido para la utilización del programa GNS3(25/08/12)

http://geexhq.com/wp-content/uploads/2009/11/simulating-network-lab.pdf

Tutorial de GNS3 (03/09/12)

http://www.garciagaston.com.ar/verpost.php?id_noticia=136

Web del IETF. 19/08/2012

http://www.ietf.org

Para qué sirve la red vpn mpls en la actualidad (05/09/12)

http://www.networkworld.es/MPLS:-Ventajas-para-las-empresas/seccion-/articulo-134391

http://www.networkworld.es/Migracion-a-MPLS--__Por-que__-__Cuando__-__Como__/seccion-articulo/articulo-187143

Primeros capítulos de MPLS Fundamental (18/08/12)

MPLSTutorial.com

http://tools.ietf.org/html/rfc5462

http://es.wikipedia.org/wiki/Asynchronous_Transfer_Mode (11/12/12)

RFc 740 Sobre sitio Remoto13/12/12

www.normes-internet.com/normes.php?rfc=rfc740&lang=es

http://es.wiktionary.org/wiki/remoto

definición de Sitio13/12/12

www.wordreference.com/definicion/sitio

RFC de OSPF 13/13/12.

https://tools.ietf.org/rfc/rfc2328.txt

http://wwwin.cisco.com/cpress/cc/td/cpress/fund/iprf/ip2912.htm

Intoducción a tecnologías WAN 13/12/12

wwwin.cisco.com/cpress/cc/td/cpress/fund/ith2nd/it2403.htm

RFC de OSPF. (2 de abril de 1998). Recuperado el 12 de 12 de 13, de RFC 2328: https://tools.ietf.org/rfc/rfc2328.txt

Cisco 7200 . (2007). Recuperado el 20 de 08 de 2012, de Series Routers: http://www.cisco.com/en/US/prod/collateral/routers/ps341/product_data_sheet09186a008008872b.html

VRF. (11 de 06 de 2009). Recuperado el 20 de 08 de 2012, de Dreamer CISCO: http://ciscodreamer.blogspot.com/2009/06/vrf-basics.html

Alex Zinin, A. (2001). Construcción de la tabla de Enrutamiento. En A. Zinin, *Cisco IP Routng* (pág. 22). Cisco Systems Inc.

7. GLOSARIO

A

ABRs Area Border Routers. Router de bordes

Área stub: Un área stub es aquella que no recibe rutas externas

AS Autonomous System. Sistema Autónomo.

ASBRs Autonomous System Border Routers. Sistemas autónomos de bordes.

ATM Asynchronous Transfer Mode. Modo de transferencia asíncrono.

B

Backbone Conjunto de routers que componen la parte troncal de una red.

Backup Designated Router (interface de enrutador designado)

BGP Border Gateway Protocol. Protocolo de pasarela externa.

Banda Ancha es un conjunto de tecnologías que permiten ofrecer a los usuarios altas velocidades de comunicación y conexiones permanentes.

C

CE Router del cliente que conecta el sitioe del cliente a la red del proveedor de servicio.

CSMA /CD acceso multiple con deteccion de portadora y deteccion de colisiones

CES routers de borde clientes.

CEF Cisco Express Forwarding. Conjunto de funcionalidades de los routers Cisco para poder ejecutar MPLS.

Core Núcleo de una red.

CoS-Aware Soporte de Clases de Servicio.

CPU Central Processing Unit. Unidad de proceso central.

D

DR Designated Router. Router designado.

DRAM Dynamic Random Access Memory. Memoria de acceso aleatorio dinámico.

DROther (interface en una red broadcast).

E

EGP External Gateway Protocol. Protocolo exterior de pasarela.

Ethernet Protocolo para redes de área local

F

FIB Forwarding Information Base. Base de información del reenvío.

Frame Relay Protocolo para la transmisión rápida de datos digitales en redes de comunicaciones.

FTP File Transfer Protocol. Protocolo de transferencia de ficheros, sistema de transferencia de ficheros en Internet

Full-Mesh Totalmente mallado.

G

GNs3 Graphical Network Simu- lator. Simulador grafico de redes que le permitirá diseñar fácilmente topologías de red y luego ejecutar simulaciones en él.

H

HTTP de HyperText Transfer Protocol (Protocolo de transferencia de hipertexto)

I

ID Identificador.

IETF Internet Engineering Task Force. Grupo de trabajo de ingenieros de Internet.

IGP Interior Gateway Protocol. Protocolo interior de pasarela.
iMBGP Internal Multiprotocol Border Gateway. Extensión de BGP para su utilización entre otros junto al protocolo MPLS.
Interworking (interfuncionamiento),
IOS Internetwork Operating System. Sistema Operativo de Interconexión de Redes. Creado por Cisco Systems.
IP Internet Protocol. Protocolo de Internet.
IPSEC Internet Protocol security. Extensión al protocolo IP al que añade servicios de seguridad.
IPv6 IP versión 6.
IS-IS Intermediate System-Intermediate System. Protocolo de enrutamiento interno.
ISP Internet Service Provider. Proveedor de servicios del Internet
IPv4 conjunto de direcciones asignadas

L

Label Etiqueta.
Label Stack Pila de Etiquetas.
LAN Local Area Network. Red de área local.
LDP Label Distribution Protocol. Protocolo de distribución de etiquetas.
LER Label Edge Router. Encaminador de etiquetas frontera.
LFIB Label Forwarding Information Base. Tabla incluida en el servicio MPLS en routers Cisco con la información de envío y recepción de etiquetas.
LIB Label Information Base. Tabla incluida en el servicio MPLS en routers Cisco con el listado de etiquetas a utilizar.
LSP Label Switched Path. Camino de conmutación de etiquetas.
LSR Label Switching Router. Encaminador de conmutación de etiquetas.
Glosario

M

MPLS Multiprotocol Label Switching. Multiprotocolo de conmutación de etiquetas.

N

Non-broadcast Multiple Access No enlace de multiple acceso

O

OSI Open System Interconnection. Sistema de interconexión abierta.

OSPF Open Shortest Path First. Protocolo abierto del primer camino más corto.

P

P Router del núcleo de red o backbone en un dominio MPLS.

Partial Mesh Mallado parcial.

PC Personal Computer. Ordenador personal.

PDU Protocol Data Unit. Unidad de datos del protocolo.

PE Router de acceso de una red no MPLS a un dominio MPLS.

PHP Penultimate-Hop-Popping. Proceso en el que el último router de un dominio MPLS retira la etiqueta y envía un paquete IP sin etiqueta.

PIX Private Internet Exchange

Point-to-point (interface punto a punto)

Point-to-multipoint punto a multipunto

PPP Point to Point Protocol. Protocolo punto a punto.

PVC Permanent Virtual Circuit. Circuito virtual permanente.

Q

QoS Quality Of Service. Calidad de servicio.

R

RD Route Distinguisher. Valor de 64 bits que se usa para evitar el solapamiento de direcciones IP en un entorno iMBGP.

Red C Conjunto de routers en la sede de cliente que están enfrentados a un dominio MPLS.

Red P Conjunto de routers del backbone o núcleo de red de un dominio MPLS.

RFC Request For Comments. Documento de especificaciones del IETF.

RIP Routing Information Protocol. Protocolo de información de encaminamiento.

RT Route Target. Identificadores de prefijos a exportar e importar en una VPN.

S

SLA Service Level Agreement. Acuerdo de Nivel de Servicio.

SVC Switched Virtual Circuit. Circuito virtual conmutado.

Switchs Ethernet (redes de area local)

T

TCP Transmision Control Protocol. Protocolo de control de la transmisión.

TCP/IP Transmisión Control Protocol/Internet Protocol. Protocolo de control de la transmisión/Protocolo IP.

TDP Tag Distribution protocol es un protocolo de distribución de etiquetas propietario de Cisco que es muy similar al estándar LDP

TE Traffic Engineering. Ingeniería de Tráfico.

TIB Tag information base, igual que LIB para LDP.

TTL Time To Live. Tiempo de vida.

U

UDP User Datagram Protocol. Protocolo de datagramas de usuario.

V

virtual link Enlace virtual

VPN Virtual Private Network. Red privada virtual.

VPN-MPLS Virtual Private Network MPLS. Red privada virtual sobre MPLS.

VRF Virtual Routing and Forwarding table. Tabla de rutas y reenvió en un router PE perteneciente a un VPN-MPLS.

w

WAN wide area network. Red de area amplia

X

x.25 Estándar para redes de paquetes recomendado por CCITT

8. ANEXO

Aquí veremos los pasos necesarios para configurar una red VPN MPLS.

Configuración e un equipo PE:

R5:

```
hostname R5
!
ip cef
!
interface Loopback0
ip address 150.1.5.5 255.255.255.255
!
mpls ip
!
interface gigabitethernet 2/0
ip address 192.168.40.2 255.255.255.252
mpls ip
gigabitethernet restart-delay 0
!
interface gigabitethernet 1/0
ip address 192.168.25.1 255.255.255.252
mpls ip
!
router ospf 100
log-adjacency-changes
network 150.1.0.0 0.0.255.255 area 0
network 192.168.40.0 0.0.0.255 area 0
```

Configuration en un equip P:

R1:

```
hostname R1
!
imp cef
!
interface Loopback0
ip address 150.1.1.1 255.255.255.255
!
mpls ip
!
interface gigabitethernet 1/0
ip address 192.168.40.21 255.255.255.252
mpls ip
serial restart-delay 0
!
interface gigabitethernet 2/0
ip address 192.168.40.9 255.255.255.252
mpls ip
!
interface gigabitethernet 3/0
ip address 192.168.40.6  255.255.255.252
mpls ip
!
router ospf 100
log-adjacency-changes
network 150.1.0.0 0.0.255.255 area 0
network 192.168.40.0 0.0.0.255 area 0
```

Configuración de los VRFs en los enrutadores PE (R6, R5, R7 y R8) los demás R1, R2, R3, R4 no requiere de una configuración adicional puesto que desempeña el papel de un equipo P)

R5:
ip vrf CustA
description Cliente A
rd 1:1
route-target export 1:1
route-target import 1:1

Ahora que se tienen configurados los VRFs en los enrutadores PE, estos VRFs se aplican a las interfaces de cada enrutador PE que esté recibiendo a un enrutador CE, pero teniendo en cuenta al respectivo usuario recibido por cada interface.

R5:
interface gigabitethernet 2/0
ip vrf forwarding CLIENTE A
ip address 192.168.40.2 255.255.255.252
Después de tener los VRFs configurados y activos, es momento de realizar la configuración BGP. Empezaremos con la configuración básica de BGP en los enrutadores CE, es decir, en todos los equipos de borde del usuario (R1, R2, R3, R4)

R9:
interface loopback 0
ip address 150.1.9.9 255.255.255.255

interface gigabitethernet 1/0
ip address 192.168.40.1 255.255.255.252

router bgp 9
bgp router-id 150.1.9.9
redistribute connected
neighbor 192.168.40.2 remote-as 101
no auto-summary

Lo que sigue es configurar los enrutadores PE para que formen adyacencias BGP con los enrutadores CE. Pondremos la configuración PE-a-PE y PE-a-CE bajo un solo proceso BGP, de tal manera que haya un solo aspecto por abordar. Cuando se configura MP-BGP, se requiere modificar la familia-de-direcciones que es IPv4 por defecto (address-family).

R5:

router bgp 101
bgp router-id 150.1.5.5
no bgp default ipv4-unicast
neighbor 192.168.40.1 remote-as 9
!
address-family ipv4 vrf CLIENTE A
neighbor 12.168.40.1 remote-as 9
neighbor 192.168.40.1 activate
exit-address-family

Para que las sucursales de cada usuario del ISP se puedan comunicar mutuamente. Vamos a configurar parejas VPNv4 entre los enrutadores PE con el

fin de que entre ellos se intercambien rutas VPNv4. Para simplificar las cosas, se creará una malla completa “full mesh” entre todos los enrutadores PE.

R5:

```
router bgp 101
neighbor 150.1.8.8 remote-as 101
neighbor 150.1.8.8 update-source lo0
neighbor 150.1.6.6 remote-as 101
neighbor 150.1.6.6 update-source lo0
neighbor 150.1.7.7 remote-as 101
neighbor 150.1.7.7 update-source lo0

!
address-family vpnv4
neighbor 150.1.8.8 activate
neighbor 150.1.8.8send-community extended
neighbor 150.1.6.6 activate
neighbor 150.1.6.6 send-community extended
neighbor 150.1.7.7 activate
neighbor 150.1.7.7 send-community extended
exit-address-family
```

Con esto concluye la configuración de VPN basadas en MPLS.