UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

"DISEÑO DE UNA RED IPVPN CON TECNOLOGÍA MPLS PARA INTERCONECTAR SEDES DE LA EMPRESA COSAPIDATA"

TRABAJO DE SUFICIENCIA PROFESIONAL
Para optar el Título Profesional de

INGENIERO ELECTRÓNICO Y TELECOMUNICACIONES

PRESENTADO POR EL BACHILLER

ADRIANZEN RUGEL, CINTHYA MILAGROS

Villa El Salvador
2017

DEDICATORIA

A mi querida familia,
por la confianza y apoyo
incondicional.

AGRADECIMIENTO

Agradezco a los maestros de la carrera profesional Ingeniería electrónica y telecomunicaciones por su dedicación, esfuerzo y tiempo dedicados a nuestro desarrollo profesional y lograr de nosotros personas útiles para la sociedad.

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

INDICE DE ANEXOS

INTRODUCCIÓN

El presente trabajo lleva por título “DISEÑO DE UNA RED IPVPN CON TECNOLOGIA MPLS PARA INTERCONECTAR SEDES DE LA EMPRESA COSAPIDATA.”, para optar el título de Ingeniero Electrónico y Telecomunicaciones, presentado por Cinthya Milagros Adrianzen Rugel.

El problema se observa en torno a la empresa, en la necesidad de tener comunicación con las sedes de Cosapi en tiempo real y de esa manera la sede principal la cual se encarga de la factibilidad y monitoreo de proyectos, tendria acceso a la base en cualquier momento y detectar problemas a tiempo. Actualmente los supervisores de cada proyecto envian mensual informes al area de factibilidad sobre los avances del proyecto a travez de la nube los cual no es seguro. Tambien se envian documentos a travez de una persona a la cual se contrata para hacer ello, esto produce retrasos.Cosapi quien cuenta con un enlace hacia el proveedor de servicios que va al POP de Arriola, que es altamente vulnerable a posibles cortes de servicio y que por ende afecta la conectividad a internet y con sedes de clientes, y a algunos aplicativos. Ademas de ello no hay manera de que la sede principal pueda hacer seguimiento a sus proyectos ya que solo hay una RPV entre cliente y proyecto, mas no una red propia de cosapi la cual se comunique con la sede principal.

Para ello, estableciendo un diseño IPVPN para las sedes de Cosapi en MPLS y un sistema autónomo se podría establecer una comunicación efectiva con los proveedores a través de internet mediante el protocolo y asi aprovechar todo el ancho de banda.

La estructura que hemos seguido en este proyecto se compone de 3 capítulos. El primer capítulo comprende el planteamiento del problema, el segundo capítulo el desarrollo del marco teórico y el tercer capítulo corresponde al desarrollo del diseño.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 DESCRIPCIÓN DE LA REALIDAD PROBLEMÁTICA

La empresa Cosapi actualmente cuenta con una red RPV para cada cliente la cual usa teconologia MPLS, es decir cada sede tiene una RPV, indepediente. La cual se comunica con la sede principal del cliente donde se prestan servicios, pero internamente no hay comunicación en tiempo real entre las sedes, y esto seria necesario ya que actualmente se envía personal para que traigan o lleven documentos. Como sabemos Cosapi es una empresa que tiene muchos proyectos y cada jefe de cada proyecto tienen que hacer reportes, informes y de alguna manera reportar a su base para su seguimiento y de esa manera justificar que el proyecto es óptimo.

Cosapi tiene un aplicativo llamado Aranda donde colocan todos sus proyectos y hace seguimiento mediente este aplicativo.

Este aplicativo se tendria que enlazar los proyectos para que en tiempo real se tenga toda esa informacion, cosa que no lo tiene cosapi por ahora.

Cosapi Cuenta con un enlace hacia el proveedor de servicios que va al POP de Arriola, lo que hace vulnerable a posibles cortes de servicio, afectando la conectividad a internet, conectividad entre sedes de los clientes, y a algunos aplicativos. Durante este tiempo se pierde información y tiempo por lo que perjudica económicamente a la empresa, considerando que cosapidata labora las 24 horas al día.

Actualmente el compartir recursos de otras sedes como servidores, telefonia, base de datos, es muy limitado debido al consumo que este proporciona, y la dificultad que se tiene al implementar nuevos servicios o hacer cambios.

Por ello se diseñará una IPVPN para las sedes de Cosapi en MPLS y un sistema autónomo de manera que pueda establecerse una comunicación efectiva con los proveedores a través de internet mediante protocolos y asi aprovechar todo el ancho de banda. Para ello, se usará el protocolo BGP para comunicarse debido a la baja cantidad de recursos del sistema que utiliza dado que permite verificar la tabla de enrutamiento sólo una vez y replicar las actualizaciones en todos los miembros además podemos usar calidad de servicio según las necesidades de la empresa.

1.2 JUSTIFICACIÓN DEL PROBLEMA

Debido a que la empresa Cosapi con más de 30 años de su funcionamiento la cual se encarga de diseñar, instalar, brindar mantenimiento

en el rubro de las telecomunicaciones y próxima a crecer más, es importante y necesario contar un una red a nivel WAN que permitan conectividad con otras sedes, asi como tambien sea de manera indepediente para cada proyecto que realice, de manera segura, confiable y rápida, así como también de una buena administración de ancho de banda para cada servicio según las necesidades de la empresa (QoS) y así poder brindarle un ancho de banda necesario para los datos que la empresa asigne como críticos de tal manera que cuando sature la navegación por internet no en la lentitud de otros servicio a los que la empresa considere como "datos críticos".

Es importante tener una red que le permita al administrador evaluar de manera independiente cómo se comporta el tráfico en cada uno de los niveles de servicio (QoS)

La seguridad para la empresa es lo más importante, por ello para garantizarla es necesario que los datos que viajaran a través de la nube sean etiquetados. A si como también pueda eliminar Bucles y fallos en STP (Spanning Tree Protocol), bucles creados por enlaces redundantes, para que de esa manera podamos obtener puntos de transmisión ser óptimos.

1.3 DELIMITACIÓN DE LA INVESTIGACIÓN

1.3.1 Espacial

Se realizará en la empresa privada Cosapidata, ubicada en Calle Los Negocios 182, Surquillo.

1.3.2 Temporal

Comprende el periodo 10 Julio 2017 a Agosto 2017.

El mismo comprende en una simulación de una RPV propia de Cosapi donde la sede principal pueda tener acceso a la base de datos de todas las sedes de la empresa las cuales trabajan en diferentes proyectos.

1.4 FORMULACIÓN DEL PROBLEMA

¿De qué manera se puede diseñar una red IPVPN para las sedes de la empresa Cosapi usando la tecnología MPLS para que sea confiable, administrable y segura, logrando aprovechar el ancho de banda proporcionado por proveedor evitando congestión en la red de transporte troncal?

1.5 OBJETIVO

1.5.1 OBJETIVO GENERAL

Diseñar de red IPVPN con tecnología MPLS para las sedes de la empresa Cosapiata, para tener una mayor seguridad en el envió de información tanto para datos críticos y no críticos, que se manejan dentro de la empresa y evitar el congestionamiento de la red troncal.

1.5.2 OBJETIVO ESPECIFICO

- Aprovechar el ancho de banda asignado al 100 %
- Lograr la publicación de rutas mediante el protocolo BGP.
- Crear políticas de calidad de servicio.

CAPITULO II

MARCO TEÓRICO

2.1 ANTECEDENTES

A lo largo del proyecto se encontraron varias tesis que sirvieron de ayuda para el presente trabajo, entre ellas están:

Giancarlo G. (2009) " Propuesta de migracion de la red NGN DE UNA OPERADORA IMPLEMENTADA EN IP HACIA MPLS". Este estudio surge debido a la alta exigencia en la calidad de servicio, las redes públicas de telefonía tienden a migrar a las Redes de Próxima Generación (NGN) con las cuales podrán soportar todos los servicios de voz y datos a través de una sola red basada en conmutación de paquetes. Esta propuesta técnica para la migración de la red, en el nivel de transporte, del protocolo IP a IP/MPLS debe proporcionar calidad de servicio que las aplicaciones de hoy en día requieren

para poder funcionar con toda su capacidad debido a la complejidad que estas presentan. Tras la propuesta se concluye que los actuales operadores peruanos de una red NGN poseen un core IP. Estas redes son empleadas para la provisión de diferentes servicios de voz y datos sin brindar la calidad de servicio adecuada.

Ricardo M. (2012) "ESTUDIO DEL DESEMPEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN MPLS-VPN SOBRE MÚLTIPLES SISTEMAS AUTÓNOMOS". Este estudio surge debido a la necesidad proporcionar a una red escalabilidad, que permitan 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. Las redes debían tener conectividad privada a grandes distancias, o conectividad con más de un proveedor a la vez. Esto implica que muchas veces existirán VPNs que deban abarcar más de un sistema autónomo. Tras el diseño se concluyó que la implementación “Multi Protocol eBGP Multisalto entre Route Reflectors” como el más adecuado. Se pudo identificar que es el que mejores prestaciones presenta, ya que empleó sólo el 2% del CPU, además de tener tiempos de convergencia menores a 60 segundos y valores de retardo no mayores a 628 ms en el caso más crítico.

FAUSTO O. (2014). "Diseño de una red privada virtual con tecnología MPLS para la Carrera de Ingeniería de Networking de la Universidad de Guayaquil". La problemática planteada en este estudio es la necesidad de estar comunicado de manera rápida, eficaz y segura, ya que existe información valiosa para la parte educativa, administrativa, económica que debe estar a buen recaudo y a tiempo para mantener la integridad de la información. Es por

eso que se propone generar un camino virtual usando tecnología MPLS para garantizar la transmisión de la data, el mismo que puede acomodarse a distintos tipos de infraestructura basado en IP, ya que debido a su naturaleza el protocolo brinda conexiones “any to any” entre distintos puntos que comprendan una VPN, teniendo así el mejor camino o ruta en cada punto. Adicionalmente la disponibilidad que se tiene a nivel de la información o los recursos de la empresa, también debe tenerse en cuenta la parte de calidad de servicio por lo que con la metodología planteada va a poder contar con clases de servicio (CoS) dentro de una VPN con MPLS para así complementar las necesidades de cada servicio en particular. Tras el diseño se concluyó que la red la tecnología MPLS permite a los ISP incrementar la fiabilidad y confianza en sus redes por lo que beneficia al reducir tiempos en su transmisión de información y brinda seguridad requerida por el cliente. Cabe indicar que pueden ser usados varios protocolos de enrutamiento dinámico como RIP, EIGRP, OSPF o inclusive enrutamiento estático, pero por las bondades que tiene cada uno de ellos se prefiere trabajar con OSPF por sus ventajas con respecto a los otros protocolos.

VICTOR O. y JUAN Z. (2005). "SERVICIO DE LAN PRIVADA VIRTUAL SOBRE MPLS" La problemática planteada en este estudio es, la demanda actual de ancho de banda que requieren algunas aplicaciones como el video, la voz sobre IP para su correcto funcionamiento y ofrecer una infraestructura de redes convergente, las empresas fabricantes de dispositivos de redes están trabajando en el desarrollo de nuevas tecnologías para que los operadores puedan ofrecer nuevos servicios económicos, eficientes y confiables. Es por eso que se propone esta tesis. Por ello se pretende diseñar una red que

permita conectividad multipunto y habilita los servicios LAN a LAN, permitiéndole al operador optimizar los servicios de interconexión de redes corporativas ubicadas sobre un mismo backbone metropolitano, VPLS es la solución para que los operadores del servicio ofrezcan un mejor rendimiento y Calidad de servicio a sus suscriptores principalmente a las corporaciones que requieren de servicios de transporte nuevos, más económicos, rápidos y flexibles. De esta tesis se puede concluir que MPLS no se desarrollo para cambiar la tecnología de enrutamiento actual, ni para ser un protocolo que se utilice a nivel WAN, tampoco fue desarrollado para optimizar el ancho de banda; las verdaderas razones de su creación son: funcionar sobre cualquier tecnología de transporte no sólo ATM, soportar el envío de paquetes tanto unicast como multicast, permitir el crecimiento constante de la Internet y además ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP.

2.2 BASES TEÓRICAS

2.2.1 Redes de comunicación:

Definición: Se puede definir una red informática como un sistema de comunicación que conecta ordenadores y otros equipos informáticos entre sí, con la finalidad de compartir información y recursos. (UAP, 2010)

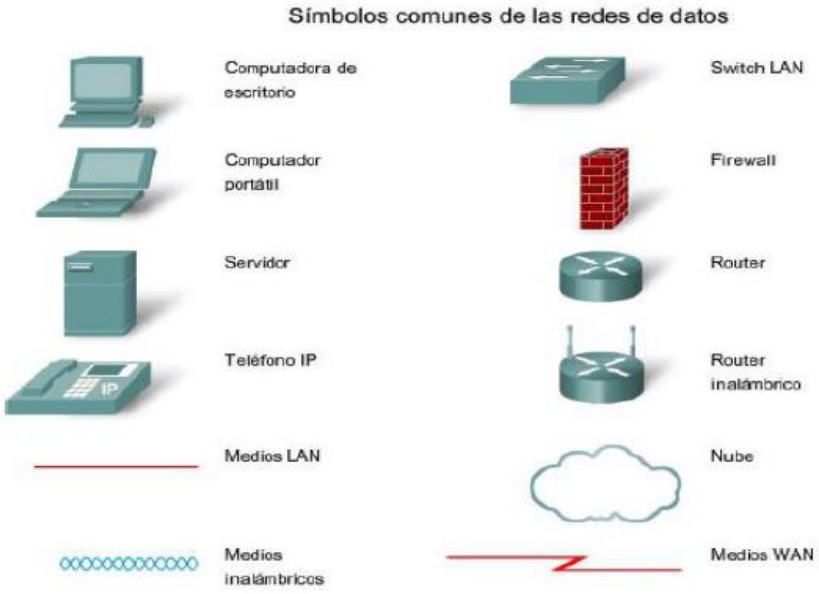
2.2.1.1 Componentes de una Red

Para determinar los elementos que componen una red debemos diferenciar entre los elementos físicos y los componentes lógicos. Entendemos por componentes físicos todo el hardware y medios físicos necesarios para la

comunicación entre ordenadores. Los componentes lógicos son los protocolos de comunicación y el software que permite esa comunicación. Resulta evidente que, dependiendo del tamaño de la red y las prestaciones que deseemos que nos ofrezca, estos componentes pueden aumentar en número y complejidad. (UAP, 2010)

En la figura 1 se muestran los elementos de una red típica.

Figura 1: Símbolos Comunes de las Redes de Datos



Fuente: CISCO

•Switch: el dispositivo más utilizado para interconectar redes de área local,

•Firewall: proporciona seguridad a las redes,

•Router: ayuda a direccionar mensajes mientras viajan a través de una red,

•Router inalámbrico: un tipo específico de router que generalmente se encuentra en redes domésticas,

• Nube: se utiliza para resumir un grupo de dispositivos de red.

Tipos de redes: Para clasificar una red se toman diversos criterios: si extensión, el uso de servidores, el tiempo de procesamiento, el método de envío, la arquitectura de la red y la topología. Según la extensión física de una red puede ser LAN, MAN, o WAN. (CNMC blog, 2010)

LAN, Local Area Network: Las redes LAN permiten a las empresas aplicar tecnología informática para compartir localmente archivos e impresoras de manera eficiente y posibilitar las comunicaciones internas.

Una red LAN se encuentra confinado dentro de un edificio o local. Cubre áreas de algunos kilómetros, el cableado es sumamente confiable por ser conocido y previsible. (CNMC blog, 2010)

MAN, Metropolitan Area Network: Una red MAN es una red que abarca un área metropolitana, como, por ejemplo, una ciudad o una zona suburbana. Una red MAN generalmente consta de una o más redes LAN, dentro de un área geográficamente común. Normalmente se utiliza un proveedor de servicios para conectar dos o mas redes LAN, utilizando líneas privadas de comunicación. (CNMC blog, 2010)

WAN, Wide Area Network: Las redes WAN interconectan redes LAN, que a su vez proporcionan acceso a los computadores o a los servidores de archivos ubicados en otros lugares. Cubre áreas de miles de kilómetros, los datos pasan por diversos tipos de cables y la probabilidad de error es mayor.

Las redes WAN pueden ser privadas o públicas. Una red WAN privada solo esta disponible para los miembros de la organización propietaria de la red, mientras que una red WAN, publica es de acceso libre. Internet es el mejor ejemplo de una red WAN publica a la que cualquiera puede conectarse.

SAN, Storage Area Nerwork: Una red SAN es una red dedicada de alto rendimiento utilizada para movilizar datos entre servidores y recursos de almacenamiento. Al ser una red separada y dedicada, se evita todo conflicto de trafico entre cliente y servidores.

La tecnología SAN permite una conexión de alta velocidad, de servidor a almacenamiento, almacenamiento a almacenamiento, o servidor a servidor.

Rendimiento. Las redes SAN permiten el acceso concurrente a arreglos de disco o cinta por 2 o más servidores a alta velocidad.

Disponibilidad. Las redes SAN **tienen** incorporada un sistema de tolerancia a fallas. Se puede hacer una copia exacta de los datos mediante una San hasta una distancia de 10 km.

Escalabilidad. al igual que una red LAN // WAN, una red SAN puede usar una amplia gama de tecnología. Esto permite la fácil reubicación de datos de copias de seguridad, operaciones, migración de archivos, y duplicación de datos entre sistemas.

VPN, Vitual Private Network:

Una red privada virtual VPN es una red privada que se contribuye dentro de una plataforma publica de servicios. Con una VPN, un empleado puede acceder remotamente a la red de la empresa a través de internet, formando un tunel seguro entre el PC del empleado y un router VPN en la sede,

Redes Peer to Peer y basadas en servidor:

No todas las redes hacen uso de servidores si no que su uso se condiciona a entornos en los cuales se requiere de un mayor rendimiento, seguridad, confiabilidad, y administración de los recursos y servicios.

A pesar de estas similitudes, las redes pueden dividirse en dos categorías:

- Punto a punto (Peer to Peer).

- Con servidor (Server- Based).

Las diferencias entre ambos tipos de redes son importantes, cada uno tiene diferentes capacidades. (CNMC blog, 2010)

Redes punto a punto: También conocida como redes de igual- a-igual. en una red punto a punto no existe jerarquía de ningún tipo entre los computadores conectados. Todos los computadores tienen la misma jerarquía y se conocen como puntos. Normalmente, cada computador funciona tanto como cliente cómos servidor, no existe ningún computador que juegue el papel de administrador responsable de la red. El usuario de cada computadora determina que información o recurso comparte en red. (CNMC blog, 2010)

Redes basadas en servidor: En un entorno con más de 10 computadores conectados a la red, una red punto-a-punto tal vez no sea lo más adecuado. Por lo tanto, algunas redes utilizan servidores dedicados. Un servidor dedicado es un computador que actúa como servidor y no como cliente o estación de trabajo. Es dedicado a que ha sido optimizado par responder rápidamente los requerimientos de los clientes de la red y para asegurar la información de los directorios del servidor.

A medida que los requerimientos de la red aumentan, se necesitaran mas de un servidor a la red.

Distribuyendo las tareas entre más de un servidor en la red, aseguramos que cada tarea se desarrolle de la manera más eficiente posible.

Topologías: Por la distribución física de los cables, una red se puede clasificar en: Bus, Estrella, Anillo, Malla, y Celular. Esto se conoce como topología física.

Las topologías mas populares entre las redes locales son:

La topología en bus y la topología en estrella. La topología en malla es propia de redes WAN. (CNMC blog, 2010)

Bus: Conocida como red de bus lineal. Es el más simple y común de los métodos para conectar computadores en red. Consiste en un cable llamado segmento que conecta a los computadores en línea simple.

Estrella: Esta topología ofrece administración centralizada de los recursos. Por lo tanto, debido a que cada computador está conectado a un punto central, se requiere de una gran cantidad de cable para instalar una gran red. Si este punto central falla, la red se viene abajo completamente.

Si un computador el cable que lo conecta a la red falla, solo la maquina que falla se desconectara de la red quedando imposibilitada de transmitir o recibir información. El resto de la red funciona en forma normal. (CNMC blog, 2010)

Anillo: Como el nombre lo sugiere se trata de una topología circular o de lazo cerrado. Las señales con pasadas de una entidad a otra en una sola dirección. Cada entidad dispone de un receptor en el cable de llegada y un transmisor en el cable de salida.

Las señales son regeneradas en cada entidad por lo que la degradación es mínima.

Celular: En una topología celular, se definen celular de servicio que dan cobertura a una determinada área, donde cada célula mantiene algún tipo de comunicación con las otras. Es ideal para servicio móviles. (CNMC blog, 2010)

Malla: Dispone de numerosos enlaces de comunicación entre las entidades, lo que la convierte en una topología robusta y tolerante a fallas.

Se usa principalmente para interconectar redes en lugar de computadores. (CNMC blog, 2010)

2.2.1.2 Redes De Agregación y Troncales: Para garantizar la calidad del servicio, es necesario concentrar el tráfico y minimizar el transporte de datos por redes muy complejas y heterogéneas. Esta uniformización es gracias a las redes de agregación, interconectadas a través de una red troncal que permiten el intercambio de datos entre ellas. (CNMC blog, 2010)

Tipos de Redes de agregación: La red de agregación representa el tramo en el que convergen los tráficos de diferentes usuarios y son utilizadas para disminuir el número de enlaces hacia un sólo protocolo de red y cuya capacidad es inferior a la suma de las capacidades de acceso. Los operadores emplean fundamentalmente dos sistemas de conversión de señalización entre redes con diferente transporte: agregación ATM y su versión mejorada, agregación IP sobre Ethernet. (CNMC blog, 2010)

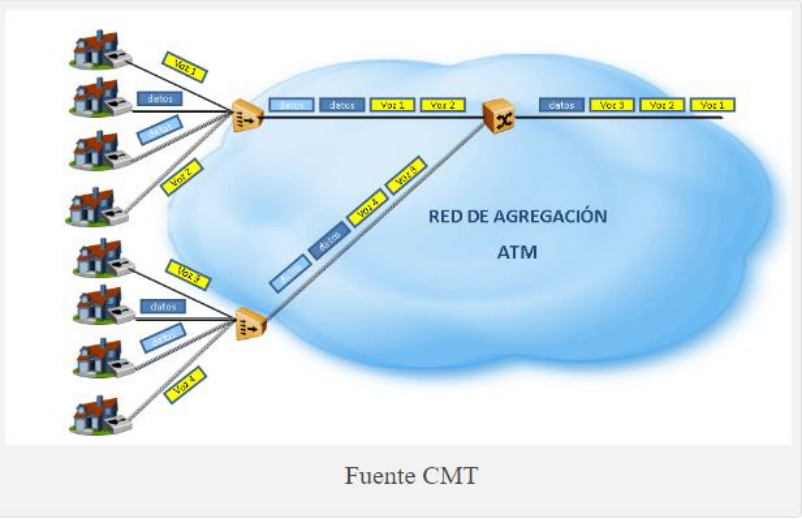
Redes ATM: Las redes ATM se crearon ante la creciente demanda de servicios diferenciados (voz, acceso a Internet, servicios de empresa etc..,) por parte de los usuarios y su utilización conllevó una serie de ventajas:

- Es un sistema de transmisión que optimiza el uso de los medios de alta velocidad.
- Interactúa con los sistemas existentes sin reducción de su efectividad.
- Asegura la entrega precisa y predecible.
- Permite que se asigne el mayor número de funciones posibles al hardware reduciendo así las asignadas al software, aumentando de esta forma la velocidad.

Actualmente, las redes ATM se utilizan para dar soporte a velocidades moderadas, como es el caso del ADSL, y progresivamente están siendo sustituidas por otras tecnologías como son las redes Ethernet basadas en

tramas de datos. Por el contrario, como podéis comprobar en el siguiente gráfico, en las redes ATM la información se transmite en forma de paquetes o celdas de longitud constante y que pueden ser conmutadas individualmente. (CNMC blog, 2010)

Figura 2: Redes ATM



Fuente CMT

Fuente: CNMC blog, 2010.

Red de agregación Carrier Ethernet

Las líneas Ethernet son las más utilizadas para dar servicios avanzados de banda ancha a empresas. El uso de la tecnología Ethernet en el despliegue de redes de área local (LAN) marcó un salto cualitativo respecto a las limitaciones presentes en tecnologías más tradicionales, y su utilización conllevó una serie de mejoras:

Equipamiento económico: Las líneas Ethernet implican un coste más bajo por Mbps y altas velocidades de transferencia, que se han ido incrementado progresivamente de 10 Mb/s a 10 Gb/s (Gigabit Ethernet).

Infraestructura convergente: Permiten ofrecer a los usuarios diferentes servicios empaquetados de banda ancha: Triple play, agregación de tráfico de redes móviles (2G, 3G, HSDPA,) y servicios de conectividad Ethernet.

El Metro Ethernet Forum (MEF) define esta evolución de las redes de agregación IP como Carrier-Ethernet, que se distingue del Ethernet de redes de área local (LAN) por los siguientes 5 atributos:

Escalabilidad: Los proveedores de servicio necesitan que sus redes sean escalables y proporcionen una amplia cobertura a sus usuarios.

Protección: Una de las metas de Ethernet es alcanzar los mismos niveles de rendimiento que han caracterizado a tecnologías precedentes.

Calidad del servicio superior: Permiten que los usuarios puedan disfrutar de niveles de servicio diferenciados, según los requerimientos de cada aplicación.

Gestión de servicio: Posibilitan que la red pueda configurarse de forma rápida para soportar nuevos servicios.

Soporte TDM: Facilitan la migración progresiva de las redes TDM a las Ethernet.

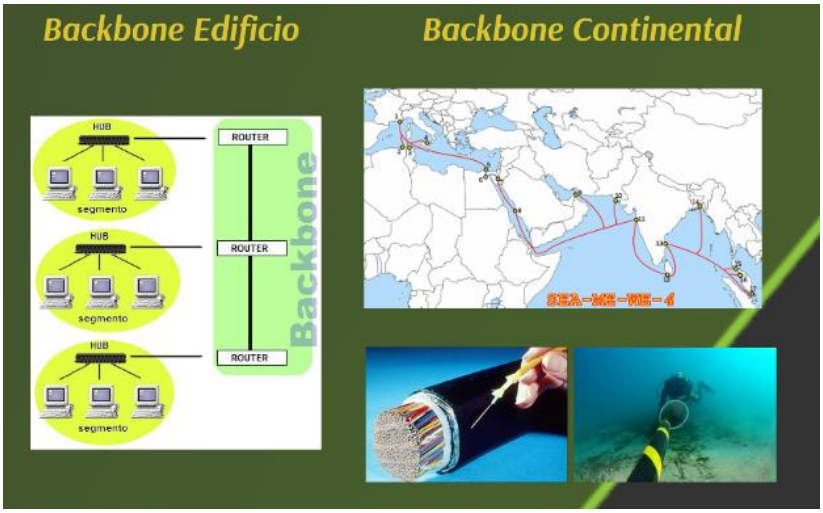
Estas redes soportan dos tipos de servicios de conexión: 1) punto a punto (Líneas Privadas Ethernet, Líneas privadas virtuales y acceso Ethernet a Internet) y 2) Multipunto a multipunto (Redes privadas virtuales, Servicios de LAN transparentes, IPTV y redes multicast).

2.2.1.3 Tipos de Redes troncales

La red troncal o backbone, que se despliega con fibra óptica al igual que las redes que agrega, es el tramo correspondiente al núcleo de la red y constituye un recurso asociado a la propia red de acceso. El mercado de líneas alquiladas troncales está liberalizado, exceptuando las rutas submarinas en las

que no había sistemas alternativos al cable submarino de Telefónica. Para más información, podéis consultar la presentación sobre el mercado de líneas alquiladas. (CNMC blog, 2010)

Figura 3: Tipos de redes troncales



Fuente: CNMC blog, 2010.

2.2.1.4 El camino hacia la convergencia de niveles: IP sobre ATM

A mediados de los 90 IP fue ganando terreno como protocolo de red a otras arquitecturas en uso (SNA, IPX, AppleTalk, OSI...). Por otro lado, hay que recordar que los backbones IP que los proveedores de servicio (NSP) habían empezado a desplegar en esos años estaban construidos a base de routers conectados por líneas dedicadas T1/E1 y T3/E3. El crecimiento explosivo de la Internet había generado un déficit de ancho de banda en aquel esquema de enlaces individuales. La respuesta de los NSPs fue el incremento del número de enlaces y de la capacidad de los mismos. Del mismo modo, los NSPs se plantearon la necesidad de aprovechar mejor los recursos de red existentes, sobre todo la utilización eficaz del ancho de banda de todos los enlaces. Con los protocolos habituales de encaminamiento (basados en métricas del menor

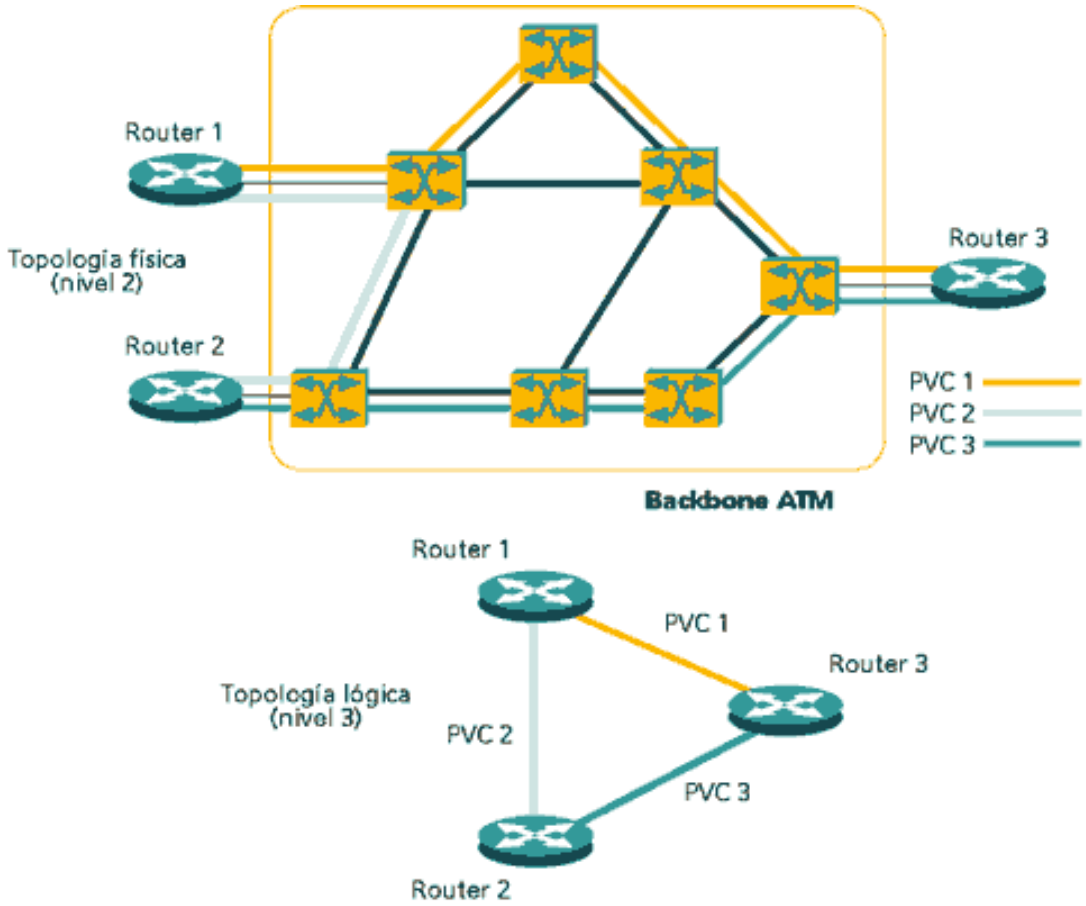
número de saltos), ese aprovechamiento del ancho de banda global no resultaba efectivo. Había que idear otras alternativas de ingeniería de tráfico.

Como consecuencia, se impulsaron los esfuerzos para poder aumentar el rendimiento de los routers tradicionales. Estos esfuerzos trataban de combinar, de diversas maneras, la eficacia y la rentabilidad de los conmutadores ATM con las capacidades de control de los routers IP. A favor de integrar los niveles 2 y 3 estaba el hecho de las infraestructuras de redes ATM que estaban desplegando los operadores de telecomunicación. Estas redes ofrecían entonces (1995-97) una buena solución a los problemas de crecimiento de los NSPs. Por un lado, proporcionaba mayores velocidades (155 Mpbs) y, por otro, las características de respuesta determinísticas de los circuitos virtuales ATM posibilitaban la implementación de soluciones de ingeniería de tráfico. El modelo de red "IP sobre ATM" (IP/ATM) pronto ganó adeptos entre la comunidad de NSPs, a la vez que facilitó la entrada de los operadores telefónicos en la provisión de servicios IP y de conexión a la Internet al por mayor. (CNMC blog, 2010)

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

representa un ejemplo en el que se puede comparar la diferencia entre la topología física de una red ATM con la de la topología lógica IP superpuesta sobre la anterior. (CNMC blog, 2010)

Figura 4: Diferencia entre la topología física de una red ATM con la de la topología lógica IP



Fuente: CNMC blog, 2010.

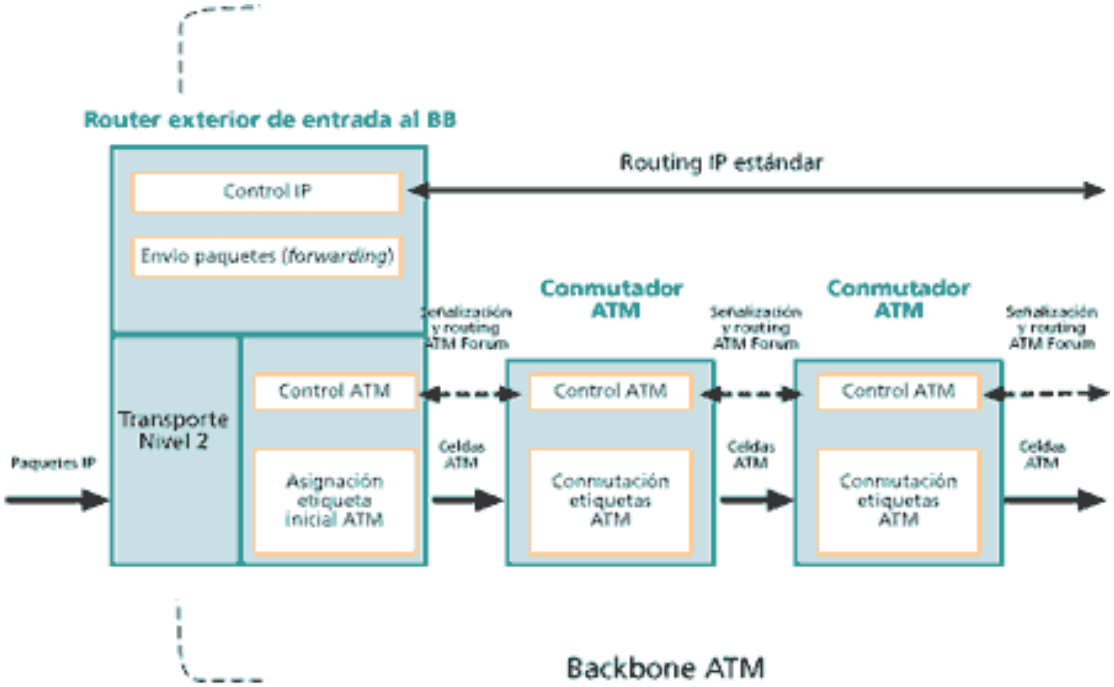
La base del modelo IP/ATM está en la funcionalidad proporcionada por el nivel ATM, es decir, los controles de software (señalización y routing) y el envío de las celdas por hardware (conmutación). En realidad, los PVCs se establecen a base de intercambiar etiquetas en cada conmutador de la red, de modo que la asociación de etiquetas entre todos los elementos ATM determina los corres-pondientes PVCs. (Más adelante se verá que el intercambio de

etiquetas es uno de los componentes fundamentales en la arquitectura MPLS). Las etiquetas tienen solamente significado local en los conmutadores y son la base de la rapidez en la conmutación de celdas. La potencia de esta solución de topologías superpuestas está en la infraestructura ATM del backbone; el papel de los routers IP queda relegado a la periferia, que, a mitad de los 90, tenían una calidad cuestionable, al estar basados en funcionamiento por software. En la figura se representa el modelo IP/ATM con la separación de funciones entre lo que es routing IP en el nivel 3 (control y envío de paquetes) y lo que es conmutación en el nivel 2 (control/señalización y envío de celdas). Aunque se trata de una misma infraestructura física, en realidad existen dos redes separadas, con diferentes tecnologías, con diferente funcionamiento y, lo que quizás es más sorprendente, concebidas para dos finalidades totalmente distintas. (García, 2006)

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

mallada. El "punto de encuentro" entre la red IP y la ATM está en el acoplamiento de los subinterfaces en los routers con los PVCs, a través de los cuales se intercambian los routers la información de encaminamiento correspondiente al protocolo interno IGP. Lo habitual es que, entre cada par de routers, haya un PVC principal y otro de respaldo, que entra automáticamente en funcionamiento cuando falla el principal. (García, 2006)

Figura 5: Modelo IP/ATM



Fuente: Barbera, J, 2000.

Sin embargo, el modelo IP/ATM tiene también sus inconvenientes: hay que gestionar dos redes diferentes, una infraestructura ATM y una red lógica IP superpuesta, lo que supone a los proveedores de servicio unos mayores costes de gestión global de sus redes. Existe, además, lo que se llama la "tasa impuesta por la celda", un overhead aproximado del 20% que causa el transporte de datagramas IP sobre las celdas ATM y que reduce en ese mismo

porcentaje el ancho de banda disponible. Por otro lado, la solución IP/ATM presenta los típicos problemas de crecimiento exponencial n x (n-1) al aumentar el número de nodos IP sobre una topología completamente mallada. Piénsese, p. ej., en una red con 5 routers externos con una topología virtual totalmente mallada sobre una red ATM. Son necesarios 5 x 4 =20 PVCs (uno en cada sentido de transmisión). Si se añade un sexto router se necesitan 10 PVCs más para mantener la misma estructura (6 x 5=30). Una pega adicional del crecimiento exponencial de rutas es el mayor esfuerzo que tiene que hacer el correspondiente protocolo IGP. (García, 2006)

Como conclusión, podemos decir que el modelo IP/ATM, si bien presenta ventajas evidentes en la integración de los niveles 2 y 3, lo hace de modo discontinuo, a base de mantener dos redes separadas. El MPLS, tal como se verá en las secciones siguientes, logra esa integración de niveles sin discontinuidades. (García, 2006)

Un paso más en la convergencia hacia IP: conmutación IP

La convergencia continuada hacia IP de todas las aplicaciones existentes, junto a los problemas de rendimiento derivados de la solución IP/ATM, llevaron posteriormente (1997-98) a que varios fabricantes desarrollasen técnicas para realizar la integración de niveles de forma efectiva, sin las discontinuidades señalas anteriormente. Esas técnicas se conocieron como "conmutación IP" (IP switching) o "conmutación multinivel" (multilayer switching). Una serie de tecnologías privadas -entre las que merecen citarse: IP Switching de Ipsilon Networks, Tag Switching de Cisco, Aggregate Route-Base IP Switching (ARIS) de IBM, IP Navigator de Cascade/Ascend/Lucent y Cell

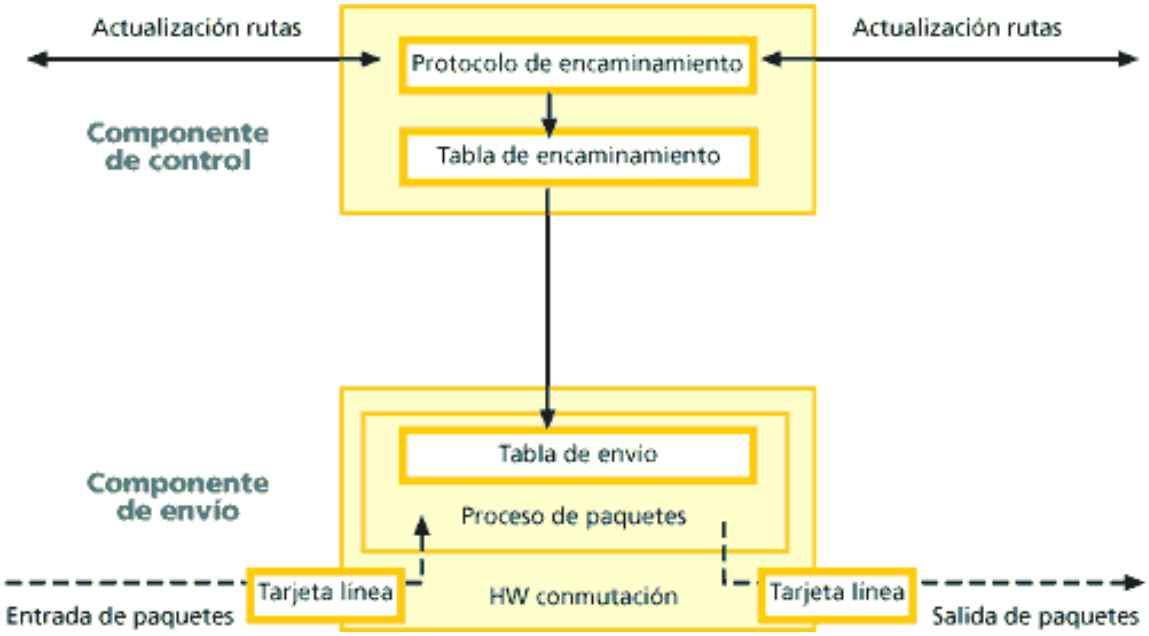
Switching Router (CSR) de Toshiba-condujeron finalmente a la adopción del actual estándar MPLS del IETF. El problema que presentaban tales soluciones era la falta de interoperatividad, ya que usaban diferentes tecnologías privadas para combinar la conmutación de nivel 2 con el encaminamiento IP (nivel 3). Se resume a continuación los fundamentos de esas soluciones integradoras, ya que permitirá luego comprender mejor la esencia de la solución MPLS.

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

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

En la figura se representa la separación funcional de esas dos componentes, una de control y la otra de envío. La componente de control utiliza los protocolos estándar de encaminamiento (OSPF, IS-IS y BGP-4) para el intercambio de información con los otros routers para la construcción y el mantenimiento de las tablas de encaminamiento. Al llegar los paquetes, la componente de envío busca en la tabla de envío, que mantiene la componente de control, para tomar la decisión de encaminamiento para cada paquete. En concreto, la componente de envío examina la información de la cabecera del paquete, busca en la tabla de envío la entrada correspondiente y dirige el paquete desde el interfaz de entrada al de salida a través del correspondiente hardware de conmutación. (García, 2006)

Figura 6: Decisión de encaminamiento



Fuente: Barbera, J, 2000.

Al separar la componente de control (encaminamiento) de la componente de envío, cada una de ellas se puede implementar y modificar independientemente. El único requisito es que la componente de encaminamiento mantenga la comunicación con la de envío mediante la tabla de envío de paquetes y actualice la información. El mecanismo de envío se implementa mediante el intercambio de etiquetas, similar a lo visto para ATM. La diferencia está en que ahora lo que se envía por el interfaz físico de salida son paquetes "etiquetados". De este modo, se está integrando realmente en el mismo sistema las funciones de conmutación y de encaminamiento.

En cuanto a la etiqueta que marca cada paquete, decir que es un campo de unos pocos bits, de longitud fija, que se añade a la cabecera del mismo y

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

El algoritmo de intercambio de etiquetas permite así la creación de "caminos virtuales" conocidos como LSP (Label-Switched Paths), funcionalmente equivalentes a los PVCs de ATM y Frame Relay. En el fondo, lo que hace es imponer una conectividad entre extremos a una red no conectiva por naturaleza, como son las redes IP, pero todo ello sin perder la visibilidad del nivel de red (de aquí los nombres de conmutación IP o conmutación multinivel). Esta es la diferencia básica con el modelo IP/ATM. Al hablar de MPLS con más detalle se entenderán mejor estas peculiaridades. (García, 2006)

2.2.1.5 IPVPN ó RPV:

Es un Servicio de Red Privada Virtual RPV o IP (IP-VPN) que permite interconectar todo tipo de sedes entre sí de manera sencilla, eficiente y segura. Las siglas **MPLS** (Multi Protocol Label Switching) es una tecnología de red desarrollada para llevar la velocidad de conmutación de nivel2 a redes de nivel3. Se utiliza una topología mallada (todos con todos), aunque se pueden

definir topologías parcialmente malladas o en estrella. Las sedes de la IP-VPN se conectan directamente a la red de fibra según las distintas opciones de acceso disponibles en cada ubicación. Con MPLS, el análisis detallado y el encabezado de Capa 3 se realiza sólo una vez, en el borde del router, que se encuentra en cada borde de la red. Sólo la etiqueta de longitud fija del paquete se examina para enviar el paquete en su camino. Al otro extremo de la red, un router de borde del cliente intercambia la etiqueta por el encabezado apropiado vinculado a esa etiqueta. Un resultado clave es que las decisiones pueden lograrse a través de una sola tabla de etiqueta de longitud fija. Esto permite a MPLS habilitar routers y los conmutadores para tomar decisiones de varias direcciones de destino, la tecnología MPLS también crea ventajas de QoS para clientes. MPLS encapsula y asigna etiquetas a IP y paquetes de acuerdo a los ID de VPN y CoS preestablecido.

Los enrutadores de red IP usan las etiquetas de paquetes para cambiar paquetes basados en la prioridad asignada en la etiqueta. Por conmutación de paquetes de acuerdo con la prioridad asignada,

Los transportistas son capaces de crear un conjunto de rutas predefinidas diferentes clases de tráfico para garantizar una ingeniería de tráfico, resultando en ventajas de QoS para clientes finales. Aprovechando los beneficios de MPLS, Global IP VPN, Ofrece tres clases de servicio (CoS) para asegurar una QoS diferenciada basada en las necesidades únicas de diferentes aplicaciones de red. Estas opciones de servicio incluyen Multimedia (para Voz o Video sobre IP), Premium (Para aplicaciones de datos sensibles al tiempo) y Standard para aplicaciones orientadas al rendimiento, como archivos transferencias y correo

electrónico). La QoS también está respaldada por la un Programa de Garantía, que proporciona a todo el mundo. (Cisco System, 2001)

2.2.1.6 MPLS

La convergencia real: MPLS

Ya se dijo anteriormente que el problema principal que presentaban las diversas soluciones de conmutación multinivel era la falta de interoperatividad entre productos privados de diferentes fabricantes. Además de ello, la mayoría de esas soluciones necesitaban ATM como transporte, pues no podían operar sobre infraestructuras de transmisión mixtas (Frame Relay, PPP, SONET/SDH y LANs). Se quería obtener un estándar que pudiera funcionar sobre cualquier tecnología de transporte de datos en el nivel de enlace. De aquí que el Grupo de Trabajo de MPLS que se estableció en el IETF en 1977 se propuso como objetivo la adopción de un estándar unificado e interoperativo. (García, 2006)

Ideas preconcebidas sobre MPLS

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

IETF. Los objetivos establecidos por ese grupo en la elaboración del estándar eran:

- MPLS debía funcionar sobre cualquier tecnología de transporte, no sólo ATM
- MPLS debía soportar el envío de paquetes tanto unicast como multicast
- MPLS debía ser compatible con el Modelo de Servicios Integrados del IETF, incluyendo el protocolo RSVP
- MPLS debía permitir el crecimiento constante de la Internet
- MPLS debía ser compatible con los procedimientos de operación, administración y mantenimiento de las actuales redes IP

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

- El filtrado de paquetes en los cortafuegos (FW) de acceso a las LAN corporativas y en los límites de las redes de los NSPs es un requisito fundamental para poder gestionar la red y los servicios con las necesarias garantías de seguridad. Para ello se requiere examinar la información de la cabecera de los paquetes, lo que impide prescindir del uso del nivel 3 en ese tipo de aplicaciones.
- No es probable que los sistemas finales (hosts) implementen MPLS. Necesitan enviar los paquetes a un primer dispositivo de red (nivel 3) que pueda examinar la cabecera del paquete para tomar luego las correspondientes decisiones sobre su envío hasta su destino final. En

este primer salto se puede decidir enviarlo por routing convencional o asignar una etiqueta y enviarlo por un LSP.

- Las etiquetas MPLS tienen solamente significado local (es imposible mantener vínculos globales entre etiquetas y hosts en toda la Internet). Esto implica que en algún punto del camino algún dispositivo de nivel 3 debe examinar la cabecera del paquete para determinar con exactitud por dónde lo envía: por routing convencional o entregándolo a un LSR, que lo expedirá por un nuevo LSP.
- Del mismo modo, el último LSR de un LSP debe usar encaminamiento de nivel 3 para entregar el paquete al destino, una vez suprimida la etiqueta, como se verá seguidamente al describir la funcionalidad MPLS.

Descripción funcional del MPLS

La operación del MPLS se basa en las componentes funcionales de envío y control, aludidas anteriormente, y que actúan ligadas íntimamente entre sí. Empecemos por la primera. (García, 2006)

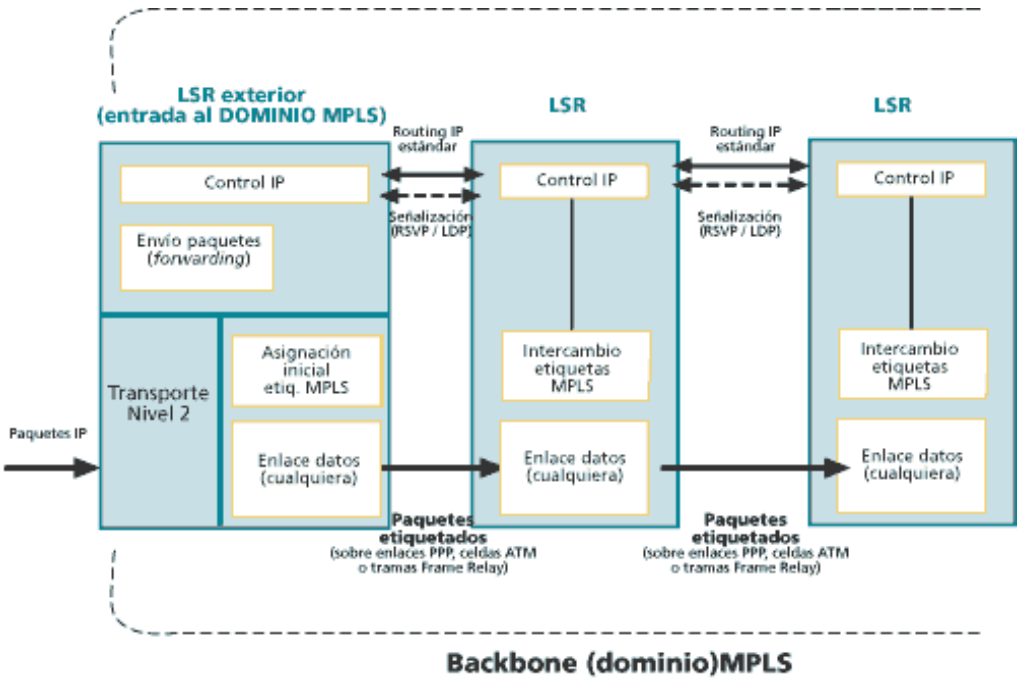
a) Funcionamiento del envío de paquetes en MPLS

La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP por la red. Los LSPs son simplex por naturaleza (se establecen para un sentido del tráfico en cada punto de entrada a la red); el tráfico dúplex requiere dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (Label-Swiching Router) a otro, a través del

dominio MPLS. Un LSR no es sino un router especializado en el envío de paquetes etiquetados por MPLS.

En la figura se puede ver la funcionalidad del MPLS. Compárese con los esquemas vistos antes en las figuras anteriores para observar las analogías y diferencias. Al igual que en las soluciones de conmutación multinivel, MPLS separa las dos componentes funcionales de control (routing) y de envío (forwarding). Del mismo modo, el envío se implementa mediante el intercambio de etiquetas en los LSPs. Sin embargo, MPLS no utiliza ninguno de los protocolos de señalización ni de encaminamiento definidos por el ATM Forum; en lugar de ello, en MPLS o bien se utiliza el protocolo RSVP o bien un nuevo estándar de señalización (el Label Distribution Protocol, LDP, del que se tratará más adelante). Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera. Si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. Ahora ya no hay que administrar dos arquitecturas diferentes a base de transformar las direcciones IP y las tablas de encaminamiento en las direcciones y el encaminamiento ATM: esto lo resuelve el procedimiento de intercambio de etiquetas MPLS. El papel de ATM queda restringido al mero transporte de datos a base de celdas. Para MPLS esto es indiferente, ya que puede utilizar otros transportes como Frame Relay, o directamente sobre líneas punto a punto.

Figura 7: Funcionalidad del MPLS

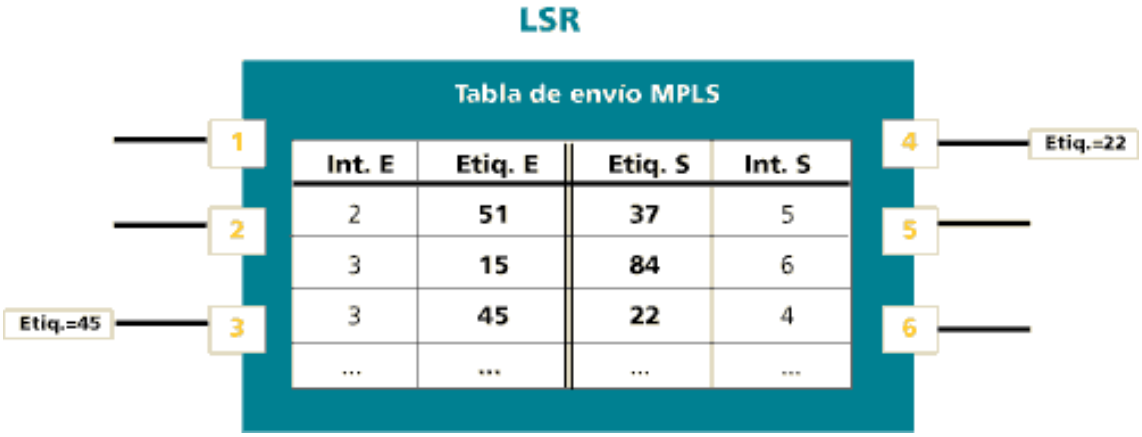


Fuente: Barbera, J, 2000.

Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR que interviene en un LSP se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs interiores del dominio MPLS. Un LSR es como un router que funciona a base de intercambiar etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control (recuérdese el esquema de la figura 3), según se verá más adelante. Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondiente a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por ese interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de

entrada en el de cola). En la figura 5 se ilustra un ejemplo del funcionamiento de un LSR del núcleo MPLS. A un paquete que llega al LSR por el interfaz 3 de entrada con la etiqueta 45 el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

Tabla 1: Tabla de envio MPLS

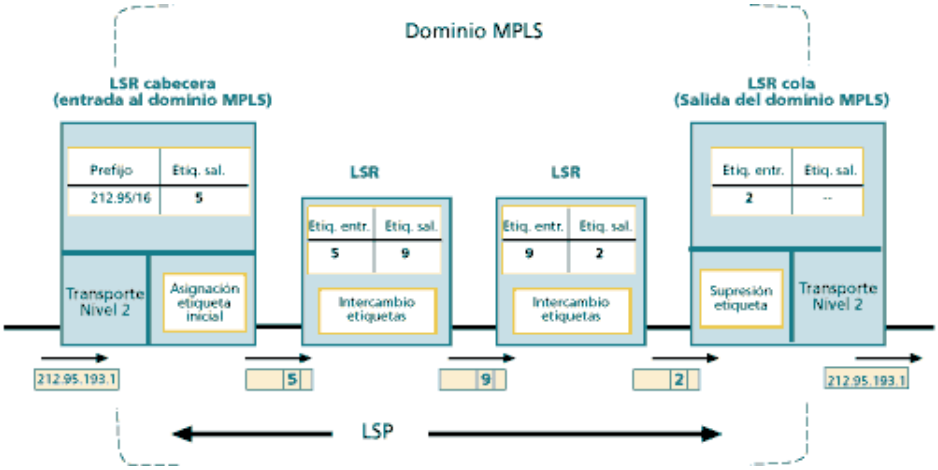


Fuente: Barbera, J, 2000.

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la figura 6 el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP. Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio de etiquetas. Al llegar el paquete al LSR de cola (salida), ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de

conmutación de etiquetas quita ésta y envía el paquete por routing convencional.

Figura 8: Dominio MPLS

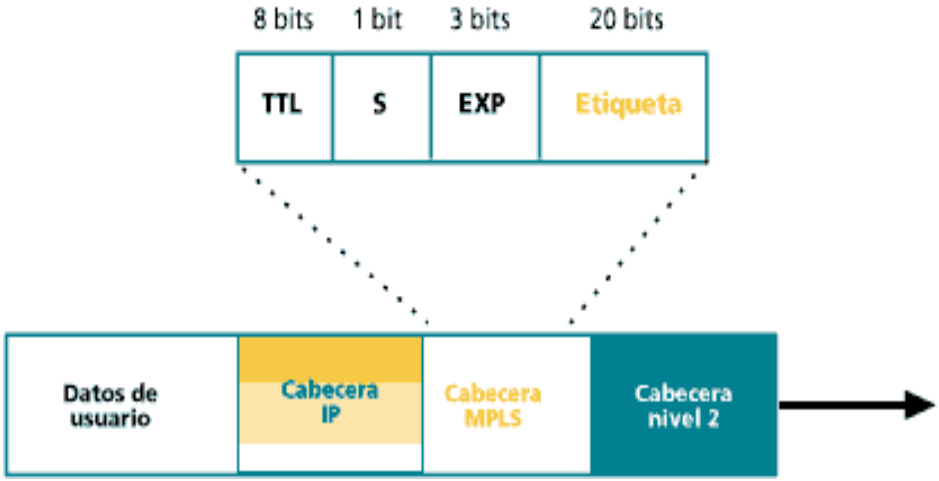


Fuente: Barbera, J, 2000.

Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no "mira" sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los caminos LSP. Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3. Según las especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. Por ello, si el protocolo de transporte de datos contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de Frame Relay), se utilizan esos campos nativos para las etiquetas. Sin embargo, si la tecnología de nivel 2 empleada no soporta un campo para etiquetas (p. ej. enlaces PPP o LAN), entonces se emplea una cabecera genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete (nivel 3).

En la figura se representa el esquema de los campos de la cabecera genérica MPLS y su relación con las cabeceras de los otros niveles. Según se muestra en la figura, los 32 bits de la cabecera MPLS se reparten en: 20 bits para la etiqueta MPLS, 3 bits para identificar la clase de servicio en el campo EXP (experimental, anteriormente llamdo CoS), 1 bit de stack para poder apilar etiquetas de forma jerárquica (S) y 8 bits para indicar el TTL (time-to-live) que sustenta la funcionalidad estándar TTL de las redes IP. De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.

Figura 9: Esquema de los campos de la cabecera genérica MPLS



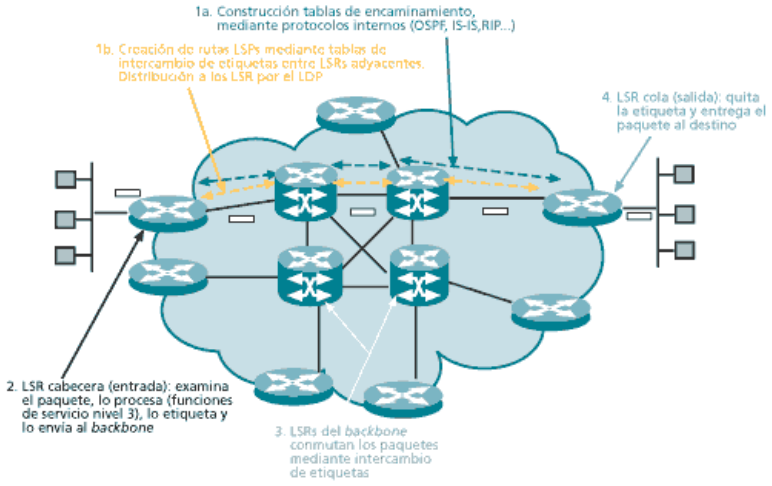
Fuente: Barbera, J, 2000.

b) Funcionamiento global MPLS

Una vez vistos todos los componentes funcionales, el esquema global de funcionamiento es el que se muestra en la figura, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. Es importante destacar que en el borde de la nube MPLS tenemos una red

convencional de routers IP. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de routers a una distancia de un sólo salto. Funcionalmente es como si estuvieran unidos todos en una topología mallada (directamente o por PVCs ATM). Ahora, esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de routers). La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP. Todo ello abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario, tal como se explica en la sección siguiente.

Figura 10: Esquema global de funcionamiento



Fuente: Barbera, J, 2000.

c) Control de la información en MPLS

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

- Cómo se generan las tablas de envío que establecen los LSPs
- Cómo se distribuye la información sobre las etiquetas a los LSRs

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

El segundo aspecto se refiere a la información de "señalización" (las comillas se ponen por el impacto que puede suponer este término para los puristas del mundo IP, de naturaleza no conectiva). Pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas; de hecho, se están estandarizando algunos existentes con las correspondientes extensiones; unos de ellos es el protocolo RSVP del Modelo

de Servicios Integrados del IETF (recuérdese que ése era uno de los requisitos). Pero, además, en el IETF se están definiendo otros nuevos, específicos para la distribución de etiquetas, cual es el caso del Label Distribution Protocol (LDP). Consúltese las referencias correspondientes del IETF.

d) Aplicaciones de MPLS

Las principales aplicaciones que hoy en día tiene MPLS son:

Ingeniería de tráfico

Diferenciación de niveles de servicio mediante clases (CoS)

Servicio de redes privadas virtuales (VPN)

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

2.2.1.7 Ingeniería de tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. A comienzos de los 90 los esquemas para adaptar de forma efectiva los flujos de tráfico a la topología física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos

seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos). En el esquema de la figura 9 se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

El camino más corto entre A y B según la métrica normal IGP es el que tiene sólo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes hagan aconsejable la utilización del camino alternativo indicado con un salto más. MPLS es una herramienta efectiva para esta aplicación en grandes backbones, ya que:

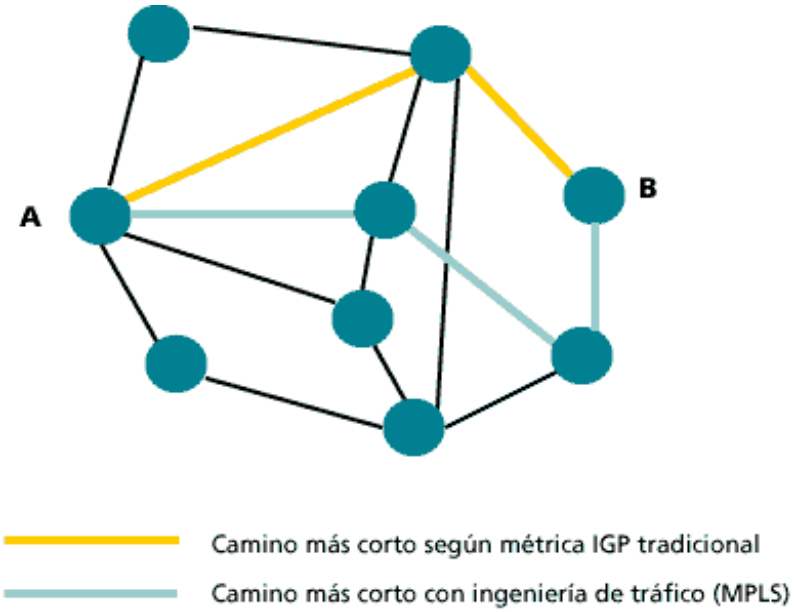
Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.

Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.

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

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

Figura 11: Encaminamiento restringido



Fuente: Barbera, J, 2000.

a) Clases de servicio (CoS)

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

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De es te modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP

Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. P. ej., un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort, tres niveles de servicio, primera, preferente y turista, que, lógicamente, tendrán distintos precios.

b) ELEMENTOS DE UNA RED MPLS

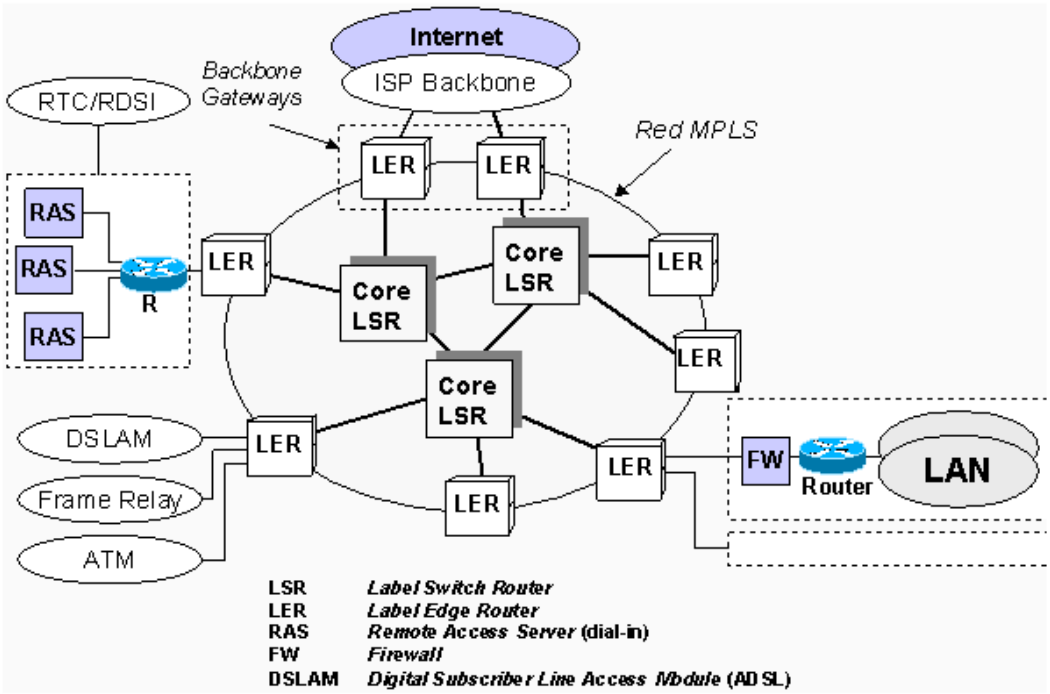
En MPLS un concepto muy importante es el de LSP (Label Switch Path), que es un camino de tráfico específico a través de la red MPLS, el cual se crea utilizando los LDPs (Label Distribution Protocols), tales como RSVP-TE (ReSerVation Protocol Traffic Engineering) o CR-LDP (Constraint-based Routing Label Distribution Protocol); siendo el primero el más común. El LDP posibilita a los nodos MPLS descubrirse y establecer comunicación entre sí con el propósito de informarse del valor y significado de las etiquetas que serán utilizadas en sus enlaces contiguos. Es decir, mediante el LDP se establecerá un camino a través de la red MPLS y se reservarán los recursos físicos necesarios para satisfacer los requerimientos del servicio previamente definidos para el camino de datos.

Una red MPLS está compuesta por dos tipos principales de nodos, los LER (Label Edge Routers) y los LSR (Label Switching Routers). Los dos son físicamente el mismo dispositivo, un router o switch de red troncal que incorpora el software MPLS; siendo su administrador, el que lo configura para uno u otro modo de trabajo. Los nodos MPLS al igual que los "routers" IP normales, intercambian información sobre la topología de la red mediante los protocolos, tales como OSPF (Open Shortest Path First), RIP (Routing Information Protocol) y BGP (Border Gateway Protocol), a partir de los cuales construyen tablas de enrutamiento basándose principalmente en la alcanzabilidad a las redes IP destinatarias. Teniendo en cuenta dichas tablas de enrutamiento, que indican la dirección IP del siguiente salto al que le será enviado el paquete para que pueda alcanzar su destino final, se establecerán las etiquetas MPLS; y por lo tanto, los LSP que seguirán los paquetes. No obstante, también pueden establecerse LSP que no se correspondan con el camino mínimo calculado por el protocolo de enrutamiento.

Los LERs están ubicados en el borde de la red MPLS para desempeñar las funciones tradicionales de enrutamiento y proporcionar conectividad a sus usuarios, generalmente routers IP convencionales. El LER analiza y clasifica el paquete IP entrante considerando hasta el nivel 3, es decir, considerando la dirección IP de destino y la QoS demandada; añadiendo la etiqueta MPLS que identifica en qué LSP está el paquete. Es decir, el LER en vez de decidir el siguiente salto, como haría un "router" IP normal, decide el camino entero a lo largo de la red que el paquete debe seguir. Una vez asignada la cabecera MPLS, el LER enviará el paquete a un LSR. Los LSR están ubicados en el núcleo de la red MPLS para efectuar rutas de alto rendimiento basado en la

conmutación por etiqueta, considerando únicamente hasta el nivel 2. Cuando le llega un paquete a una interfaz del LSR, éste lee el valor de la etiqueta de entrada de la cabecera MPLS, busca en la tabla de conmutación la etiqueta e interfaz de salida, y reenvía el paquete por el camino predefinido escribiendo la nueva cabecera MPLS. Si un LSR detecta que debe enviar un paquete a un LER, extrae la cabecera MPLS; como el último LER no conmuta el paquete, se reducen así cabeceras innecesarias.

Figura 12: Elementos de una red típica.



Fuente: Huedrobo, J. 2002

c) IMPLEMENTACIONES DE MPLS

MPLS como una solución IP sobre Ethernet, IP sobre ATM, e IP sobre Frame Relay. No se contempla la aplicación de MPLS a las redes ópticas de

próxima generación, conocida como GMPLS (Generalized MPLS), por encontrarse aún en proceso de estudio y estandarización por parte del IETF. GMPLS es una extensión natural de MPLS para ampliar el uso de MPLS como un mecanismo de control y provisión, no únicamente de caminos en dispositivos basados en paquetes, sino también de caminos en dispositivos no basados en paquetes; como los conmutadores ópticos de señales multiplexadas por división en longitud de onda, los conmutadores de fibras ópticas, y los conmutadores de señales digitales multiplexadas por división en el tiempo. Es decir, MPLS busca una integración total en la parte de control de las redes de conmutación de paquetes IP y las redes ópticas SONET/SDH y DWDM; dando lugar a las redes ópticas inteligentes de próxima generación, cuya evolución final será la integración de IP directamente sobre DWDM utilizando algún mecanismo de encapsulamiento como los “digital wrappers”.

La implementación de MPLS como una solución IP sobre Ethernet, Fast Ethernet o Gigabit Ethernet, es la conocida como IP pura. Puesto que IPv4 es un protocolo diseñado mucho antes que MPLS, en este caso, la etiqueta MPLS está ubicada después de la cabecera de nivel 2 y antes de la cabecera IP. Los LSR saben como conmutar utilizando la etiqueta MPLS en vez de utilizar la cabecera IP. El funcionamiento de IPv4 ha sido totalmente satisfactorio, no obstante, el sorprendente crecimiento de Internet evidenció importantes carencias, como: la escasez de direcciones IP, la imposibilidad de transmitir aplicaciones en tiempo real y los escasos mecanismos de seguridad. Estas limitaciones propiciaron el desarrollo de la siguiente generación del protocolo Internet o IPv6, definido en la RFC 1883. La versión IPv6 puede ser instalada como una actualización del software en los dispositivos de red de Internet e

interoperar con la versión actual IPv4, produciéndose esta migración progresivamente durante los próximos años. En este caso, la etiqueta MPLS forma parte de la propia cabecera IPv6, estando su uso descrito en la RFC 1809.

La implementación de MPLS como una solución IP sobre ATM también está muy extendida. Primeramente, indicar que, MPLS no fue desarrollado para reemplazar ATM, sino para complementarlo. De hecho, la aparición de "switches" ATM e IP con soporte de MPLS, ha integrado las ventajas de los routers IP y los switches ATM y ha supuesto una mejora de la relación precio/rendimiento de estos dispositivos. La diferencia principal entre MPLS y otras soluciones de IP sobre ATM, es que las conexiones MPLS se establecen utilizando LDP, y no por los protocolos de señalización ATM tradicionales, tales como PNNI (Private Network to Network Interface). Por otro lado, MPLS elimina la complejidad de hacer corresponder el direccionamiento IP y la información de encaminamiento directamente en las tablas de conmutación de ATM, puesto que LDP entiende y utiliza direcciones IP y los protocolos de encaminamiento utilizados en las redes MPLS son los mismos que los utilizados en las redes IP. En este caso, descrito en la RFC 3035, la etiqueta es el valor del VPI/VCI (Virtual Path Identifier/Virtual Channel Identifier) de la cabecera de la celda ATM.

Finalmente, MPLS también se ha desarrollado como una solución IP sobre Frame Relay. En este caso, descrito en la RFC 3034, la etiqueta es el DLCI (Data Link Control Identifier) de la cabecera Frame Relay.

c) BENEFICIOS DE MPLS

La migración a IP está provocando profundos cambios en el sector de las telecomunicaciones y configura uno de los retos más importantes para los ISP, inmersos actualmente en un proceso de transformación de sus infraestructuras de cara a incorporar los beneficios de esta tecnología. MPLS nació con el fin de incorporar la velocidad de conmutación del nivel 2 al nivel 3; a través de la conmutación por etiqueta; pero actualmente esta ventaja no es percibida como el principal beneficio, ya que los gigarouters son capaces de realizar búsquedas de rutas en las tablas IP a suficiente velocidad como para soportar todo tipo de interfaces. Los beneficios que MPLS proporciona a las redes IP son: realizar ingeniería del tráfico o TE (Traffic Engineering), cursar tráfico con diferentes calidades de clases de servicio o CoS (Class of Service) o grados de calidad de servicio o QoS (Quality of Service), y crear redes privadas virtuales o VPN (Virtual Private Networks) basadas en IP.

La TE permite a los ISP mover parte del tráfico de datos, desde el camino más corto calculado por los protocolos de encaminamiento, a otros caminos físicos menos congestionados o menos susceptibles a sufrir fallos. Es decir, se refiere al proceso de seleccionar los caminos que seguirá el flujo de datos con el fin de balancear la carga de tráfico entre todos los enlaces, routers y switches en la red; de modo que ninguno de estos recursos se encuentre infrautilizado o sobrecargado. La TE, descrita en la RFC 2702, se ha convertido en la principal aplicación de MPLS debido al crecimiento impredecible en la demanda de recursos de red.

Mediante MPLS, los ISP pueden soportar servicios diferenciados o DiffServ, como viene recogido en la RFC 3270. El modelo DiffServ define varios

mecanismos para clasificar el tráfico en un pequeño número de CoS. Los usuarios de Internet demandan continuamente nuevas aplicaciones, teniendo los servicios actualmente soportados unos requerimientos de ancho de banda y de tolerancia a retrasos en la transmisión muy distintos y para satisfacer estas necesidades óptimamente, los ISP necesitan adoptar no sólo técnicas de ingeniería de tráfico, sino también de clasificación de dicho tráfico. De nuevo, MPLS ofrece a los ISP una gran flexibilidad en cuanto a los diferentes tipos de servicios que puede proporcionar a sus clientes.

Finalmente, MPLS ofrece también un mecanismo sencillo y flexible para crear VPN. Una VPN simula la operación de una WAN (Wide Area Network) privada sobre la Internet pública. Para ofrecer un servicio de VPN viable a sus clientes, un ISP debe solventar los problemas de seguridad de los datos y soportar el uso de direcciones IP privadas no únicas dentro de la VPN. Puesto que MPLS permite la creación de circuitos virtuales o túneles a lo largo de una red IP, es lógico que los ISP utilicen MPLS como una forma de aislar el tráfico. No obstante, MPLS no tiene en estos momentos ningún mecanismo para proteger la seguridad en las comunicaciones, por lo que el ISP deberá conseguirla mediante cortafuegos y algún protocolo de encriptación tipo IPsec. Existen varias alternativas para implementar VPNs mediante MPLS, pero la mayoría se basan en la RFC 2547.

La mayor parte de los "routers" y "switches" actuales destinados a redes troncales están preparados para utilizar MPLS, y muchos de los antiguos podrían soportarlo actualizando su software. No obstante, aunque varios ISP han realizado experiencias pilotos o han implantado MPLS en la parte troncal de sus redes, no se espera una introducción masiva hasta el 2003 o 2004,

cuando los fabricantes alcancen una compatibilidad total en sus equipos. Del mismo modo que ocurrió con la actualización de las infraestructuras X.25 y Frame Relay a ATM, la migración a MPLS como núcleo de las redes multiservicio con soporte de voz, vídeo y datos, se realizará de forma gradual durante varios años; máxime dada la crisis mundial del sector de las telecomunicaciones, que está repercutiendo muy negativamente en las inversiones de los operadores de red y fabricantes de equipos.

Tabla 2: Comparación ATM, IP, MPLS

Características/Backbone	Frame-Relay / ATM	IP	MPLS
Conmutación veloz de tramas	√	X	√
Total independencia entre redes de clientes (VPN en capa 2)	√	X	√
Transporte múltiple protocolo de capa 3	√	X	√
Priorización de Paquetes (QoS)	X	√	√
Facilidad en la creación de circuitos nuevos	X	√	√
Utilización óptima de troncales	X	√	√
Utilización óptima de ancho de banda en accesos	X	√	√
Fácil acceso a servicios en el proveedor (datacenter)	X	√	√
Elección de mejor ruta	X	X	√

Fuente: Acosta, H. 2016.

Arquitectura y terminología de MPLS VPN - IPVPN

En la arquitectura MPLS VPN, los router llevan información de enrutamiento del cliente proporcionar un enrutamiento óptimo para el tráfico al cliente para el tráfico entre sitios.

El modelo VPN basado en MPLS también permite a los clientes usar espacios de direcciones superpuestos, a diferencia del modelo peer-to-peer tradicional en el que el encaminamiento óptimo del tráfico de clientes obligó al

proveedor a asignar direcciones IP a cada uno de sus clientes (o al cliente implementar NAT) para evitar la superposición de espacios de direcciones.

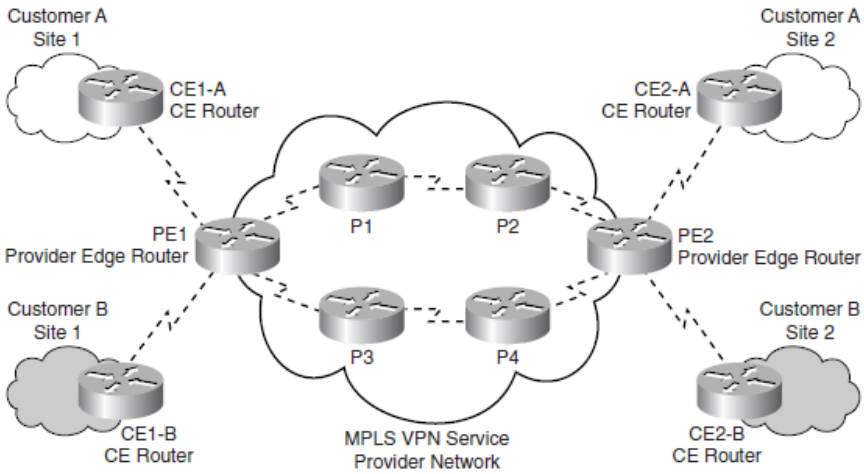
MPLS VPN es una implementación del modelo peer-to-peer; El backbone MPLS VPN y los sitios de clientes intercambian Capa 3 la información de enrutamiento del cliente y los datos se reenvían entre los sitios.

Estructura IP SP IP habilitada para MPLS.

El dominio MPLS VPN, al igual que la VPN tradicional, consiste en la red de clientes yred de proveedores. El modelo MPLS VPN es muy similar al modelo de enrutador P E dedicado en una implementación VPN peer-to-peer. Sin embargo, en lugar de implementar un enrutador PE dedicado por cliente, el tráfico del cliente está aislado en el mismo enrutador PE que proporciona conectividad, la red del proveedor de servicios para múltiples clientes.

Los componentes de una VPN MPLS se muestran a continuación en la Figura.

Figura 13: Componentes de una VPN MPLS



Fuente: Acosta, H. 2016.

Los principales componentes de la arquitectura MPLS VPN son:

Customer network: red del cliente, que es generalmente un dominio controlado por el cliente que consiste endispositivos o routers que abarcan múltiples sitios pertenecientes al cliente. En la figura, la red del cliente para el cliente A está formado por los enrutadores CE1-A Y CE2-A lo largo Con dispositivos en los sitios 1 y 2 del cliente A

CE routers, que son routers en la red del cliente que la interfaz con el servicio de la red de proveedores. En la Figura, los routers CE para un cliente son CE1-A y CE2-A, y los routers CE para cliente B son CE1-B y CE2-B.

Provider network, Que es el dominio controlado por el proveedor que consiste en proveedor de borde y de proveedores de routers de núcleo que conectan los sitios pertenecientes al cliente en una Infraestructura compartida. La red de proveedores controla el tráfico de enrutamiento entre sitios perteneciente a un cliente junto con el aislamiento tráfico de clientes. En la Figura, la red de proveedores consta de los routers PE1, PE2, P1, P2, P3, y P4.

PE routers, los cuales son los routers de la red de proveedores que se conectan a la interfaz o los routers de acceso de clientes en la red del cliente. PE1 y PE2 son el proveedor

routers de frontera en el dominio MPLS VPN para los clientes A y B en la Figura.

P routers, Que son routers en el núcleo de la red de proveedores que interactúan con

Ya sea otros routers principales del proveedor o enrutadores de borde del proveedor. Routers P1, P2, P3, y P4 son los routers de proveedores en la Figura.

MPLS VPN Modelo de enrutamiento

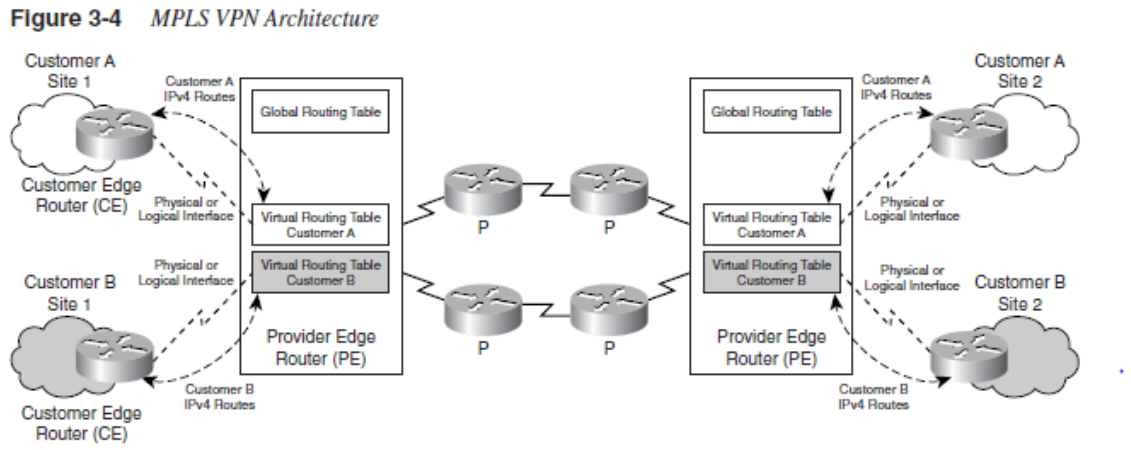
Una implementación MPLS VPN es muy similar a un modelo de peer-to-peer dedicado. Desde la perspectiva de un router CE, sólo las actualizaciones IPv4, así como los datos, son remitido al router PE. La CE router no necesita ninguna configuración específica para que pueda ser parte de un dominio MPLS VPN. El único requisito en el router CE es un protocolo de enrutamiento (o una ruta estática / default) que permite que el router pueda intercambiar informacion de enrutamiento IPv4 con el PE router conectado.

En la implementación MPLS VPN, el router PE realiza múltiples funciones. El PE en primer lugar, debe ser capaz de aislar el tráfico del cliente si hay más de uno conectado al router PE. Por lo tanto, a cada cliente se le asigna un enrutamiento independiente esta tabla es similar a un router dedicado de PE en la discusión inicial peer-to-peer. Enrutamiento a través de backbone SP se realiza utilizando un proceso de enrutamiento, en la tabla de enrutamiento global. Los routers Proporcionan conmutación de etiquetas entre los routers de borde del proveedor y desconocen las rutas VPN. CE

Los routers de la red del cliente no son conscientes de los routers P y, por tanto, de la topología de la red SP es transparente para el cliente. La Figura muestra el router del PE funcionalidad.

Los routers P sólo son responsables de la conmutación de etiquetas de los paquetes. No llevan rutas VPN y no participan en el enrutamiento MPLS VPN. Los routers PE intercambian rutas IPv4 con routers CE conectados utilizando contextos de protocolo de enrutamiento individuales. Para activar la red a un gran número de VPNs de clientes, BGP multiprotocolo está configurado entre PE.

Figura 14: Router del PE funcionalidad



Fuente: Acosta, H. 2016.

VRF: Virtual Routing and Forwarding Table

El Enrutamiento Virtual y Reenvío (VRF) es una tecnología incluida en routers de red IP (Internet Protocol) que permite a varias instancias de una tabla de enrutamiento existir en un router y trabajar simultáneamente. Esto aumenta la funcionalidad al permitir que las rutas de red sean segmentadas sin usar varios dispositivos. Dado que el tráfico es automáticamente segregados, VRF también aumenta la seguridad de la red y puede eliminar la necesidad de cifrado y autenticación. Proveedores de Servicios de Internet (ISP) a menudo toman ventaja del VRF para crear distintas redes privadas virtuales (VPNs) para los clientes, por lo que la tecnología es también conocida como VPN enrutamiento y reenvío.

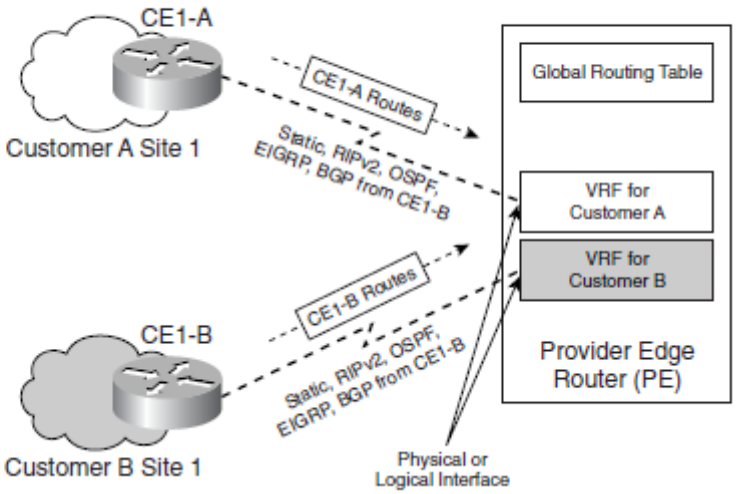
VRF actúa como un router lógico, pero mientras que un router lógico puede incluir muchas tablas de enrutamiento, una instancia VRF sólo utiliza una, además, VRF requiere una tabla de reenvío que designa el siguiente salto para cada paquete de datos, una lista de dispositivos que pueden ser llamados

al enviar el paquete, y un conjunto de normas y protocolos de enrutamiento que rigen la forma en que el paquete se reenvía. Estas tablas evitan el tráfico dado que están siendo reenviadas fuera de la ruta de un VRF específico y también mantienen fuera el tráfico que podría permanecer fuera de la ruta del VRF.

Como se muestra en la Figura, Cisco IOS soporta una variedad de protocolos de enrutamiento, así como los procesos de enrutamiento individuales (OSPF, EIGRP, etc.) por el router. Sin embargo, para algunos de enrutamiento protocolos, tales como RIP y BGP, iOS es compatible con una única instancia del protocolo de enrutamiento, por lo tanto, para poner en práctica por VRF de enrutamiento mediante estos protocolos que son completamente aislado, VRF de otros, que podrían utilizar los mismos protocolos de enrutamiento PE-CE, el concepto de fue desarrollado contexto de enrutamiento.

Figura 15: Implementacion e n Router PE

Figure 3-5 *VRF Implementation on PE Router*



Fuente: Acosta, H. 2016.

Los contextos de enrutamiento fueron diseñados para apoyar copias aisladas de la misma VPN PE-CE enrutamiento de protocolos. Estos contextos de enrutamiento se pueden implementar como procesos separados, como en el caso de OSPF, o como múltiples instancias del mismo protocolo de enrutamiento (en BGP, RIP, etc.). Si se utilizan varias instancias del mismo protocolo de enrutamiento, cada instancia tiene su propio conjunto de parámetros.

Tenga en cuenta que las interfaces VRF pueden ser lógico o físico, pero cada interfaz puede ser asignado a un solo VRF.

Route Distinguisher, Route Targets, MP-BGP, and Address Families

Distintivo de ruta, Metas de ruta, MP-BGP, y dirección de las familias. En el modelo de enrutamiento MPLS VPN, el enrutador PE proporciona aislamiento entre los clientes que utilizan VRFs. Sin embargo, esta información debe ser llevada entre los routers PE para habilitar los datos de transferencia entre los sitios del cliente vía el backbone de MPLS VPN. El enrutador PE debe ser capaz de implementar procesos que permiten la superposición de espacios de direcciones en redes de clientes. El enrutador PE también debe aprender estas rutas de clientes conectados y asi propagar esta información utilizando el backbone de proveedor compartido. Esto está hecho por la asociación de un identificador de rutas (RD) por tabla de enrutamiento virtual en un enrutador PE.

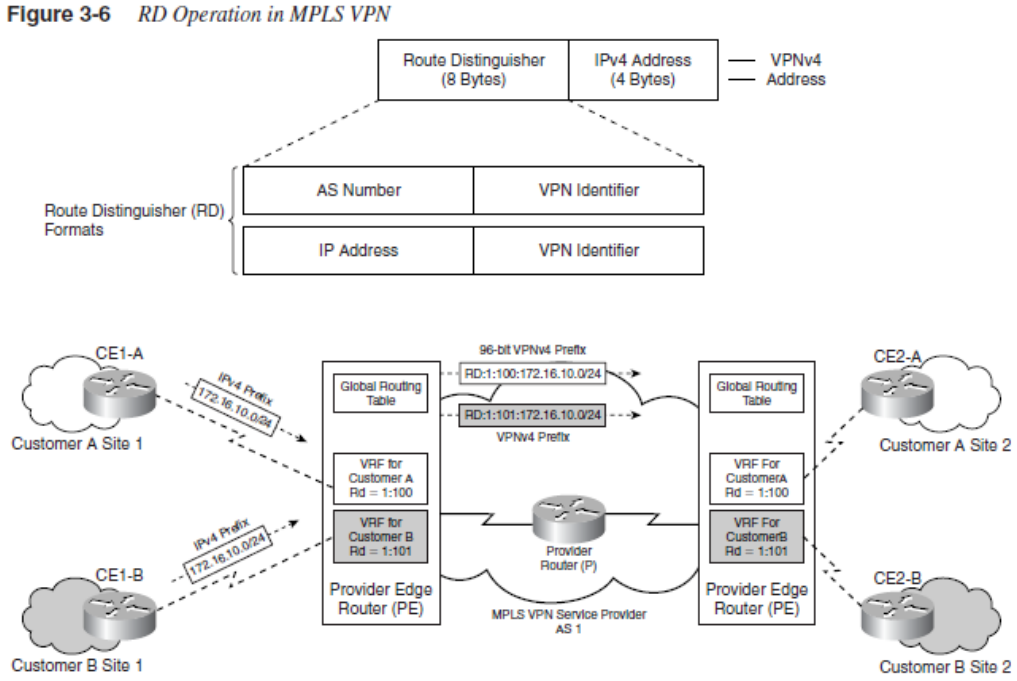
Un RD es un identificador único de 64 bits que se agrega al prefijo o ruta del cliente de 32 bits aprendido de un ranurador del CE, que le hace una dirección única de 96 bits que se puede transportar.

Entre los enrutadores PE en el dominio MPLS. Por lo tanto, un RD único se configura por VRF en el enrutador PE. La dirección resultante, que es el total de 96 bits (prefijo de cliente de 32 bits + 64 bits usa un dentificador único o RD), se denomina dirección VPN versión 4 (VPNv4).

Las direcciones VPNv4 se intercambian entre routers PE en la red del proveedor además las direcciones IPv4 (32 bits). El formato de un RD se muestra en la Figura. En figuras anteriores, RD puede ser de dos formatos. Si el proveedor no tiene un número BGP AS, se puede usar el formato de dirección IP y, si el proveedor tiene un número AS, el AS tiene formato de número se puede utilizar. La Figura también muestra el mismo prefijo IP, 172.16.10.0/24,

Recibida de dos clientes diferentes, se hace única por el prepending diversos valores de RD.

Figura 16: Operación en MPLS VPN



Fuente: Acosta, H. 2016.

El protocolo utilizado para el intercambio de estas rutas VPNv4 entre routers PE es multiprotocolo BGP (MP - BGP). BGP capaz de llevar VPNv4 (96-bit) prefijos, además de otros

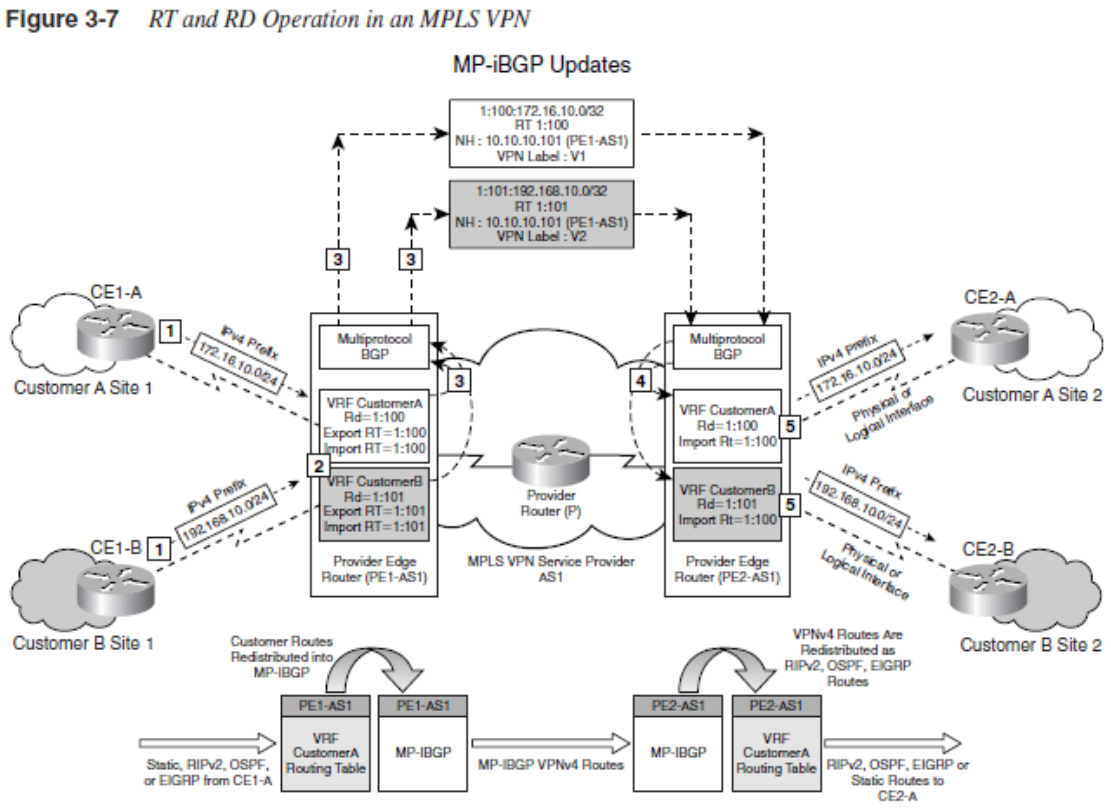
Familia de direcciones se llama MP-BGP. El requerimiento de IGP para implementar iBGP (BGP interno) aún se mantiene en el caso de una implementación MPLS VPN. Por lo tanto, el enrutador PE debe ejecutarse a un IGP que proporciona información NLRI para iBGP si ambos routers PE están en el mismo AS, Cisco actualmente soporta OSPFv2 e ISIS en la red de proveedores MPLS como IGP. MP-BGP también es responsable de la asignación de una etiqueta VPN. Reenvío de paquetes en una MPLS VPN mandatos que el router especificado como el siguiente salto en la actualización BGP entrante

Es el mismo enrutador que asigna la etiqueta VPN. La escalabilidad fue la principal razón de elección de BGP como el protocolo para llevar la información de enrutamiento del cliente. Además, BGP permite el uso de la dirección VPNv4 en un entorno de enrutador MPLS VPN que permite superponiendo rangos de direcciones con múltiples clientes.

Una sesión MP-BGP entre routers PE en un solo BGP AS se llama una sesión MP-iBGP y sigue reglas como en la implementación de iBGP con respecto a los atributos BGP. Si el VPN se extiende más allá de un único AS, VPNv4 rutas se intercambiarán entre AS en el AS ytilizando una sesión MP-eBGP.

Como la actualización se convierte en una actualización MP-BGP se muestra en la figura.

Figura 17: RT y RD operación en un MPLS VPN



Fuente: Acosta, H. 2016.

OSPF PE-CE Routing Protocol Overview, Configuration and Verification

OSPF PE-CE Protocolo de enrutamiento configuración y Verificación se ha desarrollado la compatibilidad con el protocolo de enrutamiento PE-CE de Open Short Path (OSPF)

Proveedores de servicios MPLS VPN a clientes que han implementado OSPF como Intra-sitio y, por lo tanto, el uso preferido de OSPF como el VPN inter-sitio

Protocolo de enrutamiento en un entorno MPLS VPN. Las próximas secciones le presentan a los problemas con la implementación de modelos de enrutamiento OSPF tradicionales en MPLS VPN

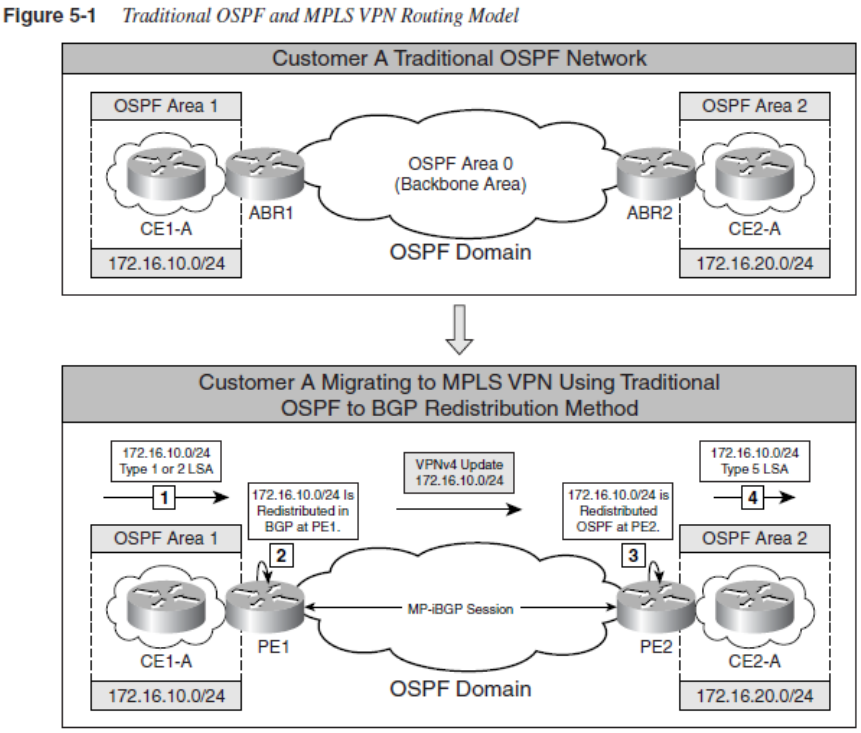
Ambientes y el concepto de la OSPF superbackbone para resolverlos. además, el OSPF PE-CE configuración de enrutamiento en un ambiente MPLS VPN y OSPF falsos enlaces,

Utilizado para resolver enrutamiento subóptimo causado por enlaces backdoor entre sitios OSPF en MPLS VPN, se discuten.

Modelo de enrutamiento OSPF tradicional:

El dominio OSPF tradicional se divide en áreas de backbone (Area 0), en la Figura 5-1 muestra al Cliente A implementando el modelo OSPF tradicional en el cual las áreas no-backbone, Area 1 y Area 2 pertenecientes al sitio 1 y al sitio 2, respectivamente, están conectados al área de OSPF, área 0.

Figura 18: Modelo de enrutamiento OSPF tradicional



Fuente: Acosta, H. 2016.

En un entorno MPLS VPN, las redes de los clientes están conectadas a una VPN MPLS habilitada por un proveedor. Como se muestra en la Figura, en que las Áreas del Cliente A, Áreas 1, son hora conectado a una red de proveedores habilitados para MPLS VPN. Área 1 y Área 2 tienen routers a los que llamaremos CE1-A y CE2-A que ejecutan el protocolo de enrutamiento OSPF. MP-iBGP, se utiliza entre PE1 y PE2 para propagar rutas entre el Sitio 1 (Área 1) y el Sitio 2 (Área 2).

La redistribución se realiza en los routers PE, PE1 y PE2. La figura 5-1 muestra lo si la siguiente secuencia que tiene lugar en la tradicional OSPF-BGP redistribución:

1. La red 172.16.10.0/24 se anuncia al enrutador PE1 por CE1-A como un tipo 1 o tipo 2 de estado de enlace (LSA).

2. La redistribución tradicional de la ruta OSPF-BGP tiene lugar cuando 172.16.10.0/24 es redistribuida en BGP en PE1. Esta ruta se propaga entonces como una ruta VPNv4 a PE2.

3 En PE2, el prefijo BGP VPNv4 172.16.10.0/24 se redistribuye en OSPF.

4 Esta ruta redistribuida 172.16.10.0/24 se propaga como una LSA externa tipo 5 OSPF.

Por lo tanto, el tipo de ruta OSPF o tipo LSA no se conserva cuando la ruta OSPF para 172.16.10.0 se redistribuye en BGP cuando se usan reglas de enrutamiento OSPF tradicionales en una MPLS VPN. Además, las siguientes características de las rutas externas de OSPF

No permiten una transición sin problemas para un cliente que intenta migrar de OSPF tradicional.

Enrutamiento al modelo de enrutamiento MPLS VPN:

• Las rutas internas, independientemente de su costo, siempre son preferidas a las rutas externas.

• Las rutas externas no pueden ser resumidas.

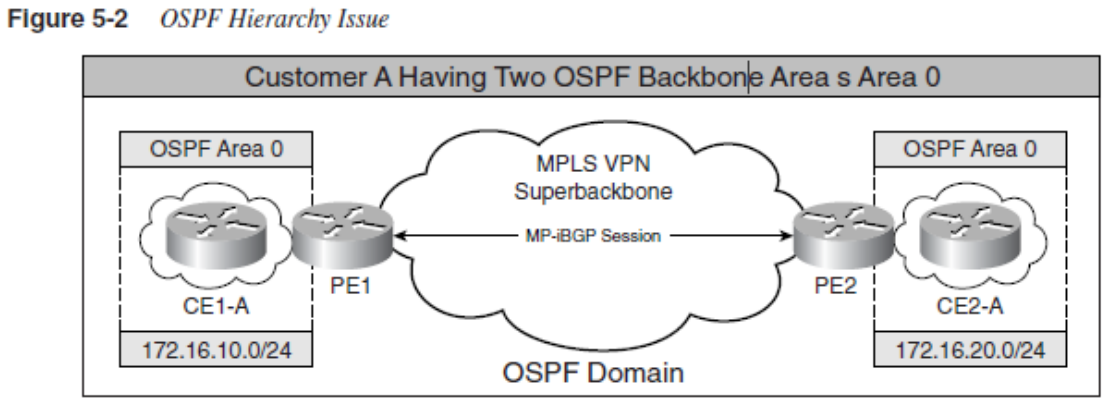
• Las rutas externas se inundan en todas las áreas OSPF.

• Las rutas externas podrían utilizar un tipo de métrica diferente que no es comparable al costo de OSPF.

• Las rutas externas de tipo 5 de LSA no se insertan en áreas de trozo o áreas no tan gruesas (NSSA).

Otro problema encontrado en las implementaciones de OSPF con MPLS VPN es que el cliente. Puede tener múltiples sitios en el Área 0, como se ilustra en la Figura, y, por lo tanto, desviarse de la jerarquía OSPF tradicional de la backbone única Area 0 con todas las áreas no backbone Conectado a esta Área 0.

Figura 19: Jerarquía OSPF



Fuente: Acosta, H. 2016.

MPLS VPN o OSPF Superbackbone Concepto

Para eludir los problemas planteados por el tradicional modelo de enrutamiento OSPF, el MPLS VPN Arquitectura para OSPF El enrutamiento PE-CE se amplió para permitir la transparencia de la Migración desde el tradicional enrutamiento OSPF al modelo de enrutamiento VPN MPLS. Otra backbone por encima de la OSPF Área 0. Esta backbone se llama OSPF o MPLS VPN Superbackbone

Como se muestra en la Figura:

• Las áreas que no son de backbone, Area 1 y Area 2, están conectadas directamente a MPLS VPN superpuesto que funciona como un Área OSPF 0. Por lo tanto, un Área real 0 no es como en el dominio OSPF tradicional. El área 0 es un requisito sólo cuando el PE router está conectado a dos áreas distintas de la backbone pertenecientes a la misma OSPF

Dominio en un enrutador PE.

• Los enrutadores PE, PE1 y PE2, que conectan las áreas OSPF en el dominio del cliente en el Superbackbone, aparecen como enrutadores de frontera de área OSPF para los dispositivos.

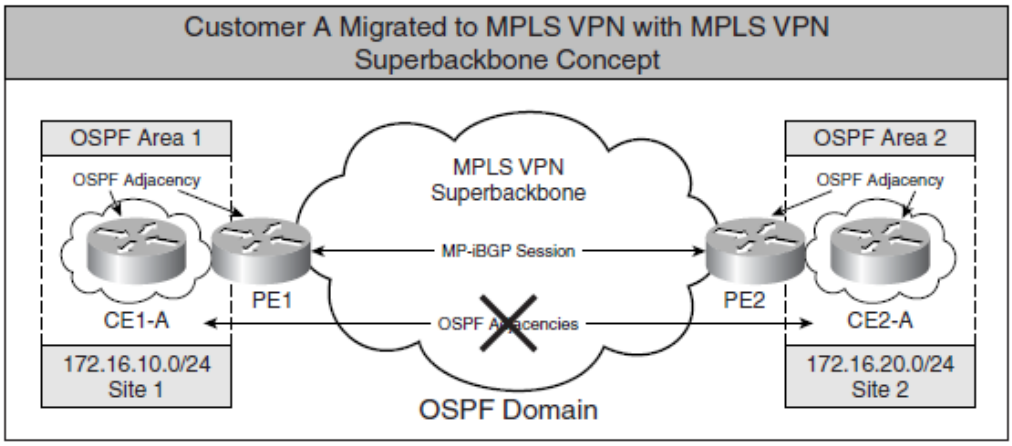
Los dominios OSPF del cliente. CE CE-A y CE2-A no tienen conocimiento de ningún otro OSPF más allá del superbackbone MPLS VPN debido a su transparencia.

• El superbackbone MPLS VPN se implementa utilizando MP-iBGP entre routers PE.

La información OSPF se transmite a través del superbackbone MPLS VPN usando BGP comunidades extendidas. Estas comunidades extendidas son establecidas y utilizadas por routers PE.

• No hay adyacencias OSPF o inundaciones en el superbackbone MPLS VPN para los sitios de clientes conectados a la superbackbone, excepto cuando se usan falsos enlaces OSPF.

Figura 20: superbackbone MPLS VPN



Fuente: Acosta, H. 2016.

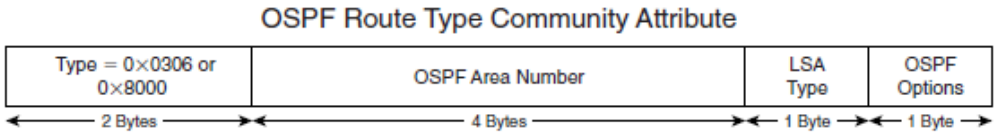
BGP Comunidades ampliadas para OSPF PE-CE Routing en el superbackbone MPLS VPN, se llevan los siguientes atributos extendidos BGP: Tipo de ruta OSPF: Propaga la información del tipo de ruta OSPF a través del MP-iBGP backbone. La Figura muestra el atributo de las comunidades extendidas del tipo de ruta OSPF. La Figura muestra el detalle del tipo de ruta OSPF para el prefijo 172.16.20.0, 192.168.99.0, y 192.168.199.0.

• **OSPF router ID—**• ID del enrutador OSPF: identifica el ID del enrutador del PE en la instancia relevante de VRF de OSPF. Esta dirección no forma parte del espacio de direcciones del proveedor y es única en la red OSPF.

• **OSPF domain ID**—ID de dominio OSPF: identifica el dominio de un prefijo OSPF específico en el MPLS VPN backbone. De forma predeterminada, este valor es igual al valor del ID de proceso de OSPF y puede ser sobrescrita por el comando domain ID ip-address bajo OSPF proceso. Si el ID de dominio de la ruta no coincide con el ID de dominio de la PE, la ruta se traduce a la ruta OSPF externa (LSA Tipo 5) con el tipo métrico E2, suponiendo que la ruta se recibió en la tabla VRF. Todo el enrutamiento entre OSPF es a través de LSAs Tipo 5.

Figura 21: Enrutamiento entre OSPF

Figure 5-4 *OSPF Route Type, Router ID, and Domain ID*



Fuente: Acosta, H. 2016.

Utilizado para garantizar la compatibilidad hacia atrás. OSPF Area Number - 4 bytes, que codifica un número de área de 32 bits. Para rutas externas, el valor es 0. Un valor distinto de 0 identifica la ruta como interna al dominio OSPF y como el área identificada. Los números de área son relativos a un dominio OSPF particular.

Tipo de ruta OSPF - 1 byte, codificado como sigue:

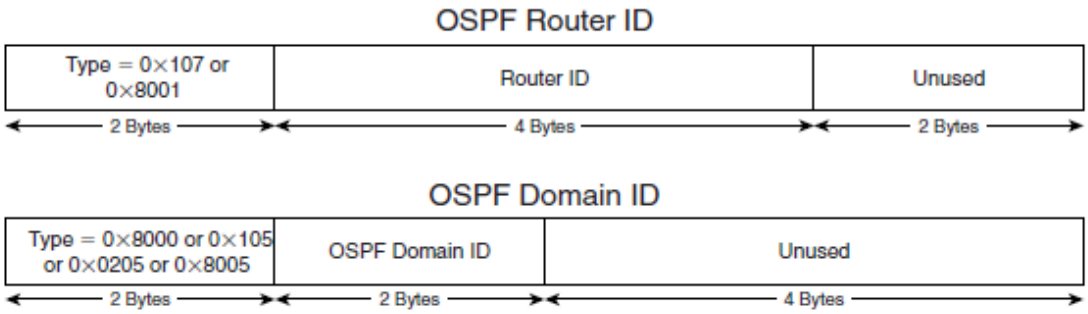
OSPF Option - Campo de 1 byte, se utiliza para rutas externas (Tipo 5 y 7 LSAs), si LSB de la opción _ 1. Ruta es de tipo métrico E2.

Figura 22: Ruta OSPF

OSPF Route Type - 1 byte, encoded as follows:

Value	Route Type
1 or 2	For Intra-Area Routes (Type 1 or Type 2 LSA)
3	Summary Route or LSA Type 3
5	External Routes or Type 5 LSA. In this case, the area number Is 0.
7	NSSA Routes
129	For Sham Link Endpoint Addresses

OSPF Option - 1 byte field, it is used for external routes (Type 5 and 7 LSAs), if LSB of option = 1, route is of metric type E2.



Fuente: Huidobro, J. y Millan, R. 2002.

CAPITULO III

DISEÑO Y DESCRIPCIÓN DEL SISTEMA

3.1. ANÁLISIS DE SISTEMA

3.1.1. Requerimiento de ancho de banda para las clases de servicio.

El producto de RPV 5 CoS es un servicio de transmisión de datos IP con tecnología de red MPLS (Multiprotocol Label Switching) que le permite al Cliente establecer cinco niveles de clases de servicio (CoS) adecuados para las aplicaciones de voz, video o datos de diferentes niveles de criticidad. Al aplicar políticas de clases de servicio o CoS sobre el ancho de banda contratado, se asegura un ancho de banda en la totalidad para cada tipo de tráfico y, al mismo tiempo, se define una política de encolamiento diferencial de paquetes en función de la clase de servicio en caso de que ocurra un incidente de congestión, asegurando que las aplicaciones sensibles al retardo en el tiempo y al descarte de paquetes, como aquéllas de voz y/o video, tengan

mayor prioridad en el transporte interno de la red y mantengan el nivel de desempeño que necesitan.

El ancho de banda del acceso deberá ser igual a la suma de los anchos de banda de cada una de las clases de servicio (CoS) que contrate el Cliente. Si no hubiera disponible comercialmente un ancho de banda igual a la suma de las velocidades de las clases de servicio contratadas, se deberá asignar la velocidad inmediatamente superior.

$$BW_{\text{Acceso a la Red}} = BW_{\text{CoS 1}} + BW_{\text{CoS 2}} + BW_{\text{CoS 3}} + BW_{\text{CoS 4}} + BW_{\text{CoS 5}}$$

Las políticas utilizadas para las cinco CoS son las siguientes:

Tabla 3: Requerimiento de ancho de banda la para red de "Cosapi".

	CoS5	CoS4	CoS3	CoS2	CoS1
Descripción	Voz en tiempo real	Video Premium	Datos Críticos	Datos Transaccionales	Datos Generales
Aplicaciones	Voz sobre IP	Video de alta velocidad sobre IP	Aplicaciones de datos sensibles a retardo o críticas para el negocio (SAP, Siebel, etc.)	Aplicaciones Transaccionales	Aplicaciones no prioritarias
Prioridad	Máxima	Alta 2	Alta 1	Mediana	Mínima
Tiempo Real	Sí	Sí	No	No	No
Exceso de Tráfico	Se descarta	Se descarta	Se remarca como CoS1	Se remarca como CoS1	No aplica remarcado

Fuente: Capacitación Claro.

- El tráfico de la clase de servicio Datos Generales (CoS1) puede utilizar los anchos de banda de las clases que no estén cursando tráfico pudiendo llegar al total de ancho de banda del acceso (100%)

- El tráfico que se clasifica en la clase de servicio Datos Generales (CoS1) es aquel asociado con aplicaciones no prioritarias para el cliente dado que ésta clase, al ser la de menor prioridad, podría experimentar variaciones en el retardo o pérdida de paquetes en función del grado de utilización de las aplicaciones prioritarias.

- En caso haya tráfico excedente en CoS2 (Datos Transaccionales), este será direccionado a CoS1 (Datos Generales), aplicándose para este excedente la prioridad correspondiente a CoS1.

- En caso haya tráfico excedente en CoS3 (Datos Críticos), este será direccionado a CoS1 (Datos Generales), aplicándose para este excedente la prioridad correspondiente a CoS1.

- Para el caso de CoS4 (Vídeo) y CoS5 (Voz), el tráfico excedente se descartará. Los valores de DSCP marcados desde el CPE serán transmitidos a través del backbone de Claro de manera transparente, sin alteración.

3.1.1.1 Software de la Plataforma

Los IOS recomendados y que han sido probados son:

Tabla 4: IOS de la Plataforma MPLS +Metro Ethernet Implementada

Hardware	Features	IOS
Cisco GSR 12406	Service Provider	c12kprp-p-mz.120-31.S6.bin
Cisco 7513	Service Provider	rsp-pv-mz.123-21.bin
Cisco 7206 VXR – NPE 400	Service Provider	c7200-p-mz.123-21.bin
Cisco 7206 VXR – NPE G1	Service Provider	c7200-p-mz.123-21.bin
Cisco 7206 VXR – NPE G2	Service Provider	c7200p-spservicesk9-mz.124-4.XD7.bin
Cisco Catalyst 4510R	Enhanced L3 3DES (OSPF, EIGRP, IS-IS)	cat4000-i5s-mz.122-25.EWA2.bin
Cisco Catalyst 4506	Enhanced L3 3DES (OSPF, EIGRP, IS-IS)	cat4000-i5s-mz.122-25.EWA2.bin
Cisco Catalyst 4503	Enhanced L3 3DES (OSPF, EIGRP, IS-IS)	cat4000-i5s-mz.122-25.EWA2.bin

Fuente: Capacitacion Claro.

3.1.2 Análisis de protocolos.

Se diseñará e implementará una red privada virtual en la sede remota (Cliente) para que pueda tener acceso hacia la sede principal (Proyecto Cosapi). Para ello primero se realizará el diseño, la simulación y finalmente la implementación,

3.1.2.1 Análisis de GNS3.

Para la simulacion de este proyecto se utilizará la herramienta GNS3 ya que nos permite realizar una simulación casi real, se utilizan los mismos IOS de cisco. Los IOS que se seleccionaron son los que soportan los protocolos a utilizar como son BGP, OSPF, QoS.

Utilizare GNS3 version 1.5.3 ya que es un simulador gráfico de red que permite diseñar topologías de red complejas, y permite emular las IOS que ejecutan los routers Cisco.

Como protocolo de nivel 3 para la distribucion de etiquetas:

- Multiprotol Label Swtiching (MPLS), para lo cual ha habilitado LDP (LDP- Protocolo estandar).

Los protocolos de ruteo usado en la red para la publicacion y distribucion de redes son:

- OSPF para las redes internas.

- Multiprotocol iBGP para las redes VPN IPv4 que representan las de los clientes MPLS/VPN.

- BGP para las redes IPv4 de Internet.

3.1.2.2 Protocolos de Enrutamiento

Los protocolos de enrutamiento que pueden utilizarse para ofrecer el servicio hacia los clientes finales estan en funcion al tipo de enrutadores involucrados en la comunicación.

3.1.2.3. Enrutamiento P1-PE-P2-PE, PE-PE

Para la implementacion de la Red MPLS/VPN+Metro local, los IGP son OSPF y Interno MP BGP (MP-iBGP). En esta forma la conectividad de los clientes se realiza con la exportacion e importacion de los valores correctos para Router Targets (RT). Los prefijos deben ser exportados de una VRF local (VPN Routing and Forwarding) a la sesion MP-BGP y importado nuevamente dentro de las VRF´s remotas.

3.1.2.4. Enrutamiento PE-CE para el servicio RPV Local

Este enrutamiento permite anunciar las redes del cliente hacia la Red MPLS/VPN Local, los protocolos de enrutamiento validados para esta funcion

son enrutamiento dinamico. Las redes de clientes para ser anunciadas desde los equipos CPEs deberan utilizar la opcion Network de BGPv4, y debera evitarse cualquier tipo de redistribucion de protocolos hacia BGPv4.

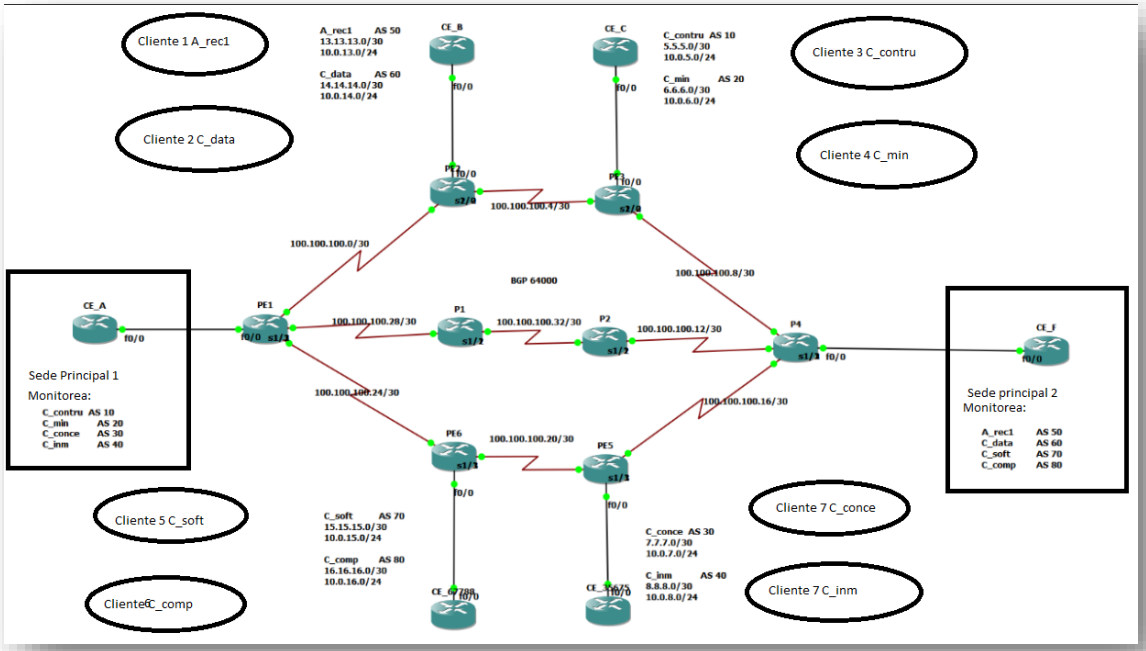
3.1.2.5. Enrutamiento CE – Red del Cliente.

Este enrutamiento permite la interaccion entre la red RPV con la red del sede - cliente. La seleccion del protocolo de enrutamiento en este caso debera adecuarse a las politicas de enrutamiento internas de las sedes. Este protocolo de enrutamiento se utiliza exclusivamente para el enrutamiento interno del sitio del cliente- sede y no debera redistribuirse al proceso BGPv4 utilizado para la comunicacion con el equipo PE. Los protocolos de enrutamiento que utilizare es en este caso OSPF.

3.1.2.6. Análisis de topología

La figura muestra la topología a implementar, en la que cada vrf corresponde a sedes de cosapi la cual trabajan en diferentes proyectos, donde CE_A y CE_F son router que estan ubicados en la sede principal y con ellos se monitorea las sedes de los proyectos ya que contiene todas las vrf, P1 y P2 son routers de interne, son core. Esta topologia es una implementacion de nuestra red MPLS con la cual trabaja claro y contiene equipos robustos para las redes de alto escalamiento.

Figura 23: Topología a implementar



Fuente: Elaboración propia.

Las distribuciones de VRF las tendremos de la siguiente manera, lo cual identificaran proyectos distintos:

VRF c_contru

VRF c_min

VRF c_conce

VRF c_inm

VRF a_rec1

VRF c_data

VRF c_soft

VRF c_comp

Las cuales serán definidas segun indica la siguiente tabla:

Tabla 5: Distribuciones de VRF

PARA	CE_A	CE_B	CE_C	CE_F	CE_D	CE_K
	C_contru AS 10	A_rec1 AS 50	C_contru AS 10	A_rec1 AS 50	C_conce AS 30	C_soft AS 70
	C_min AS 20	C_data AS 60	C_min AS 20	C_data AS 60	C_inm AS 40	C_comp AS 80
	C_conce AS 30			C_soft AS 70		
	C_inm AS 40			C_comp AS 80		

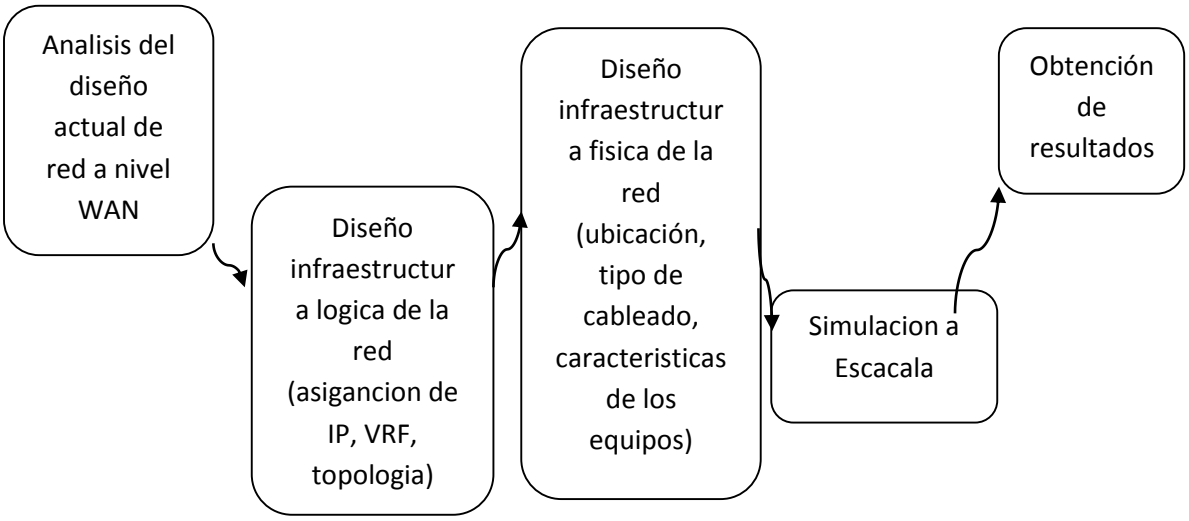
Fuente: elaboración propia.

- La comunicación entre los PE sera mediante bgp
- Los CE se comunican a traves de etiquetas y protocolo dinamico OSPF.

3.1.3. Plan de implementación.

En la siguiente figura se puede observar la secuencia de como resolveremos el problema de la empresa Cosapi. Observaremos los pasos fundamentales que tenemos que hacer para lograr un diseño de red acorde a las necesidades de la empresa.

Figura 24: Diagrama de bloques para la secuencia del Diseño



Fuente: Elaboración propia.

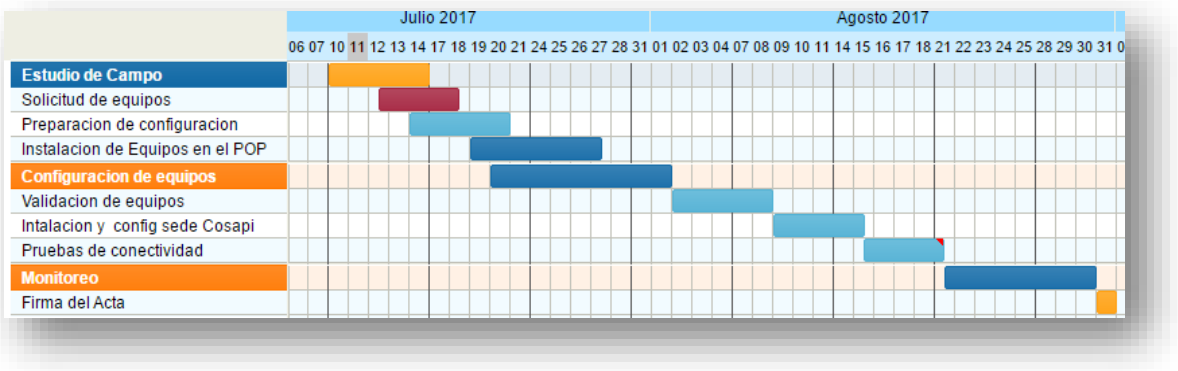
El primer paso a dar es el Análisis de la red actual de la empresa Cosapi, este paso nos hara entender como esta dividido la empresa Cosapi de acuerdo a sus proyectos, para esto necesitamos informacion de la distribucion de proyectos asi como el plano donde se encuentran hubicados.

Gracias a esta informacion procederemos con el diseño VPN, tomando en cuenta las necesidades de la empresa, esto se hara en 2 pasos, el primer paso sera el diseño de la red logica que comprende, en la topologia, como viajara la informacion, distribucion de las VRF, asignacion de IPs y loopback, tipos de protocolos a usar. El segundo sera el diseño de la infraestructura fisica de la red, la cual comprende de la parte geografica, describir el camino que recorrera la informacion, tipo de cableado y equipos a usar.

Teniendo ya el diseño de red completado, se procedera a hacer una simulacion a escala. Se hara un prototipo que consiste en una red mas pequeña, que tendra lo mas importante de la red original, pero la misma

estructura logica. Esto se hara utilizando es software GNS3 y asi obtener nuestros objetivos principales y generalizar los resultados obtenidos.

Tabla 6: Diagrama de GANTT



Fuente: Elaboración propia.

En la imagen mostrada se detalla las actividades realizadas con sus respectivos periodos de duración

3.2. DISEÑO Y SIMULACIÓN DEL SISTEMA

Hay 3 pasos fundamentales para el desarrollo de una red MPLS:

1) Definir la VRF, esta tabla de rutas que se asociara a la VPN

2) Asociar interfaces o subinterfaces a esa VRF es decir las interfaces del cliente meterlas dentro de la VRF VPN.

3) Definir, configurar esta VRF dento del multiprotocolo BGP, dicho protoclo BGP se usará para el intercambio de prefijos de la VPN.

Empezaremos definiendo las 8 VPNs a usar y colocando un nombre VRF diferente a cada uno como ya se habia mencionado.

Cosapi ingenieria y contrucción = VRF c_contru AS 10

Cosapi mineria = VRF c_min AS 20

Cosapi conceciones = VRF c_conce AS 30

Cosapi inmueble = VRF c_inm AS 40

RRHH = VRF a_rec1 AS 50

Cosapi data = VRFc_data AS 60

Cosapi software = VRFc_soft AS 70

Cosapi computer doctor = VRF c_comp AS 80

Tabla 7: Plan de direccionamiento.

DISPOSITIVO	INTERFACE	DIRECCION	VRF
ROUTER CE_A	FasEthernet 0/0.1	1.1.1.2 /30	c_contru
	FasEthernet 0/0. 2	2.2.2.2 /30	c_min
	FasEthernet 0/0. 3	3.3.3.2 /30	c_conce
	FasEthernet 0/0. 4	4.4.4.2 /30	c_inm
	Loopback 1	10.0.0.1 /24	c_contru
	Loopback 2	10.0.2.1 /24	c_min
	Loopback 3	10.0.3.1 / 24	c_conce
	Loopback 4	10.0.4.1 /24	c_inm
ROUTER PE1	FasEthernet 0/0.1	1.1.1.1 /30	c_contru
	FasEthernet 0/0.2	2.2.2.1 /30	c_min
	FasEthernet 0/0.3	3.3.3.1 /30	c_conce
	FasEthernet 0/0.4	4.4.4.1 /30	c_inm
	Serial 1/1	100.100.100.29 /30	N/A
	Serial 1/2	100.100.100.1 /30	N/A
	Serial 1/3	100.100.100.25 /30	N/A
	Loopback 0	100.100.1.1 / 32	N/A
	FasEthernet 0/0.1	9.9.9.2 /30	a_rec

	FasEthernet 0/0. 2	10.10.10.2 /30	c_data
ROUTER	FasEthernet 0/0. 3	11.11.11.2 /30	c_soft
CE_F	FasEthernet 0/0. 4	12.12.12.2 /30	c_comp
	Loopback 1	10.0.9.1 /24	a_rec
	Loopback 2	10.0.10.1 /24	c_data
	Loopback 3	10.0.11.1 / 24	c_soft
	Loopback 4	10.0.12.1 /24	c_comp
	FasEthernet 0/0.50	192.168.50.1 /30	c_conce
ROUTER	FasEthernet 0/0. 60	192.168.60.1 /30	c_inm
PE3	Serial 1/0	200.200.200.2 /30	c_conce
	Serial 1/3	200.200.200.17 /30	c_inm
	Loopback 0	200.200.100.3 /32	N/A
	FasEthernet 0/0.1	13.13.13.2 /30	a_rec1
ROUTER	FasEthernet 0/0. 2	14.14.14.2 /30	c_data
CE_B	Loopback 1	10.0.13.1 /24	a_rec1
	Loopback 2	10.0.14.1 /24	c_data
	FasEthernet 0/0.1	5.5.5.2 /30	c_contru
ROUTER	FasEthernet 0/0.2	6.6.6.2 /30	c_min
CE_c	Loopback 1	10.0.5.1 /24	c_contru
	Loopback 2	10.0.6.1 /24	c_min
	FasEthernet 0/0.1	7.7.7.1 /30	c_conce
ROUTER	FasEthernet 0/0. 60	8.8.8.1 /30	c_inm
PE5	Serial 1/1	100.100.100.22 /30	N/A
	Serial 1/3	100.100.100.17 /30	N/A
	Loopback 0	100.100.1.5 /32	N/A
	FasEthernet 0/0.1	7.7.7.2 /30	c_conce
ROUTER	FasEthernet 0/0.2	8.8.8.2 /30	c_inm
CE_D	Loopback 1	10.0.7.1 /24	c_conce
	Loopback 2	10.0.8.1 /24	c_inm

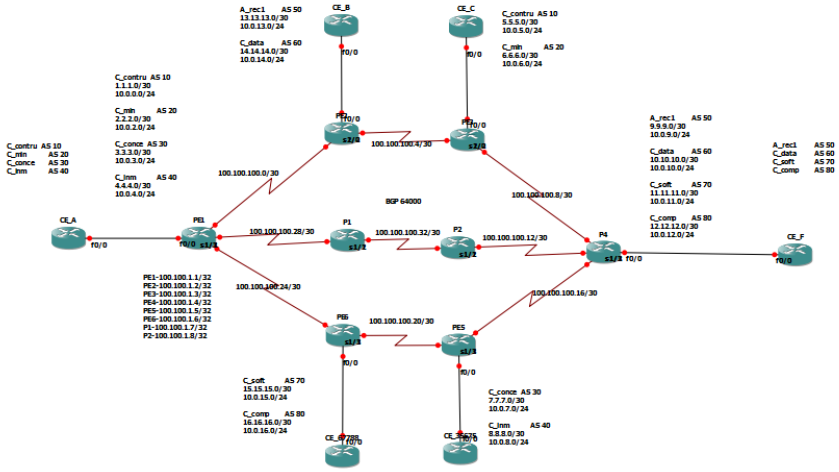
ROUTER PE6	FasEthernet 0/0.1	15.15.15.1 /30	c_soft
	FasEthernet 0/0. 60	16.16.16.1 /30	c_comp
	Serial 1/1	100.100.100.21 /30	N/A
	Serial 1/3	100.100.100.26 /30	N/A
	Loopback 0	100.100.1.6 /32	N/A
ROUTER CE_k	FasEthernet 0/0.1	15.15.15.2 /30	c_soft
	FasEthernet 0/0.2	16.16.16.2 /30	c_comp
	Loopback 1	10.0.15.1 /24	c_soft
	Loopback 2	10.0.16.1 /24	c_comp
P1	Serial 1/1	100.100.100.30 /30	N/A
	Serial 1/2	100.100.100.34 /30	N/A
	Loopback 0	100.100.1.7 /32	N/A
P2	Serial 1/1	100.100.100.14 /30	N/A
	Serial 1/2	100.100.100.33 /30	N/A
	Loopback 0	100.100.1.8 /32	N/A

Fuente: Elaboración propia.

3.2.1 Simulación

Luego diseñamos una topologia de manera que sea redundante.

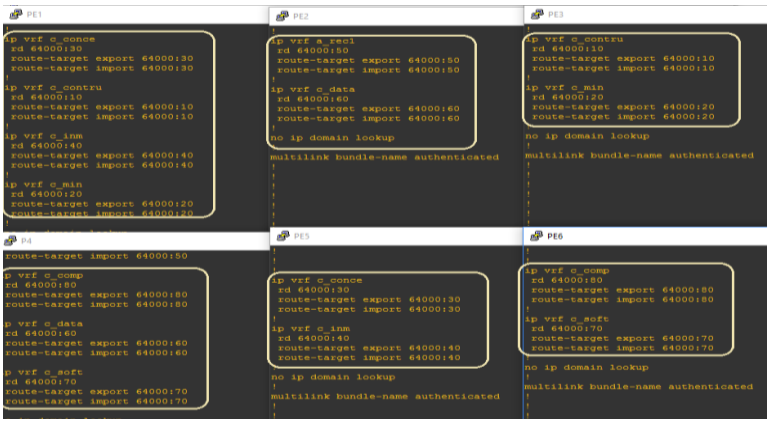
Figura 25: Diseño de Topología



Fuente: Elaboración propia.

Antes de configurar debemos definir el route distinguisher (rd), ya que este se utiliza para hacer unicos a los prefijos VPN, su funcion es añadir 64 bits a los 32 bits del prefijo IP, con ello se generan 96 bits el cual sera unico en toda la red, luego añadimos el Route Targets, este es una etiqueta que se añade al prefijo de 96 bits para identificar de que VPN viene y luego poder seleccionarlo en otros extremos para descargarse ese prefijo dentro de la VRF.

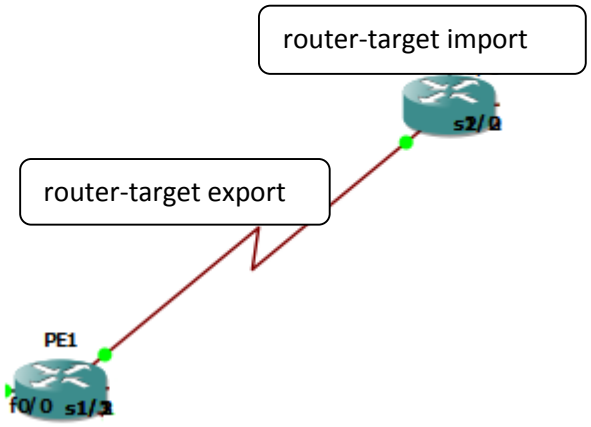
Figura 26: Prefijos VPN



Fuente: Elaboración propia.

Los prefijos que tomemos de la VRF y lo metamos dentro de la BGP VPN se incluira con el Route Targets que se coloque en el router-target export asi como en el otro extremo PE2, cuando quiera descargar a la tabla VRF, los prefijos que correspondan a esas VPN de cliente, indicara descargarse aquiellos prefijos que tengan un router target y el valor que coloquemos en el router-target import.

Figura 27: Router target



Fuente: Elaboracion propia.

El siguiente paso es añadir las interfaces del cliente, dentro de la VRF lo cual se tiene que hacer dentro de la interface.

Luego seguimos con la configuracion BGP, tenemos que hacer 2 pasos, primero definir las vecindades BGP, las sesiones BGP dentro de la tabla BGP vpn, crear un address family y empezar a definir a los vecinos sin importar que pertenezca o no a la misma VPN, establecer sesiones BGP a travez del address family.

En cisco lo que hace es en router BGP AS define los vecinos, luego el address family VPNv4 las activa.

Dentro del address family especificamos que prefijos queremos que pasen a la tabla BGP.

El router target se añade despues de saber que prefijos usar, estos prefijos estan dentro del address family donde tendremos el protocolo OSPF.

Redistribuye connecte sirve para indicar que todo lo que este conectado a la VRF lo envie dentro de la tabla BGP, junto con el router targe. que se ha indicado.

3.2.2 CONFIGURACIÓN DE DISPOSITIVOS.

3.2.2.1 Configuracion de interfase Loopback para Gestion de CE

1. interface loopback 0

// Definicion de interfase loopback para Gestion del CE

2. description Interfase Loopback de Gestión

// Nombre de la interfase loopback de Gestion

3. ip address <Dirección IP de la interfase Loopback>

// Definicion de la direccion IP, tener en cuenta que el PE tenga una ruta estatica para alcanzar la direccion IP Loopback. Esta IP es asignada por el NOC.

Configuracion de Clases de Servicio para la administracion de congestion - WAN

3.2.2.2. Configuracion de Clases de Servicio para la administracion de congestion -WAN

1. (config)#class-map match-any qos5

// Crea la clase para un trafico especifico

2. (config-cmap)#match ip dscp cs5

// Clasifica el trafico definido como CS5

3. (config)#class-map match-any qos2

// Crea la clase para un trafico datos especifico

4. (config-cmap)#match ip dscp cs2

// Clasifica el trafico definido como CS2

5. (config)#class-map match-any qos1

// Crea la clase para un trafico datos especifico

6. (config-cmap)#match ip dscp cs1

// Clasifica el trafico definido como CS1

// El trafico que no se encuentre dentro de alguna clase definida, seran considerados dentro de la clase default

3.2.2.3. Configuracion de Politicas de trafico para cada sede - WAN

1. (config)#policy-map wan

// Priorizacion del trafico de acuerdo a la clase

2. (config-pmap)#class qos5

// Trafico de CoS 3 que fue definido por el ACL

3. (config-pmap-c)#priority bw3

// Asigna prioridad de acuerdo al parametros de ancho de ancho de banda por canal de trafico

del tipo VoIP, ToIP, Videoconferencia o cualquier otro tipo de trafico sensible al retardo.

4. (config-pmap-c)#police bw3 peak1 peak 2 conform-action transmit exceed-action drop

// Limita el ancho de banda asignado como trafico con prioridad cs5 al valor de bw3, descartando el exceso

5. (config-pmap)#class qos2

// Referencia al trafico de tipo P2, y le asigna un ancho de banda

6. (config-pmap-c)#bandwidth bw2

// Asigna el ancho de banda para el trafico con prioridad 2

7. (config-pmap-c)#police bw2 peak1 peak 2 conform-action transmit exceed-action settransmit-dscp cs1

// Limita el ancho de banda asignado como trafico con prioridad 2 (cs2), el exceso de trafico sera remarcado como prioridad 1 (cs1).

8. (config-pmap)#class qos1

// Referencia al trafico de tipo P1, y le asigna un ancho de banda

9. (config-pmap-c)#bandwidth bw1

// Asigna el ancho de banda para el trafico con prioridad 1

10. (config-pmap)#Class class-default

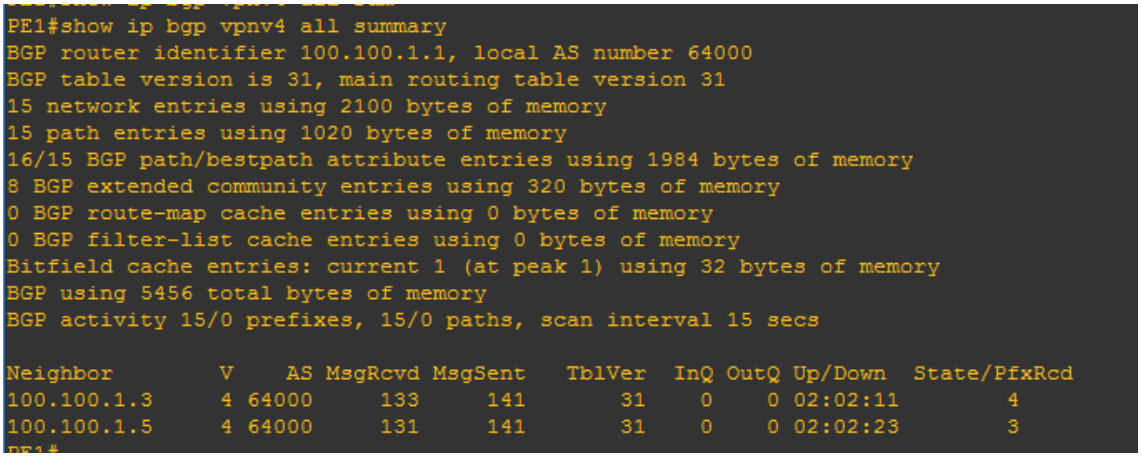
//Asigna el ancho de banda para el trafico por defecto

(config-pmap-c)# fair-queue

3.3. REVISIÓN Y CONSOLIDACIÓN DE RESULTADOS

Para PE1 podemos ver los address family VPNv4 que se ha configurado esto quiere decir que PE1 tiene 2 vecinos o ha iniciado seciones con 100.100.1.3 y 100.100.1.5 cuyo sistema autonomo AS es 64000, tambien se observa los prefijos que estamos recibiendo de cada uno los cuales seria 4 y 3, tambien vemos que esta enviando y recibiendo paquetes.

Figura 28: Prefijos recibidos

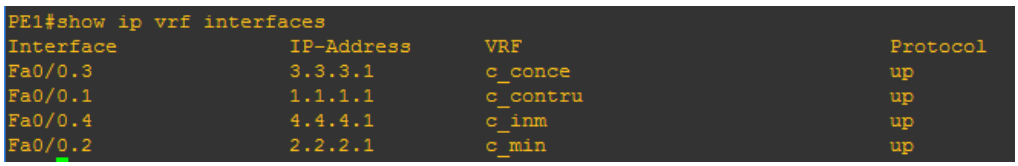


```
PE1#show ip bgp vpnv4 all summary
BGP router identifier 100.100.1.1, local AS number 64000
BGP table version is 31, main routing table version 31
15 network entries using 2100 bytes of memory
15 path entries using 1020 bytes of memory
16/15 BGP path/bestpath attribute entries using 1984 bytes of memory
8 BGP extended community entries using 320 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 5456 total bytes of memory
BGP activity 15/0 prefixes, 15/0 paths, scan interval 15 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
100.100.1.3     4 64000     133     141       31    0    0 02:02:11        4
100.100.1.5     4 64000     131     141       31    0    0 02:02:23        3
```

Fuente: Elaboración propia.

Dentro de PE1 podemos visualizar las VRF creadas y a que interface estan asociadas.

Figura 29: VRF creadas

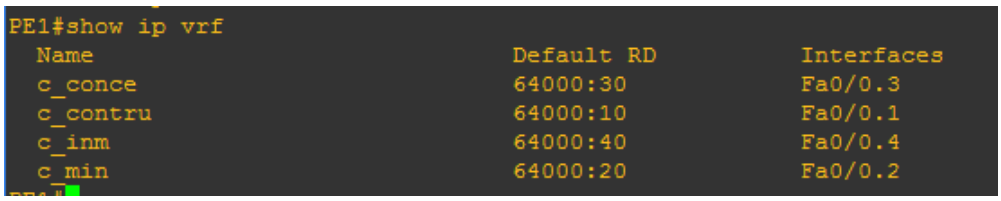


```
PE1#show ip vrf interfaces
Interface              IP-Address      VRF                              Protocol
Fa0/0.3                3.3.3.1         c_conce                          up
Fa0/0.1                1.1.1.1         c_contru                         up
Fa0/0.4                4.4.4.1         c_inm                            up
Fa0/0.2                2.2.2.1         c_min                            up
```

Fuente: Elaboración propia.

Vemos el RD configurada.

Figura 30: RD configurada.

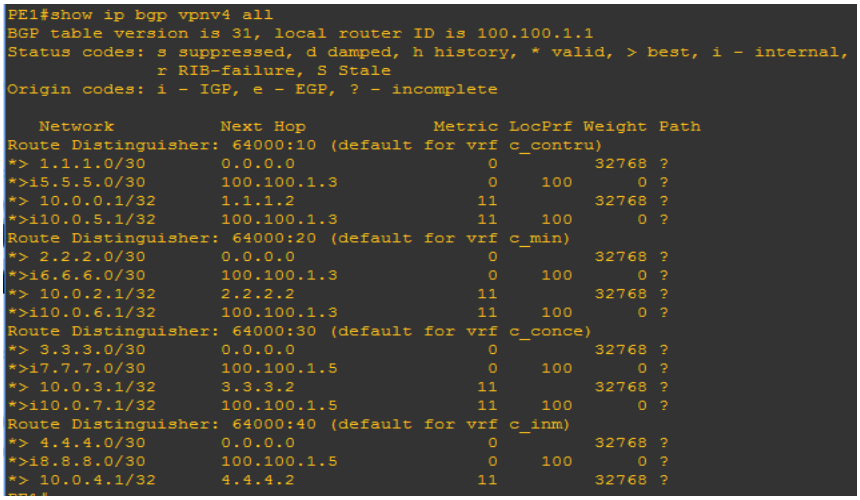


```
PE1#show ip vrf
  Name                             Default RD          Interfaces
  c_conce                          64000:30            Fa0/0.3
  c_contru                         64000:10            Fa0/0.1
  c_inm                            64000:40            Fa0/0.4
  c_min                            64000:20            Fa0/0.2
```

Fuente: Elaboración propia.

Aquí podemos visualizar todos los prefijos VPN que se estan anunciado y con que RD, su siguiente salto, y quien lo anuncia.

Figura 31: Prefijos VPN

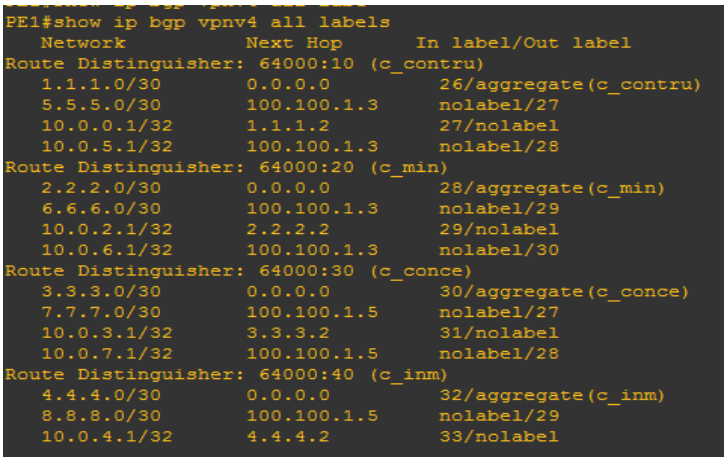


```
PE1#show ip bgp vpnv4 all
BGP table version is 31, local router ID is 100.100.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 64000:10 (default for vrf c_contru)
*> 1.1.1.0/30       0.0.0.0                  0         32768 ?
*>i5.5.5.0/30       100.100.1.3              0    100      0 ?
*> 10.0.0.1/32      1.1.1.2                 11         32768 ?
*>i10.0.5.1/32      100.100.1.3             11    100      0 ?
Route Distinguisher: 64000:20 (default for vrf c_min)
*> 2.2.2.0/30       0.0.0.0                  0         32768 ?
*>i6.6.6.0/30       100.100.1.3              0    100      0 ?
*> 10.0.2.1/32      2.2.2.2                 11         32768 ?
*>i10.0.6.1/32      100.100.1.3             11    100      0 ?
Route Distinguisher: 64000:30 (default for vrf c_conce)
*> 3.3.3.0/30       0.0.0.0                  0         32768 ?
*>i7.7.7.0/30       100.100.1.5              0    100      0 ?
*> 10.0.3.1/32      3.3.3.2                 11         32768 ?
*>i10.0.7.1/32      100.100.1.5             11    100      0 ?
Route Distinguisher: 64000:40 (default for vrf c_inm)
*> 4.4.4.0/30       0.0.0.0                  0         32768 ?
*>i8.8.8.0/30       100.100.1.5              0    100      0 ?
*> 10.0.4.1/32      4.4.4.2                 11         32768 ?
```

Fuente: Elaboración propia.

Para cada uno de los prefijos tenemos etiqueta de entrada y salidas; por ejemplo, PE1 sabe que para alcanzar el prefijo 6.6.6..0/30 tiene que pasar por 100.100.1.3 y colocarle la etiqueta 29. tenemos la etiqueta de entrada (nolabel) y la etiqueta de salida (29)

Figura 32: Etiquetas PE1



```
PE1#show ip bgp vpnv4 all labels
   Network          Next Hop      In label/Out label
Route Distinguisher: 64000:10 (c_contru)
   1.1.1.0/30       0.0.0.0         26/aggregate(c_contru)
   5.5.5.0/30       100.100.1.3     nolabel/27
   10.0.0.1/32      1.1.1.2         27/nolabel
   10.0.5.1/32      100.100.1.3     nolabel/28
Route Distinguisher: 64000:20 (c_min)
   2.2.2.0/30       0.0.0.0         28/aggregate(c_min)
   6.6.6.0/30       100.100.1.3     nolabel/29
   10.0.2.1/32      2.2.2.2         29/nolabel
   10.0.6.1/32      100.100.1.3     nolabel/30
Route Distinguisher: 64000:30 (c_conce)
   3.3.3.0/30       0.0.0.0         30/aggregate(c_conce)
   7.7.7.0/30       100.100.1.5     nolabel/27
   10.0.3.1/32      3.3.3.2         31/nolabel
   10.0.7.1/32      100.100.1.5     nolabel/28
Route Distinguisher: 64000:40 (c_inm)
   4.4.4.0/30       0.0.0.0         32/aggregate(c_inm)
   8.8.8.0/30       100.100.1.5     nolabel/29
   10.0.4.1/32      4.4.4.2         33/nolabel
```

Fuente: Elaboración propia.

Mostramos todas las etiquetas para obtener una salida más precisa, como la tabla de etiquetas de un VRF.

Etiquetas PE2

```
PE2#show ip bgp vpnv4 all labels
   Network          Next Hop      In label/Out label
Route Distinguisher: 64000:50 (a_rec1)
   9.9.9.0/30       100.100.1.4     nolabel/26
   10.0.9.1/32      100.100.1.4     nolabel/27
   10.0.13.1/32     13.13.13.2      27/nolabel
   13.13.13.0/30    0.0.0.0         28/aggregate(a_rec1)
Route Distinguisher: 64000:60 (c_data)
   10.0.10.1/32     100.100.1.4     nolabel/28
   10.0.14.1/32     14.14.14.2      29/nolabel
   10.10.10.0/30    100.100.1.4     nolabel/29
   14.14.14.0/30    0.0.0.0         30/aggregate(c_data)
```

Fuente: Elaboración propia.

Etiquetas PE3

```
PE3#show ip bgp vpnv4 all labels
   Network          Next Hop      In label/Out label
Route Distinguisher: 64000:10 (c_contru)
   1.1.1.0/30       100.100.1.1     nolabel/26
   5.5.5.0/30       0.0.0.0         27/aggregate(c_contru)
   10.0.0.1/32      100.100.1.1     nolabel/27
   10.0.5.1/32      5.5.5.2         28/nolabel
Route Distinguisher: 64000:20 (c_min)
   2.2.2.0/30       100.100.1.1     nolabel/28
   6.6.6.0/30       0.0.0.0         29/aggregate(c_min)
   10.0.2.1/32      100.100.1.1     nolabel/29
   10.0.6.1/32      6.6.6.2         30/nolabel
```

Fuente: Elaboración propia.

Network: Muestra la dirección de red de la tabla BGP.

Next Hop: Especifica la dirección de salto siguiente BGP.

In label: Muestra la etiqueta (si existe) asignada por este enrutador.

Out label: Muestra la etiqueta asignada por el enrutador de salto siguiente BGP.

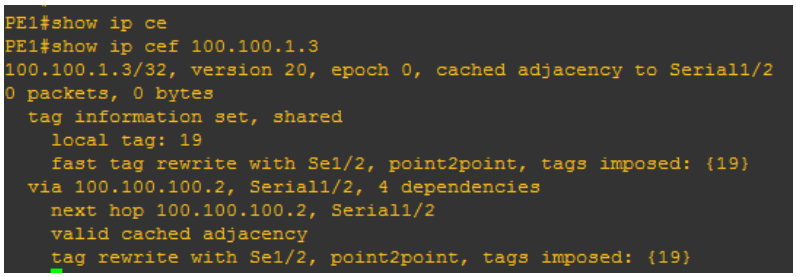
Etiquetas PE4

```
PE4#show ip bgp vpnv4 all labels
   Network          Next Hop      In label/Out label
Route Distinguisher: 64000:50 (a_rec1)
   9.9.9.0/30       0.0.0.0         26/aggregate(a_rec1)
   10.0.9.1/32      9.9.9.2         27/nolabel
   10.0.13.1/32     100.100.1.2     nolabel/27
   13.13.13.0/30    100.100.1.2     nolabel/28
Route Distinguisher: 64000:60 (c_data)
   10.0.10.1/32     10.10.10.2      28/nolabel
   10.0.14.1/32     100.100.1.2     nolabel/29
   10.10.10.0/30    0.0.0.0         29/aggregate(c_data)
   14.14.14.0/30    100.100.1.2     nolabel/30
Route Distinguisher: 64000:70 (c_soft)
   10.0.11.1/32     11.11.11.2      30/nolabel
   10.0.15.1/32     100.100.1.6     nolabel/29
   11.11.11.0/30    0.0.0.0         31/aggregate(c_soft)
   15.15.15.0/30    100.100.1.6     nolabel/27
Route Distinguisher: 64000:80 (c_comp)
   10.0.12.1/32     12.12.12.2      32/nolabel
   10.0.16.1/32     100.100.1.6     nolabel/30
   12.12.12.0/30    0.0.0.0         33/aggregate(c_comp)
   16.16.16.0/30    100.100.1.6     nolabel/28
```

Fuente: Elaboración propia.

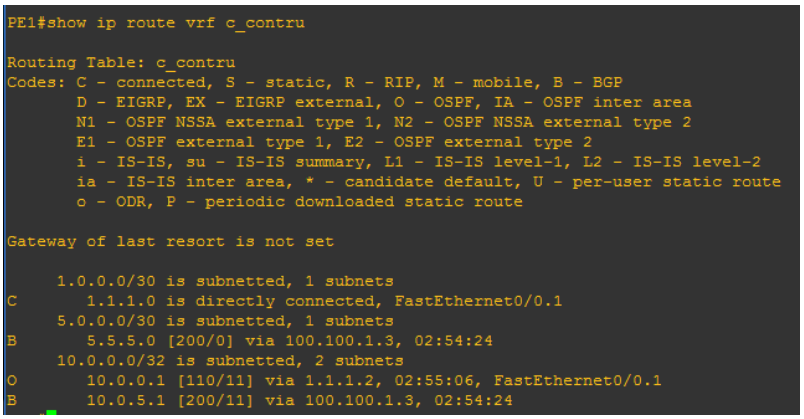
En la siguiente figura vemos la etiqueta que utilizara para llegar al siguiente salto que es 100.100.1.3

Figura 33: Etiqueta para salto



Fuente: Elaboración propia.

Figura 34: Tabla de enrutamiento con la VRF-CONTRU



Fuente: Elaboración propia.

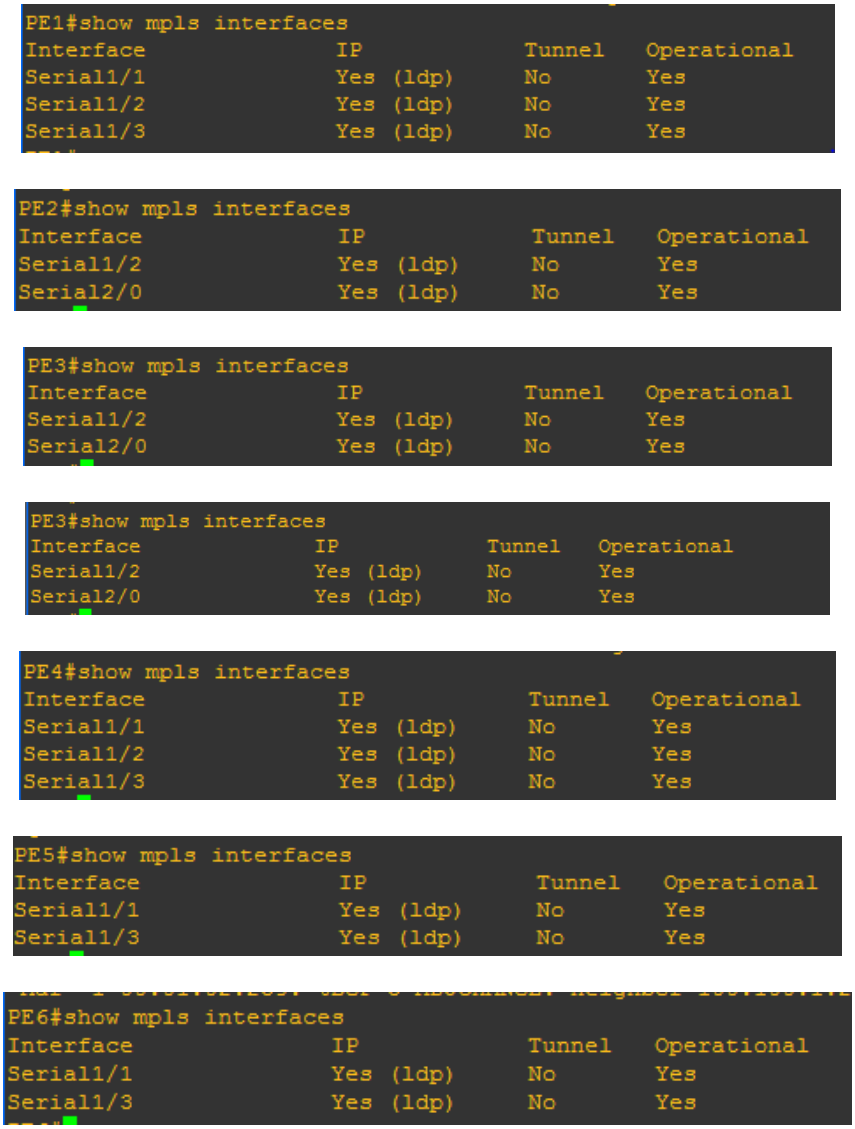
Cada vrf con su loopback, debe haber una comnutacion dinamica atraves de vrf y ospf, cada subinterface tien una vrf, se configura router reflecter, para hacer una red mas segura a nivel de caida de enlace, todo se conoe atravez de BGP, se puede comunicar con VRF a traves de otro nodo.

bgp se comunica a traves de loopback.

P1 yP2 son los backbon es una red troncal, se sua para administrar el trafico

Reduce significativamente el procesamiento de paquetes que se requiere cada vez que ingresa un paquete a un enrutador en la red.

Figura 35: Conexiones de red MPLS

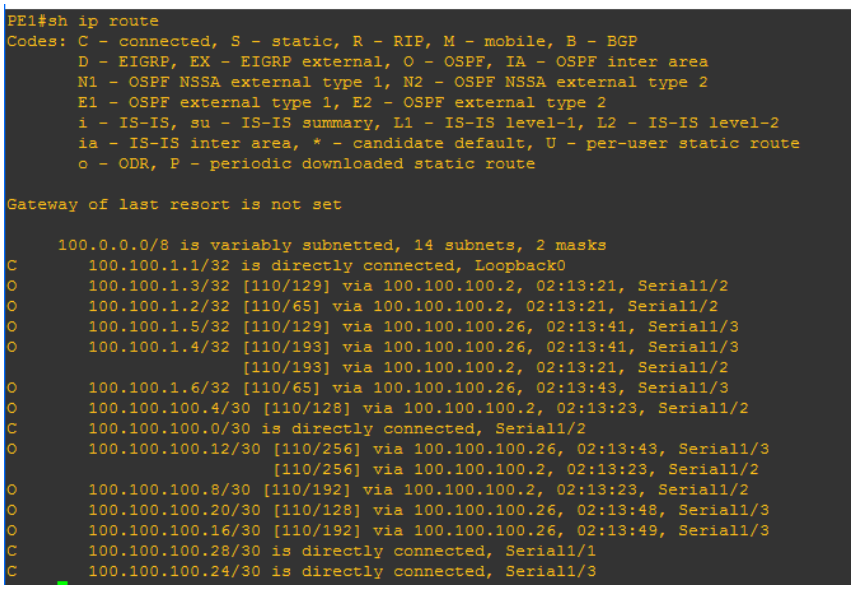


Fuente: Elaboración propia.

En la figura 35 vemos la configuración LDP de las interfaces seriales de PE1-2-3, todas las interfaces LDP en UP.

Este campo muestra que MPLS IP está configurado para una interfaz. El LDP aparece entre paréntesis a la derecha. El LDP es: Protocolo de Distribución de Etiquetas (TDP).

Figura 36: Revisión de tablas de enrutamiento para PE1

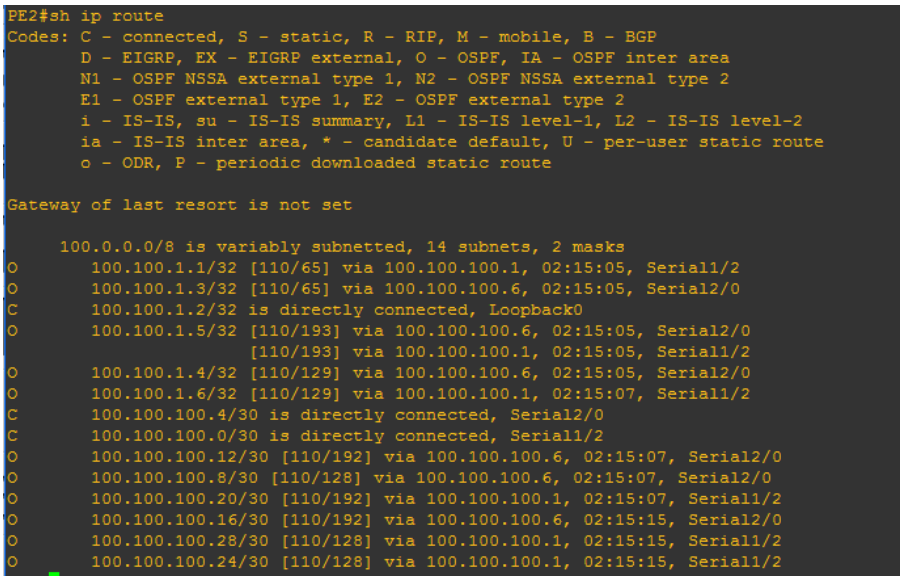


```
PE1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, 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 not set

     100.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
C       100.100.1.1/32 is directly connected, Loopback0
O       100.100.1.3/32 [110/129] via 100.100.100.2, 02:13:21, Serial1/2
O       100.100.1.2/32 [110/65] via 100.100.100.2, 02:13:21, Serial1/2
O       100.100.1.5/32 [110/129] via 100.100.100.26, 02:13:41, Serial1/3
O       100.100.1.4/32 [110/193] via 100.100.100.26, 02:13:41, Serial1/3
                       [110/193] via 100.100.100.2, 02:13:21, Serial1/2
O       100.100.1.6/32 [110/65] via 100.100.100.26, 02:13:43, Serial1/3
O       100.100.100.4/30 [110/128] via 100.100.100.2, 02:13:23, Serial1/2
C       100.100.100.0/30 is directly connected, Serial1/2
O       100.100.100.12/30 [110/256] via 100.100.100.26, 02:13:43, Serial1/3
                          [110/256] via 100.100.100.2, 02:13:23, Serial1/2
O       100.100.100.8/30 [110/192] via 100.100.100.2, 02:13:23, Serial1/2
O       100.100.100.20/30 [110/128] via 100.100.100.26, 02:13:48, Serial1/3
O       100.100.100.16/30 [110/192] via 100.100.100.26, 02:13:49, Serial1/3
C       100.100.100.28/30 is directly connected, Serial1/1
C       100.100.100.24/30 is directly connected, Serial1/3
```

Fuente: Elaboración propia.

Se verifica que las rutas del protocolo para la red MPLS y todos los vecinos estan presentes. Se veririca la tabla de enrutamiento en PE1 - PE2

Figura 37: Revisión de tablas de enrutamiento para PE2

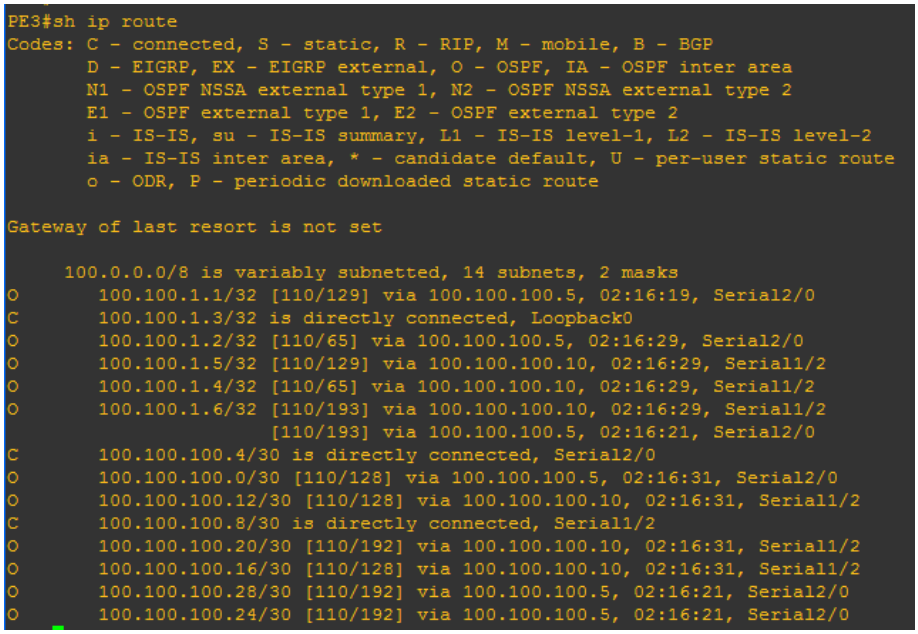


```
PE2#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, 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 not set

     100.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
O       100.100.1.1/32 [110/65] via 100.100.100.1, 02:15:05, Serial1/2
O       100.100.1.3/32 [110/65] via 100.100.100.6, 02:15:05, Serial2/0
C       100.100.1.2/32 is directly connected, Loopback0
O       100.100.1.5/32 [110/193] via 100.100.100.6, 02:15:05, Serial2/0
                       [110/193] via 100.100.100.1, 02:15:05, Serial1/2
O       100.100.1.4/32 [110/129] via 100.100.100.6, 02:15:05, Serial2/0
O       100.100.1.6/32 [110/129] via 100.100.100.1, 02:15:07, Serial1/2
C       100.100.100.4/30 is directly connected, Serial2/0
C       100.100.100.0/30 is directly connected, Serial1/2
O       100.100.100.12/30 [110/192] via 100.100.100.6, 02:15:07, Serial2/0
O       100.100.100.8/30 [110/128] via 100.100.100.6, 02:15:07, Serial2/0
O       100.100.100.20/30 [110/192] via 100.100.100.1, 02:15:07, Serial1/2
O       100.100.100.16/30 [110/192] via 100.100.100.6, 02:15:15, Serial2/0
O       100.100.100.28/30 [110/128] via 100.100.100.1, 02:15:15, Serial1/2
O       100.100.100.24/30 [110/128] via 100.100.100.1, 02:15:15, Serial1/2
```

Fuente: Elaboración propia.

Mostramos el estado actual de la tabla de enrutamiento.

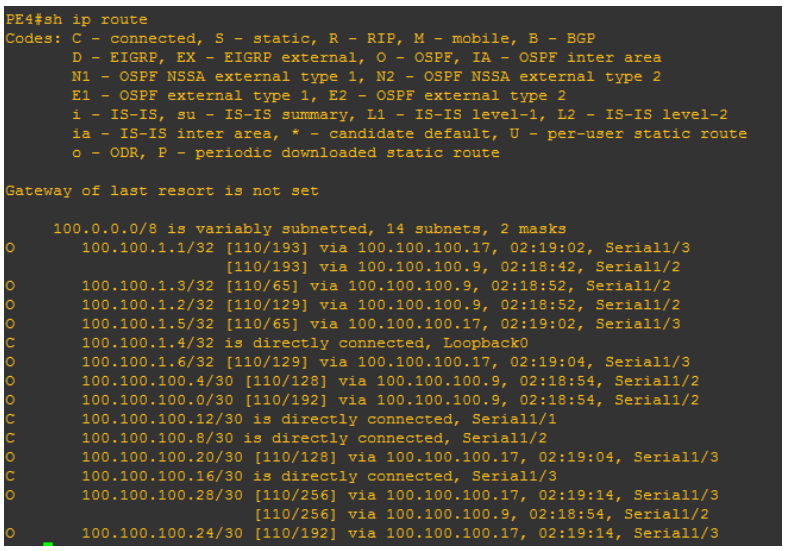
Figura 38: Revisión de tablas de enrutamiento para PE3



```
PE3#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 not set

     100.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
O       100.100.1.1/32 [110/129] via 100.100.100.5, 02:16:19, Serial2/0
C       100.100.1.3/32 is directly connected, Loopback0
O       100.100.1.2/32 [110/65] via 100.100.100.5, 02:16:29, Serial2/0
O       100.100.1.5/32 [110/129] via 100.100.100.10, 02:16:29, Serial1/2
O       100.100.1.4/32 [110/65] via 100.100.100.10, 02:16:29, Serial1/2
O       100.100.1.6/32 [110/193] via 100.100.100.10, 02:16:29, Serial1/2
                       [110/193] via 100.100.100.5, 02:16:21, Serial2/0
C       100.100.100.4/30 is directly connected, Serial2/0
O       100.100.100.0/30 [110/128] via 100.100.100.5, 02:16:31, Serial2/0
O       100.100.100.12/30 [110/128] via 100.100.100.10, 02:16:31, Serial1/2
C       100.100.100.8/30 is directly connected, Serial1/2
O       100.100.100.20/30 [110/192] via 100.100.100.10, 02:16:31, Serial1/2
O       100.100.100.16/30 [110/128] via 100.100.100.10, 02:16:31, Serial1/2
O       100.100.100.28/30 [110/192] via 100.100.100.5, 02:16:21, Serial2/0
O       100.100.100.24/30 [110/192] via 100.100.100.5, 02:16:21, Serial2/0
```

Fuente: Elaboración propia.

Figura 39: Revisión de tablas de enrutamiento para PE4

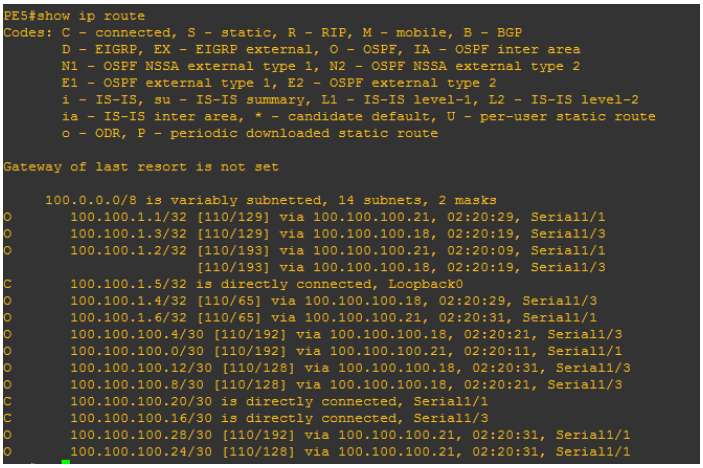


```
PE4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, 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 not set

     100.0.0.0/8 is variably subnetted, 14 subnets, 2 masks
O       100.100.1.1/32 [110/193] via 100.100.100.17, 02:19:02, Serial1/3
                       [110/193] via 100.100.100.9, 02:18:42, Serial1/2
O       100.100.1.3/32 [110/65] via 100.100.100.9, 02:18:52, Serial1/2
O       100.100.1.2/32 [110/129] via 100.100.100.9, 02:18:52, Serial1/2
O       100.100.1.5/32 [110/65] via 100.100.100.17, 02:19:02, Serial1/3
C       100.100.1.4/32 is directly connected, Loopback0
O       100.100.1.6/32 [110/129] via 100.100.100.17, 02:19:04, Serial1/3
O       100.100.100.4/30 [110/128] via 100.100.100.9, 02:18:54, Serial1/2
O       100.100.100.0/30 [110/192] via 100.100.100.9, 02:18:54, Serial1/2
C       100.100.100.12/30 is directly connected, Serial1/1
C       100.100.100.8/30 is directly connected, Serial1/2
O       100.100.100.20/30 [110/128] via 100.100.100.17, 02:19:04, Serial1/3
C       100.100.100.16/30 is directly connected, Serial1/3
O       100.100.100.28/30 [110/256] via 100.100.100.17, 02:19:14, Serial1/3
                          [110/256] via 100.100.100.9, 02:18:54, Serial1/2
O       100.100.100.24/30 [110/192] via 100.100.100.17, 02:19:14, Serial1/3
```

Fuente: Elaboración propia.

En la figura 38 podemos ver todas las rutas aprendidas para el router de borde PE4, ademas de del puerto a donde se dirige el paquete y el tiempo en la cual esta levantada la sesion.

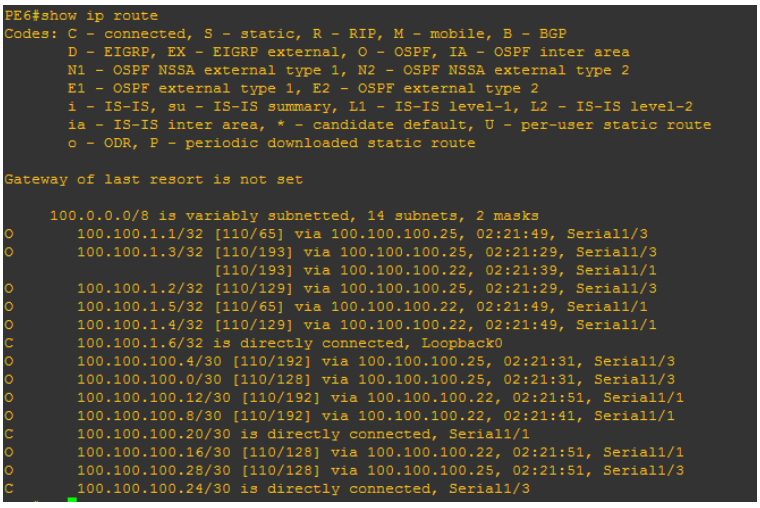
Figura 40: Revisión de tablas de enrutamiento para PE5



Fuente: Elaboración propia.

En la figura 39 podemos ver todas las rutas aprendidas para el router de borde PE5, ademas de del puerto a donde se dirige el paquete y el tiempo en la cual esta levantada la sesion.

Figura 41: Revisión de tablas de enrutamiento para PE6



Fuente: Elaboración propia.

En la figura 40 podemos ver todas las rutas aprendidas para el router de borde PE6, ademas de del puerto a donde se dirige el paquete y el tiempo en la cual esta levantada la sesion.

CONCLUSIONES

1. Frente a la red de convergencia limitada que presentaba y vulnerable a cortes de servicio y seguridad, perjudicando económicamente a la empresa. Se diseñó una simulación a escala de una red IPVPN propia, usando la tecnología MPLS logrando una red confiable y segura tanto para datos críticos y no críticos evitando así el congestionamiento de la red troncal.

2. Con la creación de una red IPVPN, se demuestra que se mejora el uso de recursos de otras sedes como servidores, archivos, base de datos, con ello tendría una mejora en cuanto a la atención de los clientes de esa manera aprovechamos el 100% del ancho de banda contratado. Tambien se logra la publicación de rutas mediante el protocolo BGP.

3. Con este diseño de red se puede aprovechar el ancho de banda al 100% ya que se maneja datos críticos como no criticas mediante políticas de calidad de servicio.

RECOMENDACIONES

1. Se recomienda utilizar la tecnología MPLS porque permite proporcionar calidad de servicio que las aplicaciones de hoy en día requieren para mejorar los recursos de la empresa, beneficiando la reducción de los tiempos de transmisión.

2. Es importante tener en cuenta la compatibilidad de procedimientos y la optimización de la tecnología de enrutamiento actual de la empresa, para establecer el mantenimiento del envío de paquetes bajo un protocolo adecuado.

- 3. Definir claramente niveles de servicio definidos con sus respectivas sanciones.

BIBLIOGRAFÍA

Cisco Systems (s. f) *Implementación de políticas de calidad de servicio (QoS) con DSCP.* Recuperado de http://www.cisco.com/cisco/web/support/LA/7 /73/ 73469_dscpvalues.html. Última fecha de consulta: 19 de julio 2016.

Acosta, H. RED IP-VPN MPLS. Administración de Servicios de Red I. 2016.Rescatado de: https://prezi.com/qirmara1r7xc/red-ip-vpn-mpls/

Barbera, J. MPLS: Una arquitectura de backbone para la Internet del siglo XXI. Congreso Mundo Internet 2000", Congreso Nacional de Usuarios de Internet e Intranet, Madrid. 2000. Rescatado de: http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1

Castro Ullauri, E. Diseño y simulación de una red MPLS para interconectar estaciones remotas utilizando el emulador GNS3. Guayaquil, 2015. Rescatado de: http://dspace.ups.edu.ec/bitstream/123456789/10297/1/UPS-GT001192.pdf

CNMC Blog. Conceptos básicos de telecos: redes de agregación y troncales. 2010. Rescatado de:

https://blog.cnmc.es/2010/04/23/conceptos-basicos-de-telecos-redes-de-agregacion-y-troncales/

Lakshman, U. MPLS Configuración en CISCO IOS Software. USA. 2005.

García Barría, C. Análisis de la Tecnología IP sobre WDM. Chile. 2006

Huidobro, J. y Millan, R. MPLS (MultiProtocol Label Switching) 2002.

Morales Dibildox, L. Investigación de Redes VPN con Tecnología MPLS. Mexico, 2006. Rescatado de: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/capitulo_3.html

Osborne, E. y Simha, A. Ingeniería de Tráfico con MPLS. CISCO, USA, 2003.

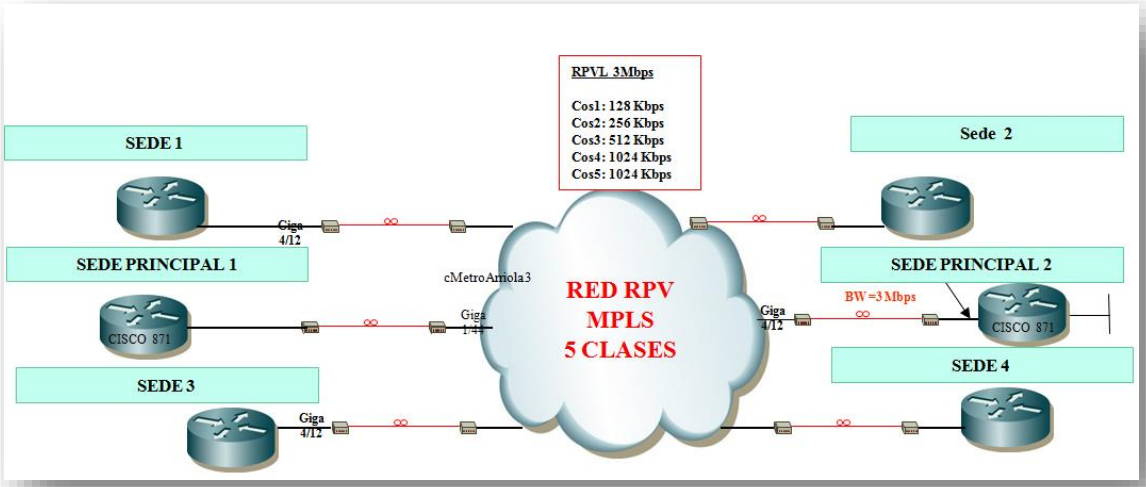
Orozco Lara, F. Diseño de una red privada virtual con tecnología MPLS para la Carrera de Ingeniería de Networking de la Universidad de Guayaquil. Guayaquil, 2014. Rescatado de: http://repositorio.ucsg.edu.ec/bitstream/3317/2198/1/T-UCSG-POS-MTEL-23.pdf

Redes de computadora. 2010. Rescatado de: http://redesdecomputadoras.es.tl/Conceptos-Basicos.htm

UAP. Fundamentos de redes y conectividad.2010. Rescatado de: http://www.uap.edu.pe/intranet/fac/material/25/20102BT250125406250107011/20102BT2501254062501070111699 7.pdf

ANEXOS

Anexo 1: Infraestructura de América Móvil



Fuente: Capacitación claro.

Anexo 2: Data-sheet router 2901

	Cisco 2901	Cisco 2911	Cisco 2921	Cisco 2951
Onboard DSP (PVDM) Slots	2	2	3	3
Memory DDR2 ECC DRAM—Default	512 MB	512 MB	512 MB	512 MB
Memory (DDR2 ECC DRAM)—Maximum	2 GB	2 GB	2 GB	2 GB
Compact Flash (External)—Default	slot 0: 256 MB slot 1: none	slot 0: 256 MB slot 1: none	slot 0: 256 MB slot 1: none	slot 0: 256 MB slot 1: none
Compact Flash (External)—Maximum	slot 0: 4 GB slot 1: 4 GB	slot 0: 4 GB slot 1: 4 GB	slot 0: 4 GB slot 1: 4 GB	slot 0: 4 GB slot 1: 4 GB
External USB 2.0 Flash Memory Slots (Type A)	2	2	2	2
USB Console Port (Type B) (up to 115.2 kbps)	1	1	1	1
Serial Console Port	1	1	1	1
Serial Auxiliary Port	1	1	1	1
Power-Supply Options	AC and PoE	AC, PoE, and DC	AC, PoE, and DC	AC, PoE, and DC
RPS Support (External)	No	Cisco RPS 2300	Cisco RPS 2300	Cisco RPS 2300
Power Specifications				
AC Input Voltage	100 to 240 VAC auto ranging	100 to 240 VAC auto ranging	100 to 240 VAC auto ranging	100 to 240 VAC auto ranging
AC Input Frequency	47 to 63 Hz	47 to 63 Hz	47 to 63 Hz	47 to 63 Hz
AC Input Current Range AC Power Supply (Maximum)	1.5 to 0.6A	2.2 to 1.0A	3.4 to 1.4A	3.4 to 1.4A
AC Input Surge Current	<50A	<50A	<50A	<50A
Typical Power (No Modules) (Watts)	40	50	60	70
Maximum Power with AC Power Supply (Watts)	150	210	320	340
Maximum Power with PoE Power Supply (Platform Only) (Watts)	175	250	370	405
Maximum End-Point PoE Power Available from PoE Power Supply (Watts)	130	200	280	370
Maximum End-Point PoE Power Capacity with PoE Boost (Watts)	N/A	750	750	750
DC Input Voltage	N/A	24 to 60 Vdc, autoranging positive or negative	24 to 60 Vdc, autoranging positive or negative	24 to 60 Vdc, autoranging positive or negative
DC Input Current	N/A	(MAX) 8A (24V) 3.5A (60V)	(MAX) 12A (24V) 5A (60V)	(MAX) 12A (24V) 5A (60V)
Physical Specifications				
Dimensions (H x W x D)	1.75 x 17.25 x 17.3 in. (44.5 x 438.2 x 439.4 mm)	3.5 x 17.25 x 12 in. (88.9 x 438.2 x 304.8 mm)	3.5 x 17.25 x 18.5 in. (88.9 x 438.2 x 469.9 mm)	3.5 x 17.25 x 18.5 in. (88.9 x 438.2 x 469.9 mm)
Rack Height	1RU (rack unit)	2RU	2RU	2RU
Rack-Mount 19 in. (48.3 cm) EIA	Included	Included	Included	Included
Rack-Mount 23 in. (58.4 cm) EIA	Optional	Optional	Optional	Optional
Wall-Mount (refer to installation guide for approved orientation)	Yes	Yes	No	No
Weight with AC Power Supply (No Modules)	13.4 lb (6.1 kg)	18 lb (8.2 kg)	29 lb (13.2 kg)	29 lb (13.2 kg)
Weight with AC PoE Power Supply (No Modules)	14.3 lb (6.5 kg)	19 lb (8.6 kg)	30 lb (13.6 kg)	30 lb (13.6 kg)
Typical Weight Fully Configured	16 lb (7.3 kg)	21 lb (9.5 kg)	34 lb (15.5 kg)	34 lb (15.5 kg)

Fuente: CISCO SYSTEM

Configuracion:

Clases de servicio para todas las sedes:

```
class-map match-any qos5
 match ip dscp cs5
 match ip dscp ef
class-map match-any qos4
 match ip dscp af41
 match ip dscp af42
 match ip dscp af43
class-map match-any qos3
 match ip dscp cs2
 match ip dscp af22
class-map match-any qos2
 match ip dscp cs1
 match ip dscp af11
 match ip dscp af13
class-map match-any P2
 match ip dscp cs1
 match ip dscp af11
 match ip dscp af13
match access-group name qos2
class-map match-any P3
 match ip dscp cs2
 match ip dscp af22
 match access-group name qos3
```

```
class-map match-any P4
 match ip dscp af41
 match ip dscp af42
 match ip dscp af43
 match access-group name qos4
class-map match-any P5
 match ip dscp cs5
 match ip dscp ef
 match access-group name qos5
!
policy-map wan
 class qos5
 police 1024000 192000 384000 conform-action transmit exceed-action drop
violate-action
drop
 priority 1024
 class qos4
 bandwidth 1024
 police 1024000 192000 384000 conform-action transmit exceed-action drop
violate-action
drop
 class qos3
 bandwidth 512
 random-detect
```

police 512000 96000 192000 conform-action transmit exceed-action set-dscp-transmit default

violate-action set-dscp-transmit default

class qos2

bandwidth 256

random-detect

police 256000 48000 96000 conform-action transmit exceed-action set-dscp-transmit default

violate-action set-dscp-transmit default

class class-default

bandwidth 128

random-detect

policy-map Shape_2944

class class-default

shape average 3072000

service-policy wan

policy-map SetDscpLan

class P5

set ip dscp cs5

class P4

set ip dscp cs3

class P3

set ip dscp cs2

class P2

set ip dscp cs1

```
 class class-default
 set ip dscp default
```

Para CE_A

```
CE_A#SHow running-config
Building configuration...

Current configuration : 2653 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE_A
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip vrf c_conce
 rd 64000:30
!
```

```
ip vrf c_contru
 rd 64000:10
!
ip vrf c_inm
 rd 64000:40
!
ip vrf c_min
 rd 64000:20
!
no ip domain lookup
archive
 log config
  hidekeys
interface Loopback1
 ip vrf forwarding c_contru
 ip address 10.0.0.1 255.255.255.0
!
interface Loopback2
 ip vrf forwarding c_min
 ip address 10.0.2.1 255.255.255.0
!
interface Loopback3
 ip vrf forwarding c_conce
 ip address 10.0.3.1 255.255.255.0
!
```

```
interface Loopback4
 ip vrf forwarding c_inm
 ip address 10.0.4.1 255.255.255.0
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding c_contru
 ip address 1.1.1.2 255.255.255.252
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip vrf forwarding c_min
 ip address 2.2.2.2 255.255.255.252
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip vrf forwarding c_conce
 ip address 3.3.3.2 255.255.255.252
!
interface FastEthernet0/0.4
```

```
 encapsulation dot1Q 4
 ip vrf forwarding c_inm
 ip address 4.4.4.2 255.255.255.252
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
```

```
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 10 vrf c_contru
 log-adjacency-changes
 capability vrf-lite
 network 1.1.1.2 0.0.0.0 area 0
 network 10.0.0.0 0.0.0.255 area 0
!
router ospf 20 vrf c_min
 log-adjacency-changes
 capability vrf-lite
 network 2.2.2.2 0.0.0.0 area 0
 network 10.0.2.0 0.0.0.255 area 0
!
router ospf 30 vrf c_conce
 log-adjacency-changes
 capability vrf-lite
 network 3.3.3.2 0.0.0.0 area 0
 network 10.0.3.0 0.0.0.255 area 0
!
router ospf 40 vrf c_inm
 log-adjacency-changes
```

```
 capability vrf-lite
 network 4.4.4.2 0.0.0.0 area 0
 network 10.0.4.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

Para PE1

```
PE1#show running-config
Building configuration...

Current configuration : 4409 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
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip vrf c_conce
 rd 64000:30
 route-target export 64000:30
 route-target import 64000:30
```

```
!
ip vrf c_contru
 rd 64000:10
 route-target export 64000:10
 route-target import 64000:10
!
ip vrf c_inm
 rd 64000:40
 route-target export 64000:40
 route-target import 64000:40
!
ip vrf c_min
 rd 64000:20
 route-target export 64000:20
 route-target import 64000:20
!
no ip domain lookup
!
multilink bundle-name authenticated
ip tcp synwait-time 5
interface Loopback0
 ip address 100.100.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
```

```
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding c_contru
 ip address 1.1.1.1 255.255.255.252
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip vrf forwarding c_min
 ip address 2.2.2.1 255.255.255.252
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip vrf forwarding c_conce
 ip address 3.3.3.1 255.255.255.252
!
interface FastEthernet0/0.4
 encapsulation dot1Q 4
 ip vrf forwarding c_inm
 ip address 4.4.4.1 255.255.255.252
!
interface FastEthernet0/1
 no ip address
```

```
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 ip address 100.100.100.29 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial1/2
 ip address 100.100.100.1 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial1/3
 ip address 100.100.100.25 255.255.255.252
 mpls label protocol ldp
 mpls ip
```

```
 serial restart-delay 0
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 10 vrf c_contru
 log-adjacency-changes
 redistribute bgp 64000 subnets
```

```
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 20 vrf c_min
 log-adjacency-changes
 redistribute bgp 64000 subnets
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 30 vrf c_conce
 log-adjacency-changes
 redistribute bgp 64000 subnets
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 40 vrf c_inm
 log-adjacency-changes
 redistribute bgp 64000 subnets
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 64000
 no synchronization
 bgp log-neighbor-changes
 neighbor 100.100.1.2 remote-as 64000
```

```
neighbor 100.100.1.2 update-source Loopback0
neighbor 100.100.1.3 remote-as 64000
neighbor 100.100.1.3 update-source Loopback0
neighbor 100.100.1.4 remote-as 64000
neighbor 100.100.1.4 update-source Loopback0
neighbor 100.100.1.5 remote-as 64000
neighbor 100.100.1.5 update-source Loopback0
neighbor 100.100.1.5 route-reflector-client
neighbor 100.100.1.6 remote-as 64000
neighbor 100.100.1.6 update-source Loopback0
neighbor 100.100.1.6 route-reflector-client
no auto-summary
!
address-family vpnv4
 neighbor 100.100.1.3 activate
 neighbor 100.100.1.3 send-community both
 neighbor 100.100.1.5 activate
 neighbor 100.100.1.5 send-community both
exit-address-family
!
address-family ipv4 vrf c_min
 redistribute connected
 redistribute ospf 20 vrf c_min
 no synchronization
exit-address-family
```

```
 !
 address-family ipv4 vrf c_inm
  redistribute connected
  redistribute ospf 40 vrf c_inm
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf c_contru
  redistribute connected
  redistribute ospf 10 vrf c_contru
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf c_conce
  redistribute connected
  redistribute ospf 30 vrf c_conce
  no synchronization
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
```

```
no cdp log mismatch duplex
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

PARA PE2

```
PE2#sh running-config
Building configuration...

Current configuration : 3316 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
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
ip vrf a_rec1
 rd 64000:50
 route-target export 64000:50
 route-target import 64000:50
!
ip vrf c_data
 rd 64000:60
 route-target export 64000:60
 route-target import 64000:60
!
no ip domain lookup
```

```
!
multilink bundle-name authenticated
archive
 log config
  hidekeys
interface Loopback0
 ip address 100.100.1.2 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding a_rec1
 ip address 13.13.13.1 255.255.255.252
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip vrf forwarding c_data
 ip address 14.14.14.1 255.255.255.252
!
interface FastEthernet0/1
 no ip address
```

```
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 ip address 100.100.100.2 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
```

```
interface Serial2/0
 ip address 100.100.100.5 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 50 vrf a_rec1
 router-id 13.13.13.1
 log-adjacency-changes
 redistribute bgp 64000 subnets
```

```
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 60 vrf c_data
 router-id 14.14.14.1
 log-adjacency-changes
 redistribute bgp 64000 subnets
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 64000
 no synchronization
 bgp log-neighbor-changes
 neighbor 100.100.1.1 remote-as 64000
 neighbor 100.100.1.1 update-source Loopback0
 neighbor 100.100.1.3 remote-as 64000
 neighbor 100.100.1.3 update-source Loopback0
 neighbor 100.100.1.3 route-reflector-client
 neighbor 100.100.1.4 remote-as 64000
 neighbor 100.100.1.4 update-source Loopback0
 neighbor 100.100.1.4 route-reflector-client
 neighbor 100.100.1.6 remote-as 64000
 neighbor 100.100.1.6 update-source Loopback0
```

```
 no auto-summary
 !
 address-family vpnv4
  neighbor 100.100.1.4 activate
  neighbor 100.100.1.4 send-community both
 exit-address-family
 !
 address-family ipv4 vrf c_data
  redistribute connected
  redistribute ospf 60 vrf c_data
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf a_rec1
  redistribute connected
  redistribute ospf 50 vrf a_rec1
  no synchronization
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
```

```
no cdp log mismatch duplex
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

PARA CE_B

```
CE_B#SHow running-config
Building configuration...

Current configuration : 1933 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

```
hostname CE_B
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip vrf a_rec1
 rd 64000:50
!
ip vrf c_data
 rd 64000:60
!
no ip domain lookup
!
multilink bundle-name authenticated
archive
 log config
  hidekeys
interface Loopback1
 ip vrf forwarding a_rec1
 ip address 10.0.13.1 255.255.255.0
```

```
!
interface Loopback2
 ip vrf forwarding c_data
 ip address 10.0.14.1 255.255.255.0
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding a_rec1
 ip address 13.13.13.2 255.255.255.252
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip vrf forwarding c_data
 ip address 14.14.14.2 255.255.255.252
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
```

```
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 50 vrf a_rec1
 log-adjacency-changes
 capability vrf-lite
 network 10.0.13.0 0.0.0.255 area 0
```

```
 network 13.13.13.2 0.0.0.0 area 0
!
router ospf 60 vrf c_data
 log-adjacency-changes
 capability vrf-lite
 network 10.0.14.0 0.0.0.255 area 0
 network 14.14.14.2 0.0.0.0 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
```

!

!

end

PARA PE_3

PE3#SH RUN

Building configuration...

Current configuration : 3135 bytes

!

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname PE3

!

boot-start-marker

boot-end-marker

no aaa new-model

memory-size iomem 5

no ip icmp rate-limit unreachable

ip cef

ip vrf c_contru

 rd 64000:10

 route-target export 64000:10

```
 route-target import 64000:10
!
ip vrf c_min
 rd 64000:20
 route-target export 64000:20
 route-target import 64000:20
!
no ip domain lookup
!
multilink bundle-name authenticated
archive
 log config
  hidekeys
ip tcp synwait-time 5
interface Loopback0
 ip address 100.100.1.3 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding c_contru
```

```
 ip address 5.5.5.1 255.255.255.252
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip vrf forwarding c_min
 ip address 6.6.6.1 255.255.255.252
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 ip address 100.100.100.9 255.255.255.252
```

```
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/0
 ip address 100.100.100.6 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
```

```
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 10 vrf c_contru
 router-id 5.5.5.1
 log-adjacency-changes
 redistribute bgp 64000 subnets
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 20 vrf c_min
 router-id 6.6.6.1
 log-adjacency-changes
 redistribute bgp 64000 subnets
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 64000
 no synchronization
 bgp log-neighbor-changes
 neighbor 100.100.1.1 remote-as 64000
```

```
 neighbor 100.100.1.1 update-source Loopback0
 neighbor 100.100.1.2 remote-as 64000
 neighbor 100.100.1.2 update-source Loopback0
 neighbor 100.100.1.4 remote-as 64000
 neighbor 100.100.1.4 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 100.100.1.1 activate
  neighbor 100.100.1.1 send-community both
 exit-address-family
 !
 address-family ipv4 vrf c_min
  redistribute connected
  redistribute ospf 20 vrf c_min
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf c_contru
  redistribute connected
  redistribute ospf 10 vrf c_contru
  no synchronization
 exit-address-family
!
ip forward-protocol nd
```

```
!
!
no ip http server
no ip http secure-server
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
CE_C
CE_C#SHow running-config
Building configuration...

Current configuration : 1921 bytes
!
version 12.4
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE_C
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip vrf c_contru
 rd 64000:10
!
ip vrf c_min
 rd 64000:20
!
no ip domain lookup
!
multilink bundle-name authenticated
archive
 log config
```

```
 hidekeys
interface Loopback1
 ip vrf forwarding c_contru
 ip address 10.0.5.1 255.255.255.0
!
interface Loopback2
 ip vrf forwarding c_min
 ip address 10.0.6.1 255.255.255.0
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding c_contru
 ip address 5.5.5.2 255.255.255.252
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip vrf forwarding c_min
 ip address 6.6.6.2 255.255.255.252
!
interface FastEthernet0/1
```

```
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
```

```
router ospf 10 vrf c_contru
 log-adjacency-changes
 capability vrf-lite
 network 5.5.5.2 0.0.0.0 area 0
 network 10.0.5.0 0.0.0.255 area 0
!
router ospf 20 vrf c_min
 log-adjacency-changes
 capability vrf-lite
 network 6.6.6.2 0.0.0.0 area 0
 network 10.0.6.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
```

```
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

PARA PE_4

```
PE4#SH running-config
Building configuration...

Current configuration : 4416 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE4
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
```

```
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip vrf a_rec1
 rd 64000:50
 route-target export 64000:50
 route-target import 64000:50
!
ip vrf c_comp
 rd 64000:80
 route-target export 64000:80
 route-target import 64000:80
!
ip vrf c_data
 rd 64000:60
 route-target export 64000:60
 route-target import 64000:60
!
ip vrf c_soft
 rd 64000:70
 route-target export 64000:70
 route-target import 64000:70
!
no ip domain lookup
!
```

```
multilink bundle-name authenticated
interface Loopback0
 ip address 100.100.1.4 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding a_rec1
 ip address 9.9.9.1 255.255.255.252
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip vrf forwarding c_data
 ip address 10.10.10.1 255.255.255.252
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip vrf forwarding c_soft
 ip address 11.11.11.1 255.255.255.252
!
interface FastEthernet0/0.4
```

```
 encapsulation dot1Q 5
 ip vrf forwarding c_comp
 ip address 12.12.12.1 255.255.255.252
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 ip address 100.100.100.13 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial1/2
 ip address 100.100.100.10 255.255.255.252
 mpls label protocol ldp
 mpls ip
```

```
 serial restart-delay 0
!
interface Serial1/3
 ip address 100.100.100.18 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
```

```
 shutdown
 serial restart-delay 0
!
router ospf 50 vrf a_rec1
 router-id 100.100.1.4
 log-adjacency-changes
 redistribute bgp 64000 subnets
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 60 vrf c_data
 router-id 100.100.1.5
 log-adjacency-changes
 redistribute bgp 64000 subnets
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 70 vrf c_soft
 router-id 100.100.1.6
 log-adjacency-changes
 redistribute bgp 64000 subnets
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 80 vrf c_comp
 router-id 100.100.1.7
 log-adjacency-changes
 redistribute bgp 64000 subnets
```

```
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 64000
 no synchronization
 bgp log-neighbor-changes
 neighbor 100.100.1.1 remote-as 64000
 neighbor 100.100.1.1 update-source Loopback0
 neighbor 100.100.1.2 remote-as 64000
 neighbor 100.100.1.2 update-source Loopback0
 neighbor 100.100.1.3 remote-as 64000
 neighbor 100.100.1.3 update-source Loopback0
 neighbor 100.100.1.5 remote-as 64000
 neighbor 100.100.1.5 update-source Loopback0
 neighbor 100.100.1.6 remote-as 64000
 neighbor 100.100.1.6 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 100.100.1.2 activate
  neighbor 100.100.1.2 send-community both
  neighbor 100.100.1.6 activate
```

```
 neighbor 100.100.1.6 send-community both
exit-address-family
!
address-family ipv4 vrf c_soft
 redistribute connected
 redistribute ospf 70 vrf c_soft
 no synchronization
exit-address-family
!
address-family ipv4 vrf c_data
 redistribute connected
 redistribute ospf 60 vrf c_data
 no synchronization
exit-address-family
!
address-family ipv4 vrf c_comp
 redistribute connected
 redistribute ospf 80 vrf c_comp
 no synchronization
exit-address-family
!
address-family ipv4 vrf a_rec1
 redistribute connected
 redistribute ospf 50 vrf a_rec1
 no synchronization
```

```
 exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
PARA CE_F
CE_F#SHow running-config
Building configuration...
```

```
Current configuration : 2673 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE_F
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip vrf a_rec1
 rd 64000:50
!
ip vrf c_comp
 rd 64000:80
!
ip vrf c_data
```

```
 rd 64000:60
!
ip vrf c_soft
 rd 64000:70
archive
 log config
  hidekeys
interface Loopback1
 ip vrf forwarding a_rec1
 ip address 10.0.9.1 255.255.255.0
!
interface Loopback2
 ip vrf forwarding c_data
 ip address 10.0.10.1 255.255.255.0
!
interface Loopback3
 ip vrf forwarding c_soft
 ip address 10.0.11.1 255.255.255.0
!
interface Loopback4
 ip vrf forwarding c_comp
 ip address 10.0.12.1 255.255.255.0
!
interface FastEthernet0/0
 no ip address
```

```
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding a_rec1
 ip address 9.9.9.2 255.255.255.252
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip vrf forwarding c_data
 ip address 10.10.10.2 255.255.255.252
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip vrf forwarding c_soft
 ip address 11.11.11.2 255.255.255.252
!
interface FastEthernet0/0.4
 encapsulation dot1Q 5
 ip vrf forwarding c_comp
 ip address 12.12.12.2 255.255.255.252
!
interface FastEthernet0/1
 no ip address
```

```
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 50 vrf a_rec1
```

```
 log-adjacency-changes
 capability vrf-lite
 network 9.9.9.2 0.0.0.0 area 0
 network 10.0.9.0 0.0.0.255 area 0
!
router ospf 60 vrf c_data
 log-adjacency-changes
 capability vrf-lite
 network 10.0.10.0 0.0.0.255 area 0
 network 10.10.10.2 0.0.0.0 area 0
!
router ospf 70 vrf c_soft
 log-adjacency-changes
 capability vrf-lite
 network 10.0.11.0 0.0.0.255 area 0
 network 11.11.11.2 0.0.0.0 area 0
!
router ospf 80 vrf c_comp
 log-adjacency-changes
 capability vrf-lite
 network 10.0.12.0 0.0.0.255 area 0
 network 12.12.12.2 0.0.0.0 area 0
!
ip forward-protocol nd
!
```

```
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
CE_F
CE_F#SHow running-config
Building configuration...

Current configuration : 2673 bytes
!
version 12.4
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CE_F
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
ip vrf a_rec1
 rd 64000:50
!
ip vrf c_comp
 rd 64000:80
!
ip vrf c_data
 rd 64000:60
!
ip vrf c_soft
```

```
 rd 64000:70
!
no ip domain lookup
!
multilink bundle-name authenticated
archive
 log config
  hidekeys
interface Loopback1
 ip vrf forwarding a_rec1
 ip address 10.0.9.1 255.255.255.0
!
interface Loopback2
 ip vrf forwarding c_data
 ip address 10.0.10.1 255.255.255.0
!
interface Loopback3
 ip vrf forwarding c_soft
 ip address 10.0.11.1 255.255.255.0
!
interface Loopback4
 ip vrf forwarding c_comp
 ip address 10.0.12.1 255.255.255.0
!
interface FastEthernet0/0
```

```
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding a_rec1
 ip address 9.9.9.2 255.255.255.252
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip vrf forwarding c_data
 ip address 10.10.10.2 255.255.255.252
!
interface FastEthernet0/0.3
 encapsulation dot1Q 3
 ip vrf forwarding c_soft
 ip address 11.11.11.2 255.255.255.252
!
interface FastEthernet0/0.4
 encapsulation dot1Q 5
 ip vrf forwarding c_comp
 ip address 12.12.12.2 255.255.255.252
!
interface FastEthernet0/1
```

```
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
```

```
router ospf 50 vrf a_rec1
 log-adjacency-changes
 capability vrf-lite
 network 9.9.9.2 0.0.0.0 area 0
 network 10.0.9.0 0.0.0.255 area 0
!
router ospf 60 vrf c_data
 log-adjacency-changes
 capability vrf-lite
 network 10.0.10.0 0.0.0.255 area 0
 network 10.10.10.2 0.0.0.0 area 0
!
router ospf 70 vrf c_soft
 log-adjacency-changes
 capability vrf-lite
 network 10.0.11.0 0.0.0.255 area 0
 network 11.11.11.2 0.0.0.0 area 0
!
router ospf 80 vrf c_comp
 log-adjacency-changes
 capability vrf-lite
 network 10.0.12.0 0.0.0.255 area 0
 network 12.12.12.2 0.0.0.0 area 0
!
ip forward-protocol nd
```

```
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

PARA PE_5

```
PE5#SHow running-config
Building configuration...

Current configuration : 3094 bytes
!
version 12.4
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
!
hostname PE5
!
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip vrf c_conce
 rd 64000:30
 route-target export 64000:30
 route-target import 64000:30
!
ip vrf c_inm
 rd 64000:40
 route-target export 64000:40
 route-target import 64000:40
!
no ip domain lookup
!
multilink bundle-name authenticated
archive
```

```
 log config
  hidekeys
ip tcp synwait-time 5
interface Loopback0
 ip address 100.100.1.5 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding c_conce
 ip address 7.7.7.1 255.255.255.252
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip vrf forwarding c_inm
 ip address 8.8.8.1 255.255.255.252
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
```

```
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 ip address 100.100.100.22 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 ip address 100.100.100.17 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial2/0
```

```
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 30 vrf c_conce
 log-adjacency-changes
 redistribute bgp 64000 subnets
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 40 vrf c_inm
```

```
 log-adjacency-changes
 redistribute bgp 64000 subnets
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 64000
 no synchronization
 bgp log-neighbor-changes
 neighbor 100.100.1.1 remote-as 64000
 neighbor 100.100.1.1 update-source Loopback0
 neighbor 100.100.1.4 remote-as 64000
 neighbor 100.100.1.4 update-source Loopback0
 neighbor 100.100.1.6 remote-as 64000
 neighbor 100.100.1.6 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 100.100.1.1 activate
  neighbor 100.100.1.1 send-community both
 exit-address-family
 !
 address-family ipv4 vrf c_inm
```

```
 redistribute connected
 redistribute ospf 40 vrf c_inm
 no synchronization
exit-address-family
!
address-family ipv4 vrf c_conce
 redistribute connected
 redistribute ospf 30 vrf c_conce
 no synchronization
exit-address-family
!
ip forward-protocol nd

no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
```

```
 logging synchronous
line vty 0 4
 login
!
!
end
```

PARA PE_2

```
P2#SHow running-config
Building configuration...

Current configuration : 1352 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
```

```
no ip icmp rate-limit unreachable
ip cef
no ip domain lookup
!
multilink bundle-name authenticated
archive
 log config
  hidekeys
ip tcp synwait-time 5
interface Loopback0
 ip address 100.100.1.8 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
```

```
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 ip address 100.100.100.14 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial1/2
 ip address 100.100.100.33 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
ip forward-protocol nd
!
!
no ip http server
```

```
no ip http secure-server
!
no cdp log mismatch duplex
control-plane
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```

PE_6

```
PE6#SHow  running-config
Building configuration...

Current configuration : 3228 bytes
!
version 12.4
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
!
hostname PE6
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
ip vrf c_comp
 rd 64000:80
 route-target export 64000:80
 route-target import 64000:80
!
ip vrf c_soft
 rd 64000:70
 route-target export 64000:70
 route-target import 64000:70
!
no ip domain lookup
!
multilink bundle-name authenticated
```

```
archive
 log config
  hidekeys
ip tcp synwait-time 5
interface Loopback0
 ip address 100.100.1.6 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip vrf forwarding c_soft
 ip address 15.15.15.1 255.255.255.252
!
interface FastEthernet0/0.2
 encapsulation dot1Q 2
 ip vrf forwarding c_comp
 ip address 16.16.16.1 255.255.255.252
!
interface FastEthernet0/1
 no ip address
 shutdown
```

```
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 ip address 100.100.100.21 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 ip address 100.100.100.26 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
```

```
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
router ospf 70 vrf c_soft
 router-id 15.15.15.1
 log-adjacency-changes
 redistribute bgp 64000 subnets
 network 0.0.0.0 255.255.255.255 area 0
```

```
!
router ospf 80 vrf c_comp
 router-id 16.16.16.1
 log-adjacency-changes
 redistribute bgp 64000 subnets
 network 0.0.0.0 255.255.255.255 area 0
!
router ospf 1
 log-adjacency-changes
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 64000
 no synchronization
 bgp log-neighbor-changes
 neighbor 100.100.1.1 remote-as 64000
 neighbor 100.100.1.1 update-source Loopback0
 neighbor 100.100.1.2 remote-as 64000
 neighbor 100.100.1.2 update-source Loopback0
 neighbor 100.100.1.4 remote-as 64000
 neighbor 100.100.1.4 update-source Loopback0
 neighbor 100.100.1.5 remote-as 64000
 neighbor 100.100.1.5 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
```

```
 neighbor 100.100.1.4 activate
 neighbor 100.100.1.4 send-community both
exit-address-family
!
address-family ipv4 vrf c_soft
 redistribute connected
 redistribute ospf 70 vrf c_soft
 no synchronization
exit-address-family
!
address-family ipv4 vrf c_comp
 redistribute connected
 redistribute ospf 80 vrf c_comp
 no synchronization
exit-address-family
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
control-plane
!
```

line con 0

 exec-timeout 0 0

 privilege level 15

 logging synchronous

line aux 0

 exec-timeout 0 0

 privilege level 15

 logging synchronous

line vty 0 4

 login

!

!

end

PARA PE_1

P1#SHow running-config

Building configuration...

Current configuration : 1352 bytes

!

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname P1

!

```
boot-start-marker
boot-end-marker
!
!
no aaa new-model
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
!
multilink bundle-name authenticated
archive
 log config
  hidekeys
ip tcp synwait-time 5
interface Loopback0
 ip address 100.100.1.7 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
```

```
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial1/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/1
 ip address 100.100.100.30 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial1/2
 ip address 100.100.100.34 255.255.255.252
 mpls label protocol ldp
 mpls ip
 serial restart-delay 0
!
interface Serial1/3
 no ip address
```

```
 shutdown
 serial restart-delay 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
no cdp log mismatch duplex
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
end
```