UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

FACULTAD DE INGENIERÍA Y ARQUITECTURA

PROYECTO DE GRADUACIÓN

UPDATING EN LA RED DE CORPORACIÓN PETROLERA MONTECRISTO

PREVIO A LA OBTENCIÓN DEL TÍTULO

INGENIERO EN TELECOMUNICACIONES

PRESENTADO POR:

21311030 MARIA FERNANDA HERNÁNDEZ GÓMEZ

ASESOR: ING. LUIS ALONZO MILIAN

CAMPUS SAN PEDRO SULA

ABRIL DE 2018

RESUMEN EJECUTIVO

La empresa COPEMSA es una de las grandes distribuidoras de hidrocarburos en el país, dicha empresa cuenta actualmente con 14 sucursales en diferentes zonas del territorio nacional. Al brindar diferentes servicios en sus localidades, y con la necesidad de mantenerse en comunicación se instaló una red en la cual se incluye cada una de sus sucursales. Dicha instalación se dio 10 años atrás por la empresa Cable and Wireless Business.

La red ha estado funcionando desde entonces de forma estable, pero el equipo que fue previamente instalado ha ido quedando obsoleto, dado a que cada año podemos encontrar en el mercado opciones más modernas que agilizan los procesos. Es por eso que se decidió hacer un "Update" en la red lo cual nos llevó a tener una comunicación más beneficiosa. Esto se mejoró instalando una serie actualizada de routers que nos permitió tener una notable mejora en la transferencia de datos. Y debido a que además de hacerse un reemplazo de routers se integró en ellos protocolos que proporcionarán mejoras notables en la red.

Todo se llevó a cabo por la empresa Cable and Wireless Business líderes en soluciones de telecomunicaciones a nivel global, quienes tienen la red de fibra óptica más grande y confiable de Honduras. Gracias a su servicio de permanente monitoreo sobre la red, podremos tener una pronta respuesta de parte del equipo de técnicos expertos en caso de haber una falla sobre la nueva integración.

ÍNDICE DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

I. PLANTEAMIENTO DE LA INVESTIGACIÓN

1.1 INTRODUCCION

En la última década con el avance de la tecnología, el Internet y las telecomunicaciones han hecho que las grandes empresas e incluso las pymes se adapten al plan de modernización. En la actualidad dichas empresas quieren expandir sus mercados, por ellos se ubican en puntos estratégicos a través del país, a partir de ellos se vislumbra la necesidad de poder mantener una comunicación segura, confiable, rápida y lo que es aún más importante a un costo accesible entre todos las sucursales de una misma empresa con el fin de compartir entre ellas información de suma importancia.

Ante este problema existen soluciones que permiten la comunicación entre dichas sucursales; siendo la herramienta más utiliza actualmente, el uso del Internet, pero esta no siempre brinda el nivel de seguridad que una empresa requiere. Además, se pueden adquirir servicios dedicados a conexión entre locales a un proveedor, pero esto requiere de un alto costo económico ya que se incrementa por las variables de número de sucursales y distancia entre ellos mismos, por lo consiguiente para mantener una comunicación segura, confiable, rápida y a un precio totalmente accesible, es necesario buscar nuevas alternativas de intercomunicación que cumpla con las características mencionadas.

Una solución viable es la del uso de una red MPLS (Multiprotocol Label Switching) en la cual también pueden integrar protocolos que requiera la red . Sin embargo, realizar esto requiere de un conocimiento avanzado en la configuración de equipo, ya que podría resultar un problema para un usuario en general si deseara realizarlo por su cuenta. Por lo cual a la empresa C&W se la ha sido asignado este proyecto, para realizar las configuraciones correspondientes.

El presente estudio muestra el desarrollo e implementación de una red VPN MPLS, usando la tecnología IOS de Cisco, y realizando dicho proyecto a la empresa nacional de comercialización de hidrocarburos COPEMSA (Coorporacion Petrolera Montecristo S.A de C.V.).

1.2 ANTECEDENTES DEL PROBLEMA

Actualmente, COPEMSA cuenta con 14 sucursales a nivel nacional, cada una tiene su propia estructura de red implementado hace 10 años por la empresa C&W, a dicha red no se le había solicitado un mantenimiento ni mucho menos una renovación de equipo. Antes de solicitarse este proyecto, la empresa se vio afectada al no recibir el ancho de banda que se estaba costeando, nuestro equipo hizo las pruebas correspondientes y como resultado se obtuvo que el ancho de banda que se estaba proporcionando era el mismo que había sido solicitado. A base de ello, se estableció que el equipo previamente instalado necesitaba ser renovado porque este estaba quedando obsoleto e inutilizable para el ancho de banda que COPEMSA está requiriendo.

1.3 DEFICIÓN DEL PROBLEMA

La Corporación Petrolera Montecristo, la cual es parte del grupo Montecristo, comercializa hidrocarburos en diferentes localidades del país, entre ellos se encuentran: La Ceiba, Puerto Cortes, La Lima, Choloma, Danlí, Tegucigalpa y San Pedro Sula, cuenta con 14 sucursales y todas ellas son parte de la red petrolera TEXACO (Texas Petrolum Company). Teniendo una distribución tan amplia en el país, una red VPN ya había sido instalada previamente por la empresa Cable and Wireless, pero debido a ciertos inconvenientes que se estaban presentando se decidió cambiar el equipo que ya está quedando obsoleto, por routers Cisco C891-K9, en dicha red también se incluirá la conmutación de etiquetas multiprotocolo (MPLS) para poder transportar los diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

1.4 OBJETIVOS DEL PROYECTO

1.4.1 Objetivo General

Hacer la renovación de equipo correspondiente a las sucursales en la zona norte del país, siempre conservándose el concepto de una red VPN y de que el equipo siga siendo de la fiable marca Cisco, para que COPEMSA obtenga como beneficio el recibimiento de la totalidad de ancho de banda que está costeando.

1.4.2 Objetivos Específicos

- Configuración e instalación de nuevo router.
- Pruebas RFC254.
- Integración de protocolo BGP.

1.5 HIPOTESIS Y VARIABLES DE LA INVESTIGACIÓN

Poder demostrar la eficiencia de nuestro servicio e implementar una mejora a la red de COPEMSA mediante la renovación de un equipo que proporciona casi el doble de transferencia de datos en comparación al equipo previamente instalado, dejando así, no solo una red más eficiente, sino garantizar que se mantendrá una red totalmente estable.

Como variables de investigación para el proyecto se incluirá el funcionamiento de una red VPN en MPLS y la integración del protocolo BGP en ella.

1.6 JUSTIFICACIÓN

Cable and Wireless Business, como una empresa responsable, líder en el campo de las telecomunicaciones y siempre a la vanguardia de las nuevas tecnologías, tiende a buscar los mejores métodos, hardware y protocolos en la infraestructura de redes. COPEMSA, ha decidido que esta es la empresa más conveniente para poder tener un servicio fiable debido a su estructura tan amplia a través del país, y ha decidido renovar el contrato con C&W Business confiando en que se dará una renovación exitosa del equipo técnico.

II. MARCO TEÓRICO

2.1 Modelo de referencia OSI

El modelo OSI se muestra en la figura (sin el medio físico). Este modelo está basado en una propuesta desarrollada por la ISO (Organización Internacional de Estándares) como un primer paso hacia la estandarización internacional de los protocolos utilizados en varias capas (Day y Zimmermann, 1983). Fue revisado en 1995 (Day, 1995). El modelo se llama OSI (Interconexión de Sistemas Abiertos) de ISO porque tiene que ver con la conexión de sistemas abiertos, es decir, sistemas que están abiertos a la comunicación con otros sistemas.

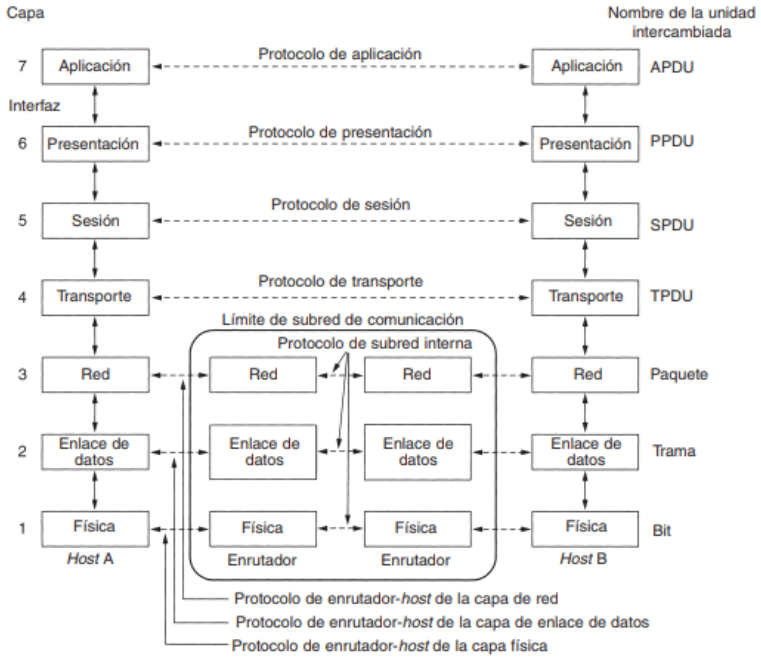


Ilustración 1. Modelo de Referencia OSI.

El modelo OSI tiene siete capas. (Tanenbaum, 2003, p.38) Resume brevemente los principios que se aplicaron para llegar a dichas capas:

1. Una capa se debe crear donde se necesite una abstracción diferente.

2. Cada capa debe realizar una función bien definida.

3. La función de cada capa se debe elegir con la intención de definir protocolos estandarizados internacionalmente.

4. Los límites de las capas se deben elegir a fin de minimizar el flujo de información a través de las interfaces.

5. La cantidad de capas debe ser suficientemente grande para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

A continuación analizaremos una por una cada capa del modelo, comenzando con la capa inferior.

2.2 La Capa Física

La capa física (capa 1) de OSI proporciona los medios de transporte para los bits que conforman la trama de la capa de Enlace de datos a través de los medios de red. Esta capa acepta una trama completa desde la capa de Enlace de datos y lo codifica como una secuencia de señales que se transmiten en los medios locales. Un dispositivo final o un dispositivo intermedio reciben los bits codificados que componen una trama. El envío de tramas a través de medios de transmisión requiere los siguientes elementos de la capa física:

- Medios físicos y conectores asociados.
- Una representación de los bits en los medios.
- Codificación de los datos y de la información de control.
- Sistema de circuitos del receptor y transmisor en los dispositivos de red.

En este momento del proceso de comunicación, la capa de transporte ha segmentado los datos del usuario, la capa de red los ha colocado en paquetes y luego la capa de enlace de datos los ha encapsulado como tramas. El objetivo de la capa física es crear la señal óptica, eléctrica o de microondas que representa a los bits en cada trama. Luego, estas señales se envían por los medios una a la vez. Otra función de la capa física es la de recuperar estas señales individuales desde los medios, restaurarlas para sus representaciones de bit y enviar los bits hacia la capa de Enlace de datos como una trama completa. (Gibson, 2011, p. 46)

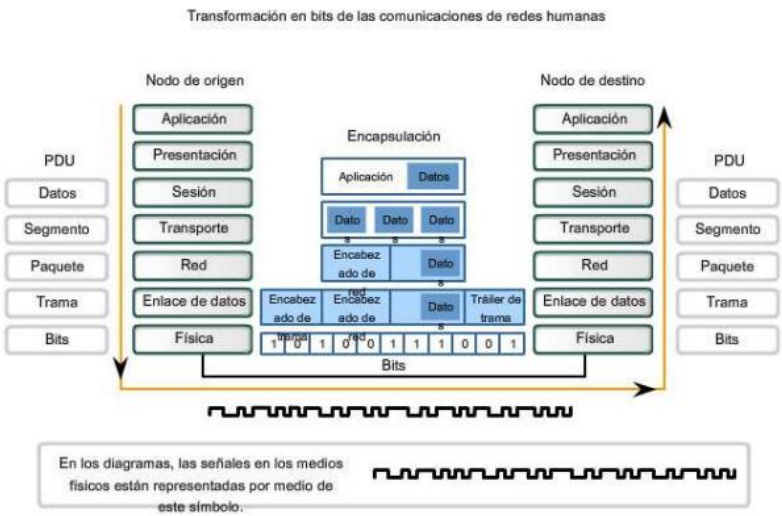


Ilustración 2. Señales en bits de capa física.

2.3 La Capa de Enlace de Datos

La capa de Enlace de Datos (capa 2) es responsable de convertir el identificador lógico (en el caso de la tecnología TCP/IP, una dirección IP) a un identificador físico. El tipo específico de identificador de Enlace de Datos depende del protocolo de Enlace de datos que se esté utilizando. Para Ethernet, se utilizan las direcciones MAC.

La capa de Enlace de datos tiene un número de funciones específicas que debe cumplir. Estas funciones incluyen brindar una interfaz de servicio bien definida a la capa de red, determinar cómo los bits de la capa física son agrupados en tramas o secuencias, hacer frente a los errores de transmisión y regular el flujo o las tramas para que los receptores lentos no sean abrumados por remitentes rápidos. (Shinde, 2009, p. 170)

Las tecnologías LAN existen principalmente en las capas de Enlace de Datos y Física de la arquitectura. Las funciones cumplidas por un puente de red o un switch ocurren principalmente en la capa de Enlace de Datos. Los switches de red son capaces de mejorar tremendamente las capacidades ofrecidas por la capa de Enlace de Datos. Esto es cierto hasta el punto en que se tiene que ser cuidadoso para que la implementación de sus funciones no afecte las operaciones de algunos protocolos que se encuentran en las capas superiores.

Para poder manejar las solicitudes de servicio de la red, la capa de Enlace de Datos está dividida en dos sub capas. (Murthy, 2010, p. 61)nos lo explica de la siguiente manera:

Una tarea importante de la capa 2 es solucionar los problemas causados por tramas de mensajes dañadas, pérdidas o duplicadas para que las capas subsecuentes estén resguardadas de errores de transmisión. La capa 1 ignora completamente los errores, admite y transmite un stream continúo de bits sin saber el significado o la estructura. La capa de Enlace de Datos debe estar alerta para realizar este trabajo. (p. 61)

2.3.1 Sub capa LLC

Logical Link Control (Control de Enlaces Lógico) es un protocolo desarrollado por la IEEE 802.2, y brinda 3 clases de servicio.

- **LLC-1** – Utilizado para servicios sin conexión.
- **LLC-2** – Utilizado para servicios orientados a conexión.
- **LLC-3** – Utilizado para reconocimientos en conjunto con servicios sin conexión.

LLC interactúa directamente con la capa de Red. LLC provee un control de flujo y un control de error y le permite a múltiples protocolos trabajar simultáneamente (Gibson, 2011).

2.3.2 Sub capa MAC

La sub capa MAC es responsable de crear una interfaz entre la sub capa LLC y la capa1, la capa Física. La sub capa MAC brinda control de acceso como también direccionamiento para la unidad de datos de protocolo (PDU). Esta sub capa es lo que hace que la comunicación multipunto con una LAN/WAN sea una realidad. Esta sub capa también es capaz de operar como un canal lógico full-dúplex en una LAN. Este canal lógico soporta los servicios unicast, multicast, y broadcast.

Gibson (2011) nos dice que la dirección MAC es representada con 12 caracteres hexadecimales (o 6 pares de caracteres hexadecimales). Cuatro bits representan cada carácter hexadecimal. Cuatro bits multiplicados por 12 caracteres nos indica que la dirección MAC tiene 48 bits de longitud. Cada dispositivo en una red tiene una dirección MAC diferente. Si las direcciones MAC en la red no son únicas, las computadoras con la misma

dirección MAC no se pueden comunicar en la red. La tabla 2 nos muestra como son asignadas las direcciones MAC.

Identificador Único de la Organización	**Número de Serie del Fabricante**
AA-BA-DB	FA-60-AD
Seis caracteres hexadecimales (24 bits)	Seis Caracteres Hexadecimales (24 bits)

Tabla 1. Asignación de direcciones MAC.

2.3.3 Etiquetado de Capa de Enlace de Datos

Al igual que todas las otras capas superiores, la capa de Enlace de Datos también agrega su propio encabezado con direccionamiento (en este caso la dirección MAC) a los datos, ignorando los datos específicos agregados como encabezado por las capas 3-7. Sin embargo, a diferencia de las demás capas, la capa de Enlace de datos también agrega algo al final del paquete, conocido como tráiler. El tráiler contiene información relacionada matemáticamente con los datos (toda la información de la capa 3-7) de tal manera que el dispositivo de destino pueda llevar a cabo un chequeo cíclico de redundancia (CRC).

2.4 La Capa de Red

La Capa de Red (Capa 3) controla las operaciones de la subred. Un aspecto clave del diseño es determinar cómo se enrutan los paquetes desde su origen a su destino. Las rutas pueden estar basadas en tablas estáticas (enrutamiento estático) codificadas en la red y que rara vez cambian.

Si hay demasiados paquetes en la subred al mismo tiempo, se interpondrán en el camino unos y otros, lo que provocará que se formen cuellos de botella. La responsabilidad de controlar esta congestión también pertenece a la capa de red, aunque esta responsabilidad también puede ser compartida por la capa de transmisión. De manera más general, la calidad del servicio proporcionado (retardo, tiempo de tránsito, inestabilidad, etcétera) también

corresponde a la capa de red. Cuando un paquete tiene que viajar de una red a otra para llegar a su destino, pueden surgir muchos problemas. El direccionamiento utilizado por la segunda red podría ser diferente del de la primera.

La segunda podría no aceptar todo el paquete porque es demasiado largo. Los protocolos podrían ser diferentes, etcétera. La capa de red tiene que resolver todos estos problemas para que las redes heterogéneas se interconecten. En las redes de difusión, el problema de enrutamiento es simple, por lo que la capa de red a veces es delgada o, en ocasiones, ni siquiera existe. (Tanenbaum, 2003, p. 40).

2.5 La Capa de Transporte

La función básica de la capa de transporte (Capa 4) capa es aceptar los datos provenientes de las capas superiores, dividirlos en unidades más pequeñas si es necesario, pasar éstas a la capa de red y asegurarse de que todas las piezas lleguen correctamente al otro extremo. Además, todo esto se debe hacer con eficiencia y de manera que aísle a las capas superiores de los cambios inevitables en la tecnología del hardware. La capa de transporte también determina qué tipo de servicio proporcionar a la capa de sesión y, finalmente, a los usuarios de la red. El tipo de conexión de transporte más popular es un canal punto a punto libre de errores que entrega mensajes o bytes en el orden en que se enviaron. Sin embargo, otros tipos de servicio de transporte posibles son la transportación de mensajes aislados, que no garantiza el orden de entrega, y la difusión de mensajes a múltiples destinos. El tipo de servicio se determina cuando se establece la conexión.

La función básica de esta capa es aceptar los datos provenientes de las capas superiores, dividirlos en unidades más pequeñas si es necesario, pasar éstas a la capa de red y asegurarse de que todas las piezas lleguen correctamente al otro extremo. Además, todo esto se debe hacer con eficiencia y de manera que aísle a las capas superiores de los cambios inevitables en la tecnología del hardware (Tanenbaum, 2003, p. 41). La capa de transporte también determina qué tipo de servicio proporcionar a la capa de sesión y, finalmente, a los usuarios de la red. El tipo de conexión de transporte más popular es un canal punto a punto libre de errores que entrega mensajes o bytes en el orden en que se enviaron. Sin embargo, otros tipos de servicio de transporte posibles son la transportación de mensajes aislados,

que no garantiza el orden de entrega, y la difusión de mensajes a múltiples destinos. El tipo de servicio se determina cuando se establece la conexión.

2.6 La Capa de Sesión

Ariganello (2013) nos dice que esta capa permite que los usuarios de máquinas diferentes establezcan sesiones entre ellos. Las sesiones ofrecen varios servicios, como el control de diálogo (dar seguimiento de a quién le toca transmitir), administración de token (que impide que las dos partes traten de realizar la misma operación crítica al mismo tiempo) y sincronización (la adición de puntos de referencia a transmisiones largas para permitirles continuar desde donde se encontraban después de una caída).

2.7 La Capa de Presentación

La capa de presentación (Capa 6) a diferencia de las capas inferiores, a las que les corresponde principalmente mover bits, a la capa de presentación le corresponde la sintaxis y la semántica de la información transmitida. A fin de que las computadoras con diferentes representaciones de datos se puedan comunicar, las estructuras de datos que se intercambiarán se pueden definir de una manera abstracta, junto con una codificación estándar para su uso "en el cable". La capa de presentación maneja estas estructuras de datos abstractas y permite definir e intercambiar estructuras de datos de un nivel más alto (por ejemplo, registros bancarios) (Tanenbaum, 2003, p. 42).

2.8 La Capa de Aplicación

La capa de aplicación (Capa 7) contiene varios protocolos que los usuarios requieren con frecuencia. Un protocolo de aplicación de amplio uso es HTTP (Protocolo de Transferencia de Hipertexto), que es la base de World Wide Web. Cuando un navegador desea una página Web, utiliza este protocolo para enviar al servidor el nombre de dicha página. A continuación, el servidor devuelve la página. Otros protocolos de aplicación se utilizan para la transferencia de archivos, correo electrónico y noticias.

(Murthy, 2010, p. 67) la define como un software de aplicación utilizado por el usuario de red para accesar a la red. Con este software, el usuario define que mensajes serán enviados por la red. Su propósito principal es brindar un conjunto de variables configurables para programas de aplicación (el programa del usuario determina el conjunto de mensajes y

cualquier acción que se llevará a cabo después de recibir un mensaje). Le provee interfaces al usuario y soporte de servicios (correo electrónico, acceso a archivos remotos y transferencia de los mismos, servicios de información distribuida, administración de bases de datos compartida). Incluye las estadísticas de administración de red, arranque y terminación de sistemas remotos, monitoreo de red, diagnósticos de aplicación, hace que la red sea transparente a los usuarios, permite compartir procesadores simples entre computadoras host, uso de bases de datos distribuidas, protocolos específicos de la industria, etc.

La ilustración muestra como el usuario de red puede tener múltiples servicios activos al mismo tiempo, el servicio se le presenta al usuario en la forma de una aplicación, y es a través de esta aplicación que se envían y se reciben los datos entre el usuario y la red.

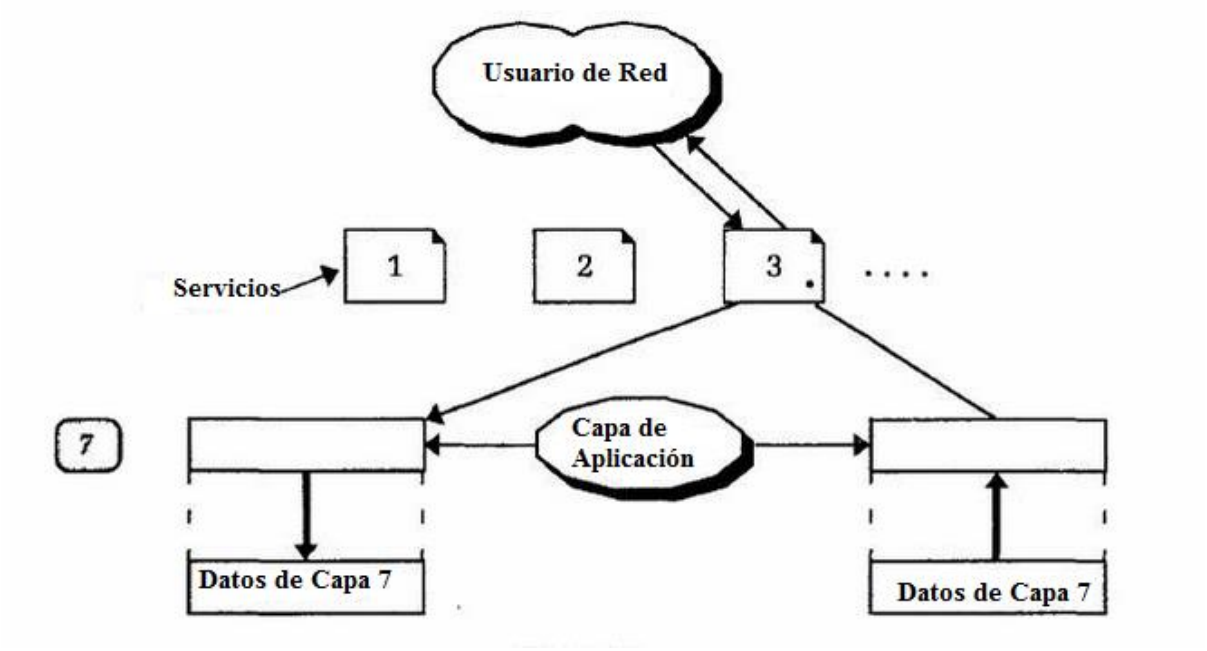


Ilustración 3. Usuario de red con múltiples servicios activos.

3.1 Direccionamiento IP

Una dirección IP es un direccionamiento usado para identificar únicamente un dispositivo en una red del IP. El direccionamiento se compone de 32 bits binarios, que pueden ser divisibles en una porción de la red y recibir la porción con la ayuda de una máscara de subred. Los 32 bits binarios se dividen en cuatro octetos (1 octeto = 8 bits). Cada octeto se convierte a decimal y se separa con un punto. Por esta razón, se dice que una dirección IP se expresa en formato decimal con puntos (por ejemplo, 172.16.81.100). El valor en cada octeto posee un rango decimal de 0 a 255 o binario de 00000000 a 11111111.

He aquí cómo se convierten los octetos binarios a decimal: La derecha la mayoría del bit, o bit menos significativo, de un octeto lleva a cabo un valor de 20. El bit apenas a la izquierda de ése lleva a cabo un valor de 21. Esto continúa hasta el bit más a la izquierda, o el bit más significativo, que lleva a cabo un valor de 27. Por lo tanto, si todos los bits son un uno, el equivalente decimal sería 255 como se muestra aquí:

```
   1  1  1  1 1 1 1 1
128 64 32 16 8 4 2 1 (128+64+32+16+8+4+2+1=255)
```

He aquí una conversión de octeto de ejemplo cuando no todos los bits están establecidos en 1.

```
0  1 0 0 0 0 0 1
0 64 0 0 0 0 0 1 (0+64+0+0+0+0+0+1=65)
```

Y esta muestra muestra una dirección IP representada en el binario y el decimal.

```
       10.       1.      23.      19 (decimal)
00001010.00000001.00010111.00010011 (binary)
```

Estos octetos se dividen para proporcionar un esquema de direccionamiento que puede adaptarse a redes pequeñas y grandes. Hay cinco clases diferentes de redes, A a E. Este documento se centra en las clases A al C, puesto que las clases D y E son reservadas y la discusión de ellas está fuera del alcance de este documento.

Dado un IP Address, su clase se puede determinar de los tres bits de orden alto (los tres bits más a la izquierda en el primer octeto). La Figura muestra la significación de los tres bits de orden superior y el rango de direcciones que caen en cada clase. Para propósitos informativos, también se muestran direcciones de Clase D y Clase E.

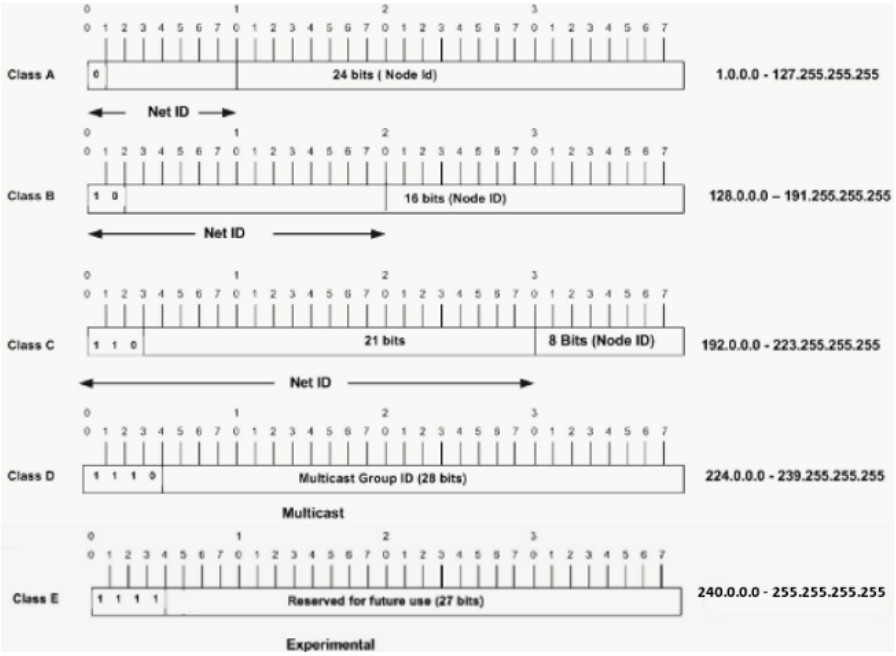


Ilustración 4. Direcciones de las diferentes clases

En una dirección de Clase A, el primer octeto es la parte de la red, así que el ejemplo de Clase A en la Figura tiene una dirección de red principal de 1.0.0.0 - 127.255.255.255. Los octetos 2,3, y 4 (los 24 bits siguientes) son para que el administrador de la red divida en subredes y hosts como estime conveniente. Las direcciones de Clase A se utilizan para redes que tienen más de 65.536 hosts (en realidad,¡ hasta 16.777.214 hosts!).

En una dirección de Clase B, los dos primeros octetos son la parte de la red, así que el ejemplo de Clase B en la Figura tiene una dirección de red principal de 128.0.0.0 - 191.255.255.255. Los octetos 3 y 4 (16 bits) son para subredes locales y hosts. Las direcciones de clase B se utilizan para redes que tienen entre 256 y 65534 hosts.

En una dirección de la Clase C, los tres primeros octetos son la parte de la red. El ejemplo del C de la clase en el cuadro tiene una dirección de red principal de 192.0.0.0 - 223.255.255.255. El octeto 4 (8 bits) es para subredes locales y hosts, perfecto para redes con menos de 254 hosts.

3.2 Mascara de Red

Una máscara de red ayuda a saber qué parte de la dirección identifica la red y qué parte de la dirección identifica el nodo. Las redes de la clase A, B, y C tienen máscaras predeterminadas, también conocidas como máscaras naturales, como se muestra aquí:

```
Class A: 255.0.0.0
Class B: 255.255.0.0
Class C: 255.255.255.0
```

Una dirección IP de una red de la Clase A que no se haya convertido en subred tendrá un par dirección/máscara similar a: 8.20.15.1 255.0.0.0. Para ver cómo la máscara le ayuda a identificar a las partes de la red y del nodo el direccionamiento, convierta el direccionamiento y la máscara a los números binarios.

```
8.20.15.1 = 00001000.00010100.00001111.00000001
255.0.0.0 = 11111111.00000000.00000000.00000000
```

Una vez que usted hace el direccionamiento y la máscara representar en el binario, después la identificación de la red y del ID del host es más fácil. Cualquier bit de dirección que tenga el bit de máscara correspondiente establecido en 1 representa la identificación de red. Cualquier bit de dirección que tenga el bit de máscara correspondiente establecido en 0 representa la identificación de nodo.

```
8.20.15.1 = 00001000.00010100.00001111.00000001
255.0.0.0 = 11111111.00000000.00000000.00000000
            ----------------------------------
             net id |      host id


netid =  00001000 = 8
hostid = 00010100.00001111.00000001 = 20.15.1
```

4.1 Redes

Una red de datos es un grupo de dispositivos finales conectados el uno al otro a través de caminos de comunicación, como también los estándares que permiten la comunicación. Una red se puede conectar a otras redes, permitiendo así una comunicación virtualmente global entre dos puntos. Muchas redes comparten información entre sí, creando así redes más grandes.

Una red es un sistema que permite que exista comunicación entre dos personas o dispositivos finales. En el mundo de las redes de computadoras, las reglas para la comunicación deben estar bien definidas. Las computadoras que se están comunicando deben conocer las reglas, para que así como dos personas hablando el mismo idioma, se puedan comunicar sin retraso (Ciccarelli & Faulkner, 2006) Si las computadoras no se entienden entre sí, no se logra nada; no hay acceso a internet, no se pueden compartir ni imprimir archivos; y todo el trabajo se detiene.

Muchas cosas pueden ser compartidas en una red. Los negocios corporativos se conducen casi exclusivamente en la red. Las redes le permiten a los usuarios compartir aplicaciones que están almacenadas en servidores en la red (aplicaciones de correo electrónico, aplicaciones de procesamiento de palabras, bases de datos, y muchas otras). Permiten la comunicación entre dispositivos finales. Los datos pueden ser compartidos entre compañías o individuos para propósitos de negocios o personales. Muchas páginas web brindan oportunidades que no hubiesen existido si las redes nunca hubieran sido implementadas. Sin mencionar como una red permite compartir archivos. Las posibilidades son infinitas, y se puede estar seguro de que alguien está trabajando en un nuevo sistema innovador.

Las redes pueden variar en su tamaño. Thakur (2010) indica que una red puede ser vasta, abarcando cientos de computadoras y regada a lo largo de continentes; puede unir ordenadores centrales, mini y micro computadoras, impresoras, máquinas de fax y buscadores; sus usuarios pueden ser un conjunto de entusiastas individuales o compañías enteras; o la red puede consistir de no más de dos máquinas, unidas con el único propósito de compartir una impresora o un disco duro. Hoy en día, muchos otros dispositivos se

pueden conectar a la red, incluyendo televisiones interactivas, teléfonos inteligentes, y sistemas de navegación.

4.1.1 Componentes de Red

Las redes modernas pueden incluir muchos componentes. Algunos de los componentes más básicos son los dispositivos finales, los routers y los switches. Los routers son utilizados en la red para transferir información entre las computadoras que no están en la misma red. Los routers son capaces de hacer esto porque mantienen una tabla de todas las redes y las rutas (direcciones) utilizadas para localizar esas redes. Los switches vienen en dos variedades. Los switches de capa 2 simplemente conectan computadoras o dispositivos finales que se encuentran en la misma red. Asimismo, los switches de capa 3 tienen esta característica, pero también son capaces de actuar como routers.

4.1.2 Switches

Los switches son dispositivos de capa 2 que cumplen con la función básica de unir segmentos de red dentro de la LAN. Los switches son distribuidos en varias ubicaciones en una red. Los switches son capaces de determinar el mejor camino hacia un segmento de red a través del Spanning Tree Protocol (STP). STP le permite a la red ser diseñada para que incluya enlaces redundantes, lo cual asegura que los datos llegarán a su destino si el enlace principal falla. STP también se asegura de que no haya ningún loop en la red, el cual se puede configurar accidentalmente con la suma de enlaces redundantes. STP ha tenido muchas mejoras en los últimos años. En la ilustración 6 se muesta un switch Cisco.

***Ilustración 5*. Switch marca CISCO**

4.1.3 Routers

Los routers hacen que sea posible que nuestros correos electrónicos lleguen a su destino. Toman las decisiones necesarias para lograr que los datos viaje de un usuario al otro. Sería virtualmente imposible cumplir con las demandas de los usuarios de hoy en día sin un router de por medio, ayudando a tomar decisiones de cómo hacer llegar los datos del punto A al punto B. Los routers son nodos de red avanzados que conectan redes de diferentes tipos. Los routers son lo suficientemente inteligentes como para hacer llegar datos de una red con una topología a otra red con una topología diferente sin ningún tipo de corrupción. En la ilustración 7 se muestra un router marca Cisco.

Ilustración 6. Routers marca cisco

5.1 Tipos de Redes

A continuación se describen los tipos de redes existentes:

5.1.1 Red PAN (Personal Area Network)

Es el sistema más básico que se utiliza para espacios reducidos en donde la distancia entre equipos es de pocos metros. Aunque puede hacerse la instalación con cable, normalmente se recurre a un sistema de red inalámbrico mediante un router que permite conectar unos pocos equipos.

5.1.2 Red LAN (Local Area Network)

Es la más conocida y la que más se instala en las empresas independientemente de si es un edificio o una oficina con varias dependencias. Su cobertura abarca desde los 200 metros a 1 kilómetro y a ella se pueden conectar ordenadores y todo tipo de periféricos (escáneres, fotocopiadoras, etc.) para que todos los trabajadores puedan intercambiar informaciones y órdenes.

5.1.3 Red WLAN (Wireless Local Area Network)

Podríamos decir que es una variante de la red LAN, pero en este caso emplea medios inalámbricos de conexión. Es una configuración que cada vez se utiliza más porque no requiere la instalación de cables y además es escalable, es decir, puede adaptarse a nuevas necesidades sin perder un ápice la calidad.

5.1.4 Red CAN (Campus Área Network)

Esta es la modalidad que se utiliza cuando, por ejemplo, tenemos varios edificios y tenemos que dar cobertura a más de 1 kilómetro. En estos casos, se interconectan varias redes locales que están instaladas en lugares concretos a una red inalámbrica para que se puedan compartir datos e información.

5.1.5 Red MAN (Metropolitan Area Network)

Abarca espacios mucho más amplios que la anterior y es la que suelen utilizar las ciudades para crear zonas Wifi de acceso gratuito.

5.1.6 Red VLAN

Si las redes descritas hasta ahora habitualmente se conectan de forma física, una VLAN lo hace de forma lógica, es decir, mediante puertos, protocolos, etc. En el caso de que una empresa tenga diferentes departamentos y quiera que operen de manera separada, sería la red más aconsejable. Además mejora la seguridad y el rendimiento.

5.1.7 Red WAN (World Area Network)

Son las que suelen desplegar las empresas proveedoras de Internet para dar cobertura de conexión para zonas muy amplias, como una ciudad o país.

5.1.8 Red VLAN (Virtual Local Area Network)

Las redes habituales (LAN) se conectan de forma física. Las redes VLAN se conectan de forma lógica (mediante protocolos, puertos, etc.), reduciendo el tráfico de red y mejorando la seguridad. Si una empresa tiene varios departamentos y quieren que funcionen en redes separadas, simplemente crea varias VLAN y separa el tráfico virtualmente.

6.1 Topologías de la Red

La topología de una red es el arreglo físico o lógico en el cual los dispositivos o nodos de una red (computadoras, impresoras, servidores, hubs, switches, enrutadores, etc.) se interconectan entre sí sobre un medio de comunicación.

- *Topología física*: Se refiere al diseño actual del medio de transmisión de la red.
- *Topología lógica*: Se refiere a la trayectoria lógica que una señal a su paso por los nodos de la red.

Existen varias topologías de red básicas (ducto, estrella, anillo y malla), pero también existen redes híbridas que combinan una o más de las topologías anteriores en una misma red.

6.1.1Topología de ducto

Una topología de ducto o bus está caracterizada por una dorsal principal con dispositivos de red interconectados a lo largo de la dorsal. Las redes de ductos son consideradas como topologías pasivas. Las computadoras "escuchan" al ducto. Cuando éstas están listas para transmitir, ellas se aseguran que no haya nadie más transmitiendo en el ducto, y entonces ellas envían sus paquetes de información. Las redes de ducto basadas en contención (ya que cada computadora debe contender por un tiempo de transmisión) típicamente emplean la arquitectura de red ETHERNET.

Las redes de bus comúnmente utilizaban cable coaxial como medio de comunicación, las computadoras se contaban al ducto mediante un conector BNC en forma de T. En el extremo de la red se ponía un terminador (si se utilizaba un cable de 50 ohm, se ponía un terminador de 50 ohms también). Eran muy susceptibles a quebraduras de cable coaxial, conectores y

cortos en el cable que son muy difíciles de encontrar. Un problema físico en la red, tal como un conector T, puede desconectar toda la red.

Con la entrada del cable par trenzado, la topología de ducto fue un poco más robusta, pero seguía existiendo la contención para accesar al cable dorsal. Ese problema de colisiones se redujo al segmentar las redes en pocos nodos. A pesar de ese problema la topología de ducto con Ethernet es la más utilizada para redes de área local (LAN).
En ambientes MAN (Metropolitan Area Network), las compañías de televisión por cable utilizan esta topología para extender sus redes.

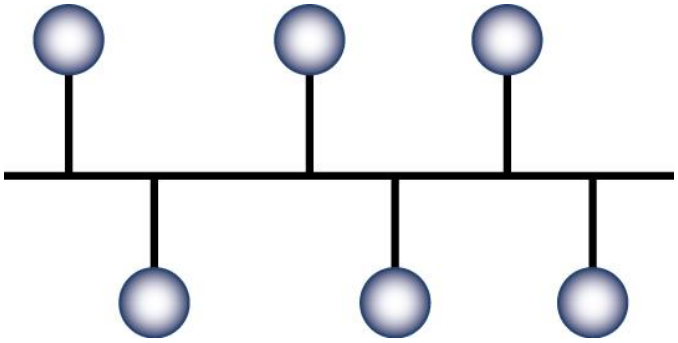


Ilustración 7. Topología de ducto

6.1.2 Topología de estrella

En una topología de estrella, las computadoras en la red se conectan a un dispositivo central conocido como concentrador (hub) o a un conmutador de paquetes (swicth).

En un ambiente LAN cada computadora se conecta con su propio cable (típicamente par trenzado) a un puerto del hub o switch. Este tipo de red sigue siendo pasiva, utilizando un método basado en contención, las computadoras escuchan el cable y contienden por un tiempo de transmisión.

Debido a que la topología estrella utiliza un cable de conexión para cada computadora, es muy fácil de expandir, sólo dependerá del número de puertos disponibles en el hub o switch (aunque se pueden conectar hubs o switchs en cadena para así incrementar el número de puertos). La desventaja de esta topología en la centralización de la comunicación, ya que si el hub falla, toda la red se cae.

Hay que aclarar que aunque la topología física de una red Ethernet basada en hub es estrella, la topología lógica sigue siendo basada en ducto.

La topología de estrella es bastante utilizada en redes MAN y WAN (Wide Area Network), para comunicaciones vía satélite y celular.

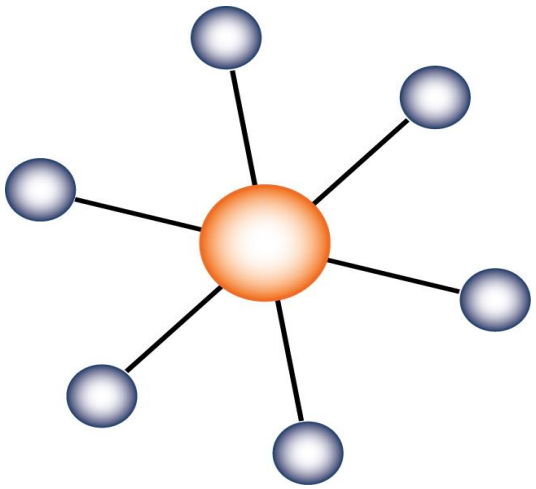


Ilustración 8. Topología de estrella

6.1.3 Topología de anillo

Una topología de anillo conecta los dispositivos de red uno tras otro sobre el cable en un círculo físico. La topología de anillo mueve información sobre el cable en una dirección y es considerada como una topología activa.

Las computadoras en la red retransmiten los paquetes que reciben y los envían a la siguiente computadora en la red. El acceso al medio de la red es otorgado a una computadora en particular en la red por un "token". El token circula alrededor del anillo y cuando una computadora desea enviar datos, espera al token y posiciona de él. La computadora

entonces envía los datos sobre el cable. La computadora destino envía un mensaje (a la computadora que envió los datos) que se fueron recibidos correctamente. La computadora que transmitió los datos, crea un nuevo token y los envía a la siguiente computadora, empezando el ritual de paso de token o estafeta (token passing) nuevamente.

La topología de anillo es muy utlizada en redes CAN y MAN, en enlaces de fibra óptica (SONET, SDH) y FDDI en redes de campus.

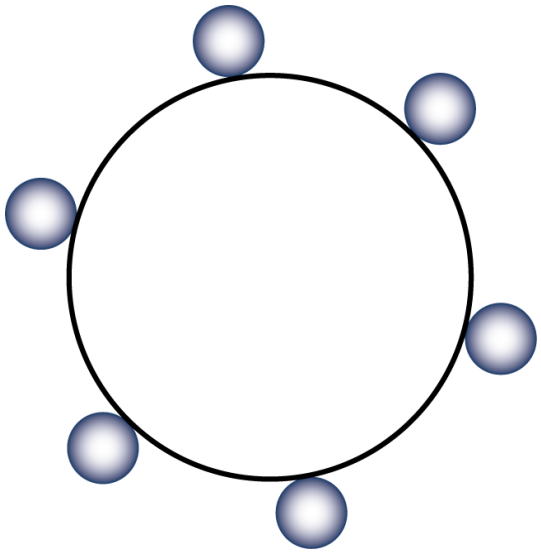


Ilustración 9. Topología de anillo

6.1.4 Topología de malla

La topología de malla utiliza conexiones redundantes entre los dispositivos de la red así como una estrategia de tolerancia a fallas. Cada dispositivo en la red está conectado a todos los demás (todos conectados con todos). Este tipo de tecnología requiere mucho cable (cuando se utiliza el cable como medio, pero puede ser inalámbrico también). Pero debido a la redundancia, la red puede seguir operando si una conexión se rompe.

Las redes de malla, obviamente, son más difíciles y caras para instalar que las otras topologías de red debido al gran número de conexiones requeridas.

La red Internet utiliza esta topología para interconectar las diferentes compañías telefónicas y de proveedoras de Internet, mediante enlaces de fibra óptica.

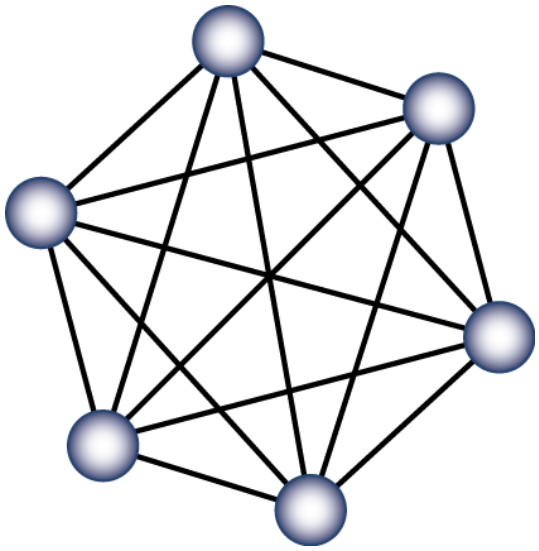


Ilustración 10. Topología de malla

7.1 VPN

VPN es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet, mediante un proceso de encapsulación y de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada.

VPN ofrece una solución de bajo costo para implementar la red a larga distancia al basarse sobre Internet, además de ofrecer autenticación de usuarios o equipos a través de cifrados, firmas digitales o claves de acceso para una identificación inequívoca; ofrece también integridad, garantizando que los datos enviados por el emisor sean exactos a los que se reciben, y confidencialidad, el cifrado hace posible que nada de lo transmitido sea interceptado o interpretada por nadie más que emisor y destino.

Requerimientos básicos de una VPN

Las redes privadas virtuales deben contar con ciertas bases antes de su implementación, tales son un set de políticas de seguridad para la codificación de datos, pues no deben ser visibles por clientes no autorizados en la red; administración de claves, para asegurar la codificación entre clientes y servidor; compartir datos, aplicaciones y recursos; un servidor de acceso y autenticación, para que en la red se tenga control de quiénes ingresan, verificar su identidad y tener registro estadístico sobre accesos; administración de direcciones, pues la VPN debe establecer una dirección para el cliente dentro de la red privada y debe asegurar que estas direcciones privadas se mantengan así; y finalmente soporte para múltiples protocolos, pues debe manejar los protocolos comunes a la red Internet, como IP, por ejemplo.

7.1.1 Tipos de VPN

VPN de acceso remoto: Consiste en usuarios que se conectan a una empresa desde sitios remotos utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso similar a estar dentro de la red local.

VPN punto a punto: Este esquema es el empleado para conectar oficinas remotas con una sede central. El servidor VPN está conectado permanentemente a Internet, acepta conexiones entrantes desde los sitios y establece el túnel VPN. Los servidores de las oficinas remotas se conectan a Internet y a través de ésta al túnel VPN de la oficina central. Se utiliza para eliminar las conexiones punto a punto tradicional.

VPN interna (over LAN): Funciona tal cual una red VPN normal, salvo que dentro de la misma red local LAN en lugar de a través de Internet. Sirve para aislar zonas y servicios de la misma red interna. Sirve también para mejorar las características de seguridad de una red inalámbrica WiFi.

8.1 MPLS

8.1.1 Antecedentes a MPLS y la evolución

El enorme crecimiento de la red Internet ha convertido al protocolo IP en la base de las actuales redes de telecomunicaciones, contando con más del 80% del tráfico cursado. La

versión actual de IP, conocida por IPv4 y recogida en la RFC 791, lleva operativa desde 1980. Este protocolo de capa de red (Nivel 3 OSI), define los mecanismos de la distribución o encaminamiento de paquetes, de una manera no fiable y sin conexión, en redes heterogéneas; es decir, únicamente está orientado a servicios no orientados a conexión y a la transferencia de datos, por lo que se suele utilizar junto con TCP (Nivel 4 de OSI) para garantizar la entrega de los paquetes. A mediados de la década de los 90, la demanda por parte de los clientes de los ISP de aplicaciones multimedia con altas necesidades de ancho de banda y una calidad de servicio o QoS garantizada, propiciaron la introducción de ATM en la capa de enlace (Nivel 2 de OSI) de sus redes. En esos momentos, el modelo de IP sobre ATM satisfacía los requisitos de las nuevas aplicaciones, utilizando el encaminamiento inteligente de nivel 3 de los routers IP en la red de acceso, e incrementando el ancho de banda y rendimiento basándose en la alta velocidad de los conmutadores de nivel 2 y los circuitos permanentes virtuales de los switches ATM en la red troncal. Esta arquitectura, no obstante, presenta ciertas limitaciones, debido a: la dificultad de operar e integrar una red basándose en dos tecnologías muy distintas, la aparición de switches ATM e IP de alto rendimiento en las redes troncales, y la mayor capacidad de transmisión ofrecida por SDH/SONET y DWDM respecto a ATM.

Durante 1996, empezaron a aparecer soluciones de conmutación de nivel 2 propietarias diseñadas para el núcleo de Internet que integraban la conmutación ATM con el encaminamiento IP; como por ejemplo, Tag Switching de Cisco o Aggregate Route-Based IP Integración y optimización de redes MPLS: Un caso práctico. 21 Switching de IBM. La base común de todas estas tecnologías, era tomar el software de control de un router IP, integrarlo con el rendimiento de reenvío con cambio de etiqueta de un switch ATM y crear un router extremadamente rápido y eficiente en cuanto a coste. La integración en esta arquitectura era mayor, porque se utilizaban protocolos IP propietarios para distribuir y asignar los identificadores de conexión de ATM como etiquetas; pero los protocolos no eran compatibles entre sí y requerían aún de infraestructura ATM. Finalmente en 1997, el IETF establece el grupo de trabajo MPLS para producir un estándar que unificase las soluciones propietarias de conmutación de nivel 2. El resultado fue la definición en 1998 del estándar

conocido por MPLS, recogido en la RFC 3031. Se desarrolló como un protocolo de conmutación por etiquetas definido para funcionar sobre múltiples protocolos como Sonet, Frame Realy, ATM, Ethernet o cualquiera sobre el que pueda funcionar PPP. Las principales motivaciones para su desarrollo son la ingeniería de tráfico, la diferenciación de clases de servicio, y las redes privadas virtuales (VPN). En un principio, también proporcionaba una mayor velocidad puesto que los routers sólo deben mirar la etiqueta para conmutar y no leer la cabecera de la capa 3 para después decidir por dónde enrutar en función del destino y/u otros parámetros. Sin embargo, hay tecnologías que han conseguido aumentar la velocidad de los routers para consultar las tablas de enrutamiento (como ASIC). Las ventajas que llevaron a desarrollar ATM: uso de conmutadores ATM más rápidos porque funcionaban con etiquetas, el poder ofrecer ingeniería de tráfico mediante circuitos virtuales... llevan a desarrollar MPLS unos años más tarde, basándose en la idea de las etiquetas, pero reduciendo la complejidad de las redes IP sobre ATM y mejorando la funcionalidad en algunos casos. IP sobre ATM conseguía aprovecharse de la velocidad que proporcionaban los conmutadores ATM para unir los routers IP, pero seguían siendo dos redes separadas (complejo de gestionar), y el número de circuitos virtuales aumenta mucho con el tamaño de la red.

Varios fabricantes intentaron mejorar esto proponiendo soluciones mediante etiquetas que separasen las funciones de routing (encaminamiento, control de por dónde se envían los paquetes) de las de forwarding (reenvío en sí). El problema ahora es que eran incompatibles entre sí. MPLS es un intento de estandarizar estas soluciones. MPLS aprovecha lo mejor de la capa 2, la rápida conmutación, sin perder de vista la capa 3, para no perder sus posibilidades. Esto se consigue separando de verdad la función de conmutación de la de enrutamiento. MPLS hace más viable la ingeniería de tráfico, permite enrutamiento rápido (porque en realidad hace conmutación, pero con información de enrutado), permite que los equipos de reenvío sean más baratos si sólo deben entender paquetes etiquetados, permite ofrecer QoS basándose en diferentes CoS (clases de servicio), hace más fáciles y flexibles las VPN (redes privadas virtuales), y además parece el primer paso para conseguir redes totalmente ópticas (ya que decidimos por dónde enviar el paquete según lo que diga la

etiqueta y no hace falta procesar la cabecera de orden 3; es decir, aunque las decisiones del enrutado sean en el dominio eléctrico, la conmutación podría ser óptica). MPLS utiliza los campos para etiquetas de ATM o Frame Relay, o añade una cabecera para el resto de protocolos entre la del nivel 3 y la del nivel 2. La diferencia con IP sobre ATM es que no tenemos una red diferente que nos proporciona conexión entre routers IP, sino que Integración y optimización de redes MPLS: Un caso práctico. 22 los niveles están integrados, y las funciones de encaminamiento y reenvío separadas pero coordinadas. Hay una parte de control, que se encarga de las decisiones de encaminamiento, pero no construye una tabla en la que consultar la dirección IP de los paquetes que lleguen, sino que informa a la parte de reenvío, que construye una tabla con etiquetas; así no es necesario mirar la cabecera de la capa 3, y decidir para cada paquete, porque la decisión ya está tomada para cada etiqueta. El único router que tiene que hacer funciones de enrutamiento es el primero, que tiene que decidir que etiqueta coloca a cada paquete. Todos los paquetes que llevan la misma etiqueta forman un grupo que se denomina Forwarding Equivalent Class (FEC).

8.1.2 Arquitectura MPLS

La denominación de multiprotocol fue posterior a la implementación de MPLS sobre routers Cisco. Antes del estándar se denominaba Tag Switching y solo permitía IPv4, después se implementó para el uso de otros protocolos como puede ser IPv6. La denominación de Label Switching es debido a que no se enruta en base a prefijos IPv4 u otro protocolo, sino que se conmuta en base a etiquetas. A continuación se describe para que se usan las etiquetas, como se usan y como se distribuyen en la red.

8.1.3 Etiquetas MPLS

Una etiqueta MPLS es un campo de 32 bits con una determinada estructura.

Ilustración 11. Formato etiqueta MPLS

Los primeros 20 bits son la etiqueta. Este valor oscila entre 0 y 220 -1 o 1.048.575 sin embargo los primeros 16 bits no se emplean normalmente, tienen significado especial. Los bits del 20 al 22 son los 3 bits experimentales (exp). Son usados exclusivamente para hacer calidad de servicio (QoS). El bit 23 es el indicador de final de pila (Bottom of Stack – BoS). Su valor es 0 a menos que sea el final de la pila, en cuyo caso tomará valor 1. La pila de etiquetas es un conjunto de etiquetas que puede estar formado por una sola etiqueta o más. El número de etiquetas que pueden formar un paquete es ilimitado aunque lo normal es que no haya más de 4. Los bits del 24 al 31 son los 8 bits que forman el TTL. Este TTL tiene la misma función que el TTL del paquete IP. En cada salto se va decrementando en una unidad y su principal función es que un paquete no esté dando vueltas por la red durante un tiempo ilimitado. Cuando alcanza el valor de 0 el paquete se descarta.

8.1.4 VPN MPLS

Las VPN MPLS o redes privadas virtuales MPLS, es la más popular y usada implementación de la tecnología MPLS. Su popularidad ha crecido exponencialmente desde que fueron inventadas. Aunque muchos proveedores de servicios las han implementado como sustitutos de sus antiguas redes ATM o Frame Relay, muchas grandes compañías las están desarrollando dada su escalabilidad y la capacidad de dividir redes en redes más pequeñas lo cual es muchas veces útil en empresas de gran tamaño, donde con la misma infraestructura tienes que dar servicio a departamentos individuales.

Modelo de VPN MPLS

Es importante familiarizarse con la terminología de VPN MPLS dado que es bastante frecuente que se extienda más allá del ámbito de VPN MPLS. Un router Provider Edge (PE) está directamente conectado al customer edge (CE) que es un router de cliente de nivel 3. Un router Provider (P) es un router que no está conectado a ningún equipo de cliente. En una VPN MPLS los P y PE tienen funcionalidad MPLS lo que significa que tienen capacidad de intercambio de etiquetas entre ellos. Un CE tiene conexión directa de nivel 3 con un router PE. Un router CE no tiene capacidad MPLS. Un router C es un equipo de cliente que no tiene conexión directa con un router PE. Los routers C y CE no necesitan tener capacidades de MPLS. En la siguiente ilustración vemos todos los elementos de una VPN.

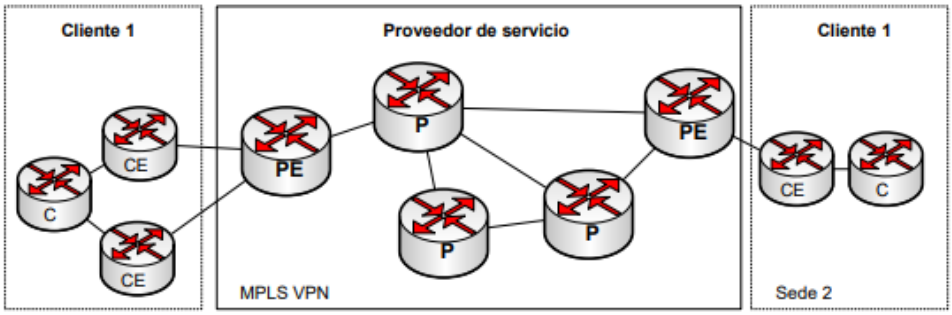


Ilustración 12. Elementos de una red VPN

Debido a que tanto los routers CE como los PE interactúan a nivel 3, es necesario que hablen entre ellos un protocolo de routing dinámico (o rutas estáticas). El CE solo tiene un equipo conectado fuera de su ubicación, el PE. El CE no tiene conectividad física directa con ningún otro CE. El nombre de este modelo se llama peer-to-peer ya que el CE y el PE tienen una conexión de nivel 3. Una VPN debe ser privada, por ello los clientes pueden tener su propio plan de direccionamiento, puede usar, tanto direccionamiento público como privado e incluso se puede repetir direccionamiento entre clientes. Si los paquetes fuesen reenviados como paquetes IP en los nodos P habría un problema de routing. Si no se les permitiese a los clientes tener su propio direccionamiento, este debería ser asignado por el proveedor de servicios. Suponiendo esto, los paquetes podrían ser reenviados atendiendo a su dirección IP destino en cada router de la red del proveedor. Esto significa que tanto los nodos P como los nodos PE deberían tener una tabla de rutas completa con el direccionamiento de cada cliente y esa tabla podría ser muy grande. El único protocolo de routing capaz de manejar semejante tabla es BGP por lo que tanto nodos P como nodos PE deberían hablar iBGP entre ellos. Llegados a este caso no sería un esquema válido debido a que no es un entorno privado para cada cliente. Otra solución sería que tanto LSRs P como LSRs PE manejasen tablas de rutas distintas para cada cliente. Debería haber tantos procesos de routing como VPNs de cliente hubiera configuradas en la red. Esta no es una solución muy escalable ya que cada vez que un nuevo cliente se diese de alta en la red habría que configurar en cada nodo (tanto P, como PE) un proceso de routing. Además, al entrar un paquete a la red a través de un PE, ¿Cómo se podría identificar a que VPN pertenece? La solución pasaría por modificar el paquete IP añadiéndole un campo de identificación de VPN. Entonces los nodos P deberían mirar además del campo IP destino el campo de VPN para reenviar

adecuadamente el paquete. Una solución escalable es que los routers P no tuviesen consciencia de VPN lo que les liberaría de la carga de tener información de las rutas para cada VPN. Precisamente esto es la solución que ofrece MPLS. Los paquetes IP de cada cliente son etiquetados en la red MPLS para conseguir una VPN privada para cada cliente. Además, los routers P no necesitan conocer la tabla de rutas gracias a la utilización de dos etiquetas MPLS. Por lo tanto, BGP no es necesario en los routers P. Las rutas para cada VPN solo se manejan en los nodos PE al igual que solo hay concepto de VPN en los PEs lo que hace que las VPN MPLS sean una solución escalable.

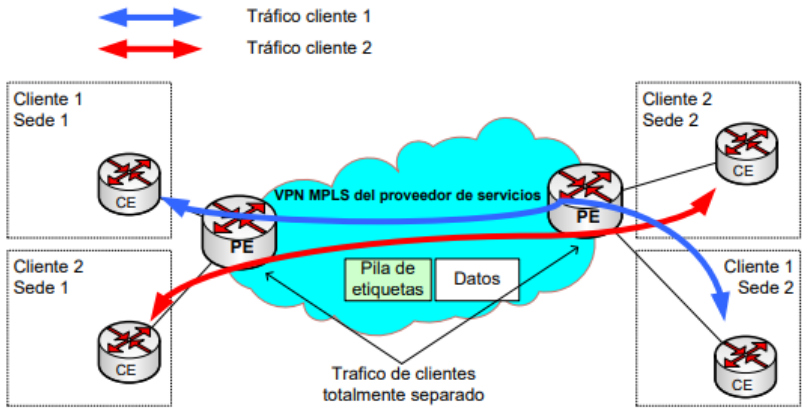


Ilustración 13. Modelo de VPN MPLS

8.1.5 Arquitectura de VPN MPLS

Los conceptos básicos para comprender el funcionamiento de una VPN en MPLS son: VRF, route distinguisher (RD), route target (RT), propagación de rutas en MP-BGP y el reenvío de paquetes etiquetados.

8.1.6 VIRTUAL ROUTING FORWARDING (VRF)

Una VRF es una instancia de enrutamiento y reenvío en la VPN. Es el nombre que recibe la combinación de la tabla de routing de la VPN, la CEF de la VRF y los protocolos de routing IP asociados en el router PE. Un nodo PE tiene una instancia de VRF para cada VPN asociada. En la siguiente ilustración podemos ver como un nodo PE tiene su tabla de rutas global IP y también una tabla de routing VRF por cada VPN conectada al PE.

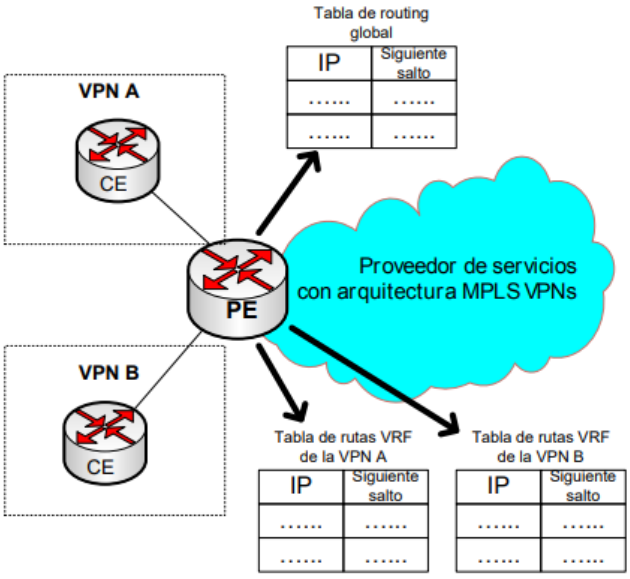


Ilustración 14. VRFs en un nodo PE

Como la tabla de rutas debe estar separada y ser privada para cada cliente dentro de un nodo PE, cada VPN debe tener su propia tabla de rutas. Esta tabla de rutas privada se llama tabla de rutas VRF. El interfaz del PE que conecta con el CE puede pertenecer solo a una VRF por lo que todos los paquetes recibidos en la interfaz de esa VRF se identifican inequívocamente como pertenecientes a esa VRF. Puesto que hay una tabla de rutas separada por VPN también hay una tabla CEF específica por VPN para reenviar esos paquetes en el router PE. Esta tabla se llama tabla CEF VRF. Al igual que con la tabla de rutas global y la tabla CEF global, la tabla CEF VRF deriva de la tabla de rutas VRF. Una interfaz solo se puede asociar a una VRF y no a varias, pero una VRF puede estar asociada a varios interfaces.

8.1.7 Route Distinguisher

Los prefijos de la VPN se propagan a través de la VPN sobre MPLS mediante Multiprotocol-BGP. El problema es que cuando BGP transporte estos prefijos sobre la red deben ser únicos y si el cliente tiene direccionamiento IP solapado el routing podría ser erróneo. Para solucionar este problema se crea el concepto de RD que convierte los prefijos IP en únicos. Cada prefijo de cada cliente recibe un identificador único RD para distinguir el mismo prefijo

de distintos clientes. El prefijo deriva de la combinación del prefijo IP y del RD y se llama prefijo VPNv4. El MP-BGP transporta los prefijos VPNv4 entre los routers PE.

El RD es un campo de 64 bits pero no indica a que VRF pertenece el prefijo. La función del RD no es ser un identificador de VPN ya que algunos escenarios de VPN más complejos pueden requerir más de un RD por VPN. Cada instancia de VRF en un nodo PE debe tener un RD asignado. El valor del campo del RD puede tener dos formatos: ASN:nn o DirecciónIP:nn donde nn representa un número. El formato más usado comúnmente es ASN:nn donde ASN es el número de sistema autónomo. Normalmente ASN es el número de sistema autónomo asignado por IANA al proveedor de servicio y nn es el número que el proveedor de servicio asigna unívocamente a la VRF. El RD no impone semántica y se usa solamente para identificar de manera única las rutas de la VPN. Esto es necesario para evitar solapamiento IP entre clientes. La combinación del RD y el prefijo IP proporciona un prefijo VPNv4 de 96 bits de longitud.

Esto es un ejemplo

```
RD: 64987:140014
Prefijo IPv4: 10.200.3.4/30
Prefijo VPNv4: 64987:140014:10.200.3.4/30
```

Un cliente puede usar diferentes RDs para una misma ruta IP. Cuando una sede de la VPN se conecta a dos PEs, las rutas de la sede VPN pueden tener dos RDs diferentes dependiendo en que PE se reciben las rutas. Cada ruta IP tendrá en ese caso dos RDs diferentes asignados y tendrá dos rutas VPNv4 totalmente diferentes, esto permite a BGP verlas como diferentes rutas y aplicarles diferentes políticas.

8.1.8 Route Target (RT)

Si los RDs se usaran solo para identificar la VPN, la comunicación entre sedes de distintas VPNs sería problemática y a veces esto es necesario p.e cuando dos clientes necesitan acceder a un mismo recurso (DMZ, servidor, segmento de red, etc.…) Una sede de un cliente A no podría comunicarse con una sede de un cliente B porque los RDs no coincidirían. El concepto de sedes de distintos clientes con comunicación entre si se llaman extranet VPN. El caso más sencillo de comunicación entre sedes de un mismo cliente (de la misma VPN) se conoce como intranet VPN. La comunicación entre sedes se controla mediante otra funcionalidad de la VPN MPLS llamada Route Target (RT).

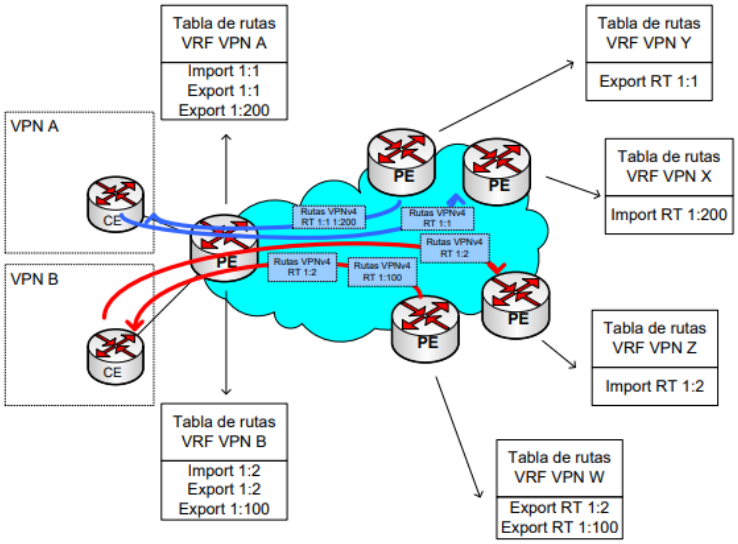


Ilustración 15. Funcionamiento de los Route Targets

Un RT es una comunidad extendida de BGP que indica que rutas deben ser importadas de MP-BGP a la VRF. Exportar un RT significa que a cada ruta VPNv4 exportada se le añade una comunidad BGP extendida (esto es el RT) cuando esta ruta se redistribuye de la tabla de rutas VRF al MP-BGP. Importar un RT significa que para cada ruta VPNv4 recibida de MP-BGP se comprueba si su comunidad extendida (RT) coincide con alguna de las asociadas a alguna VRF. Si coincide el prefijo se incluye en la tabla de rutas VRF como una ruta IP. Si no coincide el prefijo es rechazado. La siguiente ilustración muestra como los RTs controlan que rutas se importan en cada VRF desde los PEs remotos y con que RTs se exportan los prefijos VPNv4 hacia los PEs remotos. Más de un RT puede ser asociado a un prefijo VPNv4. Para

que la importación hacia la VRF se permita solo es necesario que un RT del prefijo VPNv4 coincida con alguno de los RTs importados en esa VRF.

8.1.9 PROPAGACIÓN DE RUTAS VPNV4 EN UNA VPN MPLS

Las VRFs separan las rutas de cliente en los nodos PE, pero absolutamente todos los prefijos son transportados a través de la red MPLS. Potencialmente pueden ser cientos de miles de rutas ya que pueden ser numerosas las VPNs de cliente configuradas. Para este transporte de rutas, BGP es el protocolo ideal ya que está probado y es estable para el manejo de grandes tablas de rutas, por eso es el protocolo estandarizado para internet. Gracias a la transformación de prefijos IP en prefijos VPNv4 (RD + prefijo IP), todas las rutas se pueden transportar de manera segura a través de la red. El nodo PE recibe rutas IP desde el CE mediante un IGP o mediante eBGP.

Estas rutas IP de una VPN determinada se insertan en una tabla de rutas VRF. Esta VRF depende de la que esté configurada sobre el interfaz del PE que conecta con el CE que inyecta las rutas. Estas rutas IP se convierten en rutas VPNv4 una vez que los prefijos se asignan al RD correspondiente, es entonces cuando entran en el proceso de MP-BGP. BGP se encarga de distribuir estas rutas VPNv4 hacia todos los PEs en esa VPN. El que la ruta VPNv4, después de separarse del RD, sea puesta en la tabla de VRF como rutas IP o no depende de si los RTs permiten la importación a esa VRF. Esas rutas IP son entonces anunciadas al router CE mediante un IGP o eBGP que esté corriendo entre el PE y el CE.

Para comprender todos estos procesos, en la siguiente ilustración se ven los pasos que se establecen para que se produzca comunicación IP entre dos CEs a través de una VPN MPLS.

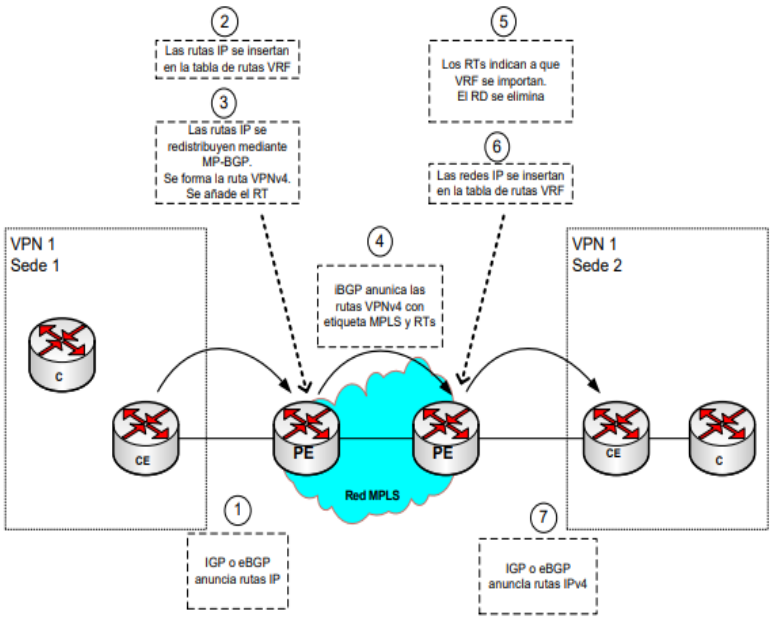


Ilustración 16. Propagación de rutas en una VPN MPLS paso a paso

8.1.10 Reenvió de paquetes en una red VPN MPLS

Los paquetes no pueden ser reenviados como paquetes puros IP entre dos sedes. Los routers P no pueden reenviarlos porque no tienen información alguna de VRFs. MPLS soluciona este problema etiquetando los paquetes. La manera más habitual es hacerlo con LDP entre todos los routers P y PE así todo el tráfico IP es reenviado basado en etiquetas. También se puede usar RSVP con extensiones para ingeniería de tráfico pero LDP es lo más común. Los paquetes IP son reenviados basándose en etiquetas desde el Ingress PE hasta el Egress PE. Un nodo P nunca tiene que tiene que consultar la cabecera IP. Esta es la manera en que los paquetes se conmutan entre el Ingress PE y el Egress PE. Esta etiqueta se llama etiqueta IGP, ya que es la etiqueta que se asocia a un prefijo IP en la tabla de routing global de los routers P y PE y es anunciada por el IGP.

Para resumir, el tráfico VRF a VRF tiene dos etiquetas en una red VPN MPLS. La etiqueta externa es la etiqueta IGP y es distribuida mediante LDP o RSVP entre todos los routers P y PE salto a salto. La etiqueta más interna es la etiqueta VPN que es anunciada por MP-BGP de PE a PE. Los routers P consultan la etiqueta IGP para reenviar los paquetes hacia el nodo PE correcto. Los Egress PE usan la etiqueta de VPN para reenviar el paquete al CE correcto.

En el siguiente ejemplo podemos ver como es el reenvío de paquetes en una red VPN MPLS. Los paquetes entran en el router PE en la VRF asociada al interfaz de entrada como un paquete IP. Es reenviado a través de la red VPN MPLS con dos etiquetas. Los routers P reenvían el paquete mirando la etiqueta externa. Esta etiqueta externa es intercambiada en cada nodo P. Las etiquetas son eliminadas en el Egress PE y el paquete es enviado como un paquete IP sobre el interfaz que corresponda a la VRF adecuada hacia el CE. El CE se encuentra mirando la etiqueta VPN.

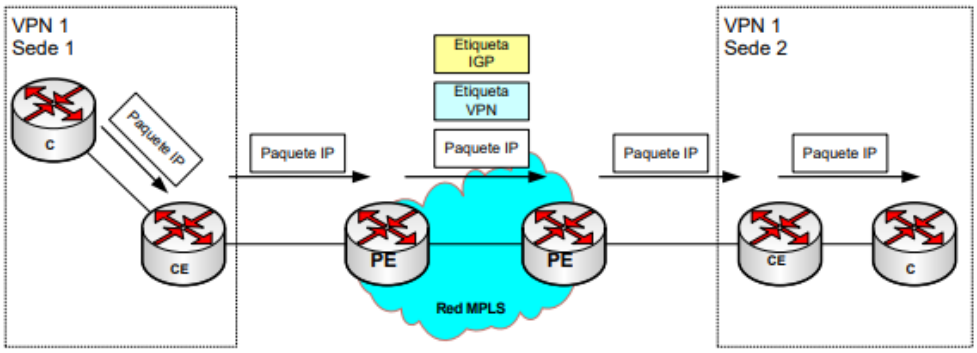


Ilustración 17. Formato de paquetes en una red VPN MPLS

También es necesario conocer un poco acerca de las características de BGP necesarias en una VPN MPLS.

BGP ha sido durante muchos años el estándar de protocolo de routing entre dominios. Es el protocolo que hace que internet funcione. Los proveedores de servicios intercambian rutas mediante BGP. Se interconectan con otros proveedores de servicios mediante eBGP y en su red hablan iBGP. BGP es un protocolo de rutas que está totalmente adaptado para transportar cientos de miles de rutas. También es un protocolo que permite implementar políticas flexibles y extendidas. Son estas características las que le convierten en un buen candidato para transportar rutas VPN MPLS. Como mencionamos antes, lo que realmente transporta son prefijos VPNv4. BGP-4 está descrito en la RFC 1771, pero en esta RFC solo se describe el uso de BGP para transportar rutas IP pero BGP puede hacer mucho más que transportar rutas IP. La RFC 2858, "Multiprotocol extensions por BGP-4" fue escrita para extender BGP y que fuese capaz de transportar otra información de routing además de IP.

Un equipo BGP permite a sus vecinos BGP que extensiones multiprotocolo para BGP-4 soporta utilizando anuncios de capacidades. Los vecinos BGP se mandan entre si las capacidades que soportan. Las capacidades que dos vecinos compartan, son las que pueden usar. La RFC 3392 "Capabilities Advertisement with BGP-4" describe el funcionamiento de los anuncios de capacidad.

Cuando un nodo que tiene BGP configurado manda un mensaje de "open" a sus vecinos BGP, puede incluir un parámetro de capacidad opcional listando todas las capacidades del equipo. Todos los vecinos BGP pueden hacer lo mismo. Las extensiones multiprotocolo para BGP-4 definen dos nuevos atributos: Multiprotocol Reachable NLRI y Multiprotocol Unreachable NLRI. Estos atributos anuncian o dan de baja rutas. Ambos tienen dos campos: el Address Family Identifier (AFI) y el Subsequent Address Family Identifier (SAFI). La combinación de estos atributos describe exactamente qué tipo de rutas BGP se transportan.

La siguiente tabla indica algunos códigos AFI y su descripción:

Número	Descripción
0	Reservado
1	IPv4
2	IPv6
11	IPX
12	AppleTalk

Tabla 2.Códigos AFI y su descripción

La siguiente tabla muestra códigos SAFI y su descripción:

Número	Descripción
1	NLRI para reenvió unicast
2	NLRI para reenvío multicast
3	NLRI para reenvío unicast y multicast
4	NLRI para reenvío de IPv4 y etiquetas
128	NLRI para reenvío VPN etiquetado

Tabla 3. Código SAFI y su descripción

Para soportar el comportamiento multiprotocolo de BGP en tecnología Cisco, existe el concepto de familia de direcciones (address family). Las cuatro familias de direcciones que actualmente se soportan son: IPv4, IPv6, VPNv4 (VPN IPv4) y VPNv6 (VPN IPv6). Las siguientes familias de direcciones que se pueden combinar con las anteriores son unicast, multicast y VRF.

III. METODOLOGÍA

3.1 Enfoque y Métodos

Este proyecto está basado en brindar una mejora a la red de COPEMSA haciéndose un reemplazo de los routers previamente instalados. Anteriormente la empresa C&W Business les había proporcionado routers cisco 1811 y se decidió hacer una renovación de ellos por routers cisco 881-K9 los cuales brindan como ventaja una mayor transferencia de datos.

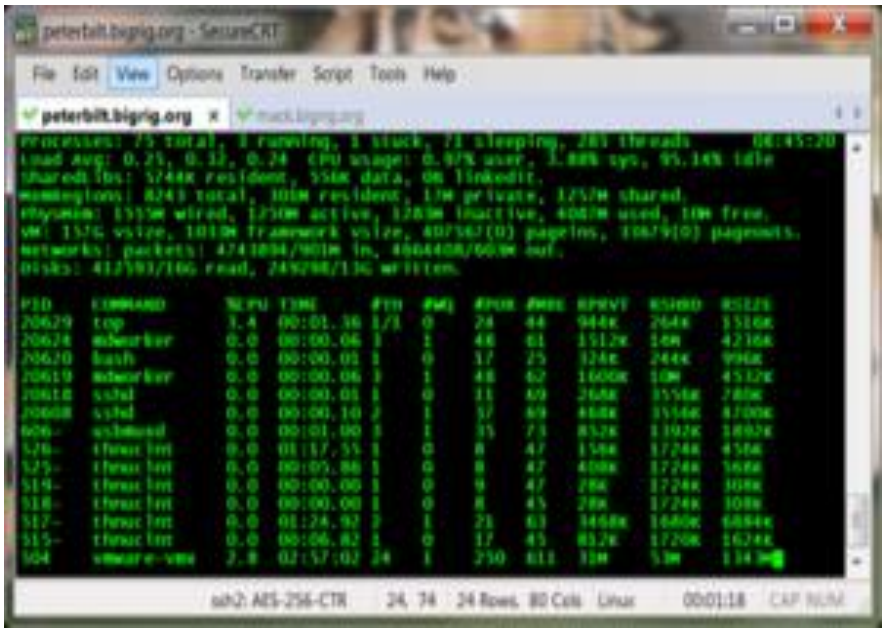


Ilustración 18. Muestra de programa SecureCRT

Se determinaron los nodos de los cuales provenía cada sucursal de COPEMSA a la cual se haría la renovación y para ello se utilizó el terminal telnet para Windows SecureCRT, siendo identificada cada sucursal por un circuit ID diferente. Cada uno de los sitios tiene su enlace principal y de protección, a las cuales fueron identificadas las vlan tanto de MPLS como de gestión con su respectiva dirección IP, y con toda esta información adjunta se establecieron las configuraciones que se implementarían en los routers.

3.2 Materiales

Ilustración 19. Router Cisco 881-K9

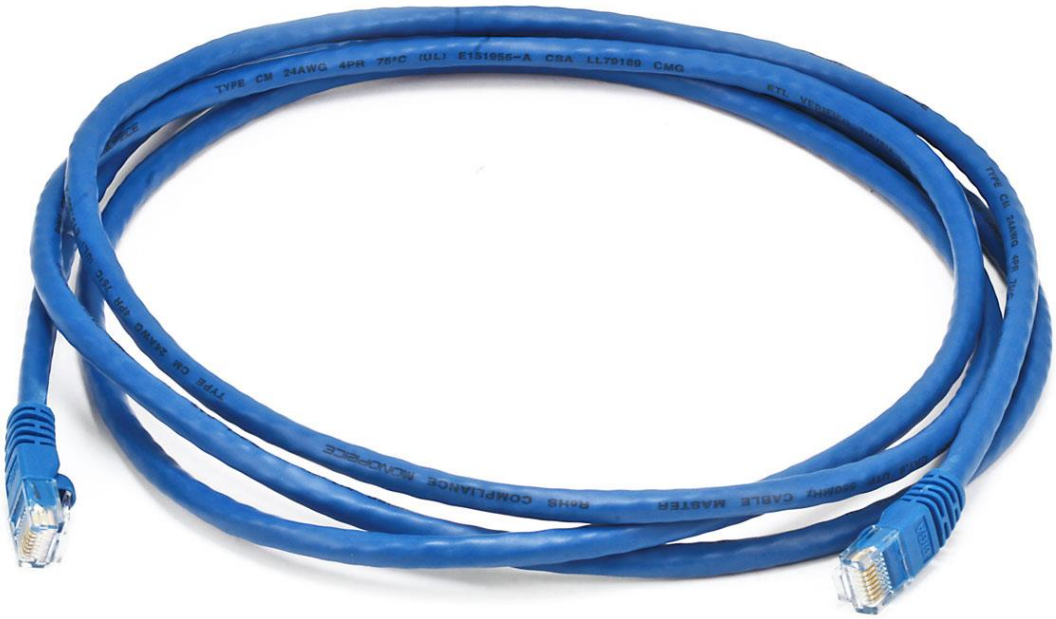


Ilustración 20. Ethernet Patch Cabe- Snagless RJ45

Ilustración 21. Cable de consola Cisco

Ilustración 22. JDSU Probador de red de comunicación

3.3 Técnicas e instrumentos aplicados

Luego de hacer un intercambio en los routers, se aseguró que la red proporcionara correctamente el ancho de banda de 10 Mbps a cada una de las sucursales. Para ello se utilizó el equipo JDSU con el cual realizamos pruebas RFC2544. En la siguiente tabla se muestran las pruebas de transmisión en la red mediante servicio Ethernet que pueden realizarse con dicho equipo.

Característica	Funcionalidad
Pruebas de Loopback	Funciona como un dispositivo de loopback para pruebas de latencia y para la RFC 2544
Análisis y filtro de tráfico Ethernet e IP	Filtra y analiza el tráfico de llegada para determinar el Throughput y QoS del cliente.
Diagnóstico de Capa Física	Verifica que el circuito esté levantado y conectado y que la capa física esta correcta.
Reportes Gráficos	Generación de reportes profesionales para la validación o almacenamiento de los resultados de las pruebas de Nivel de Servicio.
Soporte VLAN incluyendo Q-in-Q	Verifica que las priorizaciones de las VLAN y las Q-in-Q están correctamente configuradas en la red.
Generación de tráfico y mediciones de potencia óptica	Verifica enlaces ópticos (pérdida óptica y QoS)
Generación de tráfico Ethernet e IP	Verifica para asegurar que los parámetros de QoS se están cumpliendo al emular el tráfico del cliente.
Ping y Traceo de ruta	Verifica que existe conectividad entre 2 puntos
Prueba de tráfico RFC 2544	Verifica que los Acuerdos de Nivel de Servicio se están cumpliendo al realizar pruebas conforme al estándar internacional.

Tabla 4. Tipos de pruebas de transmisión mediante servicio Ethernet

En la prueba RFC2544 se tienen 2 dispositivos JDSU, en el cual uno de ellos fue ubicado en la oficina generando un loopback del tráfico de modo que los parámetros tales como latencia y throughtput puedan ser medidos a través de la red. La latencia es el tiempo total que tarda un frame en viajar desde la fuente hacia su destino, este tiempo total es la suma del procesamiento de los elementos de la red y el retraso de propagación a lo largo del medio de transmisón. Y el throughput es la cantidad de datos que puede ser transportado desde el origen hasta el destino. RFC 2544 nos permite también poder hacer pruebas de frame loss y back to back frame.

3.4 Fuentes de Información

Se utilizaron diversas fuentes de información, entre ellas libros en físico proporcionados por la biblioteca de UNITEC, como también los recursos electrónicos a los cuales se puede acceder mediante la página web del Centro de Recursos para el Aprendizaje e Investigación (CRAI) de UNITEC. Se utilizaron manuales de cada uno de los equipos, sus especificaciones técnicas, y también los manuales electrónicos que vienen con el software instalado.

IV. RESULTADOS Y ANÁLISIS

4.1 Resultados/Análisis

El poder implementar la tecnología MPLS permitió crear una red totalmente privada y segura entre las sucursales con independencia de internet. Mediante MPLS también gestionamos la prioridad del tráfico, según las necesidades corporativas, gestionando todos los servicios disponibles (Datos, telefonía, video vigilancia, etc). Se brindó un soporte de QoS en donde se priorizo el tráfico, lo cual es una prestación clave ya que la compañía utiliza voz y video en las redes de datos. Se obtuvo un rendimiento mejorado en un 40% ya que se hizo una reducción en el número de saltos entre puntos, esto debido a una mejora en los tiempos de respuesta y del rendimiento de las aplicaciones. El servicio MPLS brindara a futuro una mejora en la recuperación ante desastre de diversas maneras. En primer lugar, nos permitió conectar los centros de datos mediante múltiples conexiones redundantes a la nube MPLS y, a través de ella, a otros sitios de la red. Además, los sitios remotos pueden ser reconectados fácil y rápidamente a las localizaciones de backup en caso de necesidad; a diferencia de lo que ocurre con las redes ATM y Frame Relay, en las cuales se requieren circuitos virtuales de backup permanentes o conmutados.

También se integró la solución BGP / MPLS IP que permitirá un creciente tamaño del despliegue de una VPN (en términos de VPN, sitios y rutas), añadiendo más enrutadores y teniendo más capacidad de la red. Esto es posible debido a que los enrutadores CE intercambian rutas con el enrutador PE que está conectado al proveedor, en lugar de hacerlo

con cada uno de los otros enrutadores CE en la VPN. BGP nos permitió la utilidad para la distribución de información de VPN entre proveedores de servicios. Además, el uso de la ruta de control de acceso se aprovechó para reducir el número de rutas de anuncios enviados a un BGP con conexión peer con el objetivo de filtrado de ruta de la VPN. El rendimiento se mejoró por el despliegue utilizando rutas de los reflectores, ya que redujo la tramitación de carga en la ruta del reflector.

Capitulo V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

1. Se llevó a cabo un exitoso cambio en el equipo de la empresa petrolera COPEMSA quienes en su red ya tenían integrada una VPN, y se mejoró este servicio haciendo la integración de la tecnología MPLS.
2. Pudimos observar la eficacia de la integración del protocolo BGP al poder desviar el tráfico basándose en criterios determinados por la arquitectura de la red, también en la facilidad de compartir y preguntar sobre la tabla de routing IP interior aun teniendo su propia tabla de routing.
3. Mediante las pruebas RFC2544 realizadas con el equipo JDSU se obtuvo una mejora del 32% con la integración de los nuevos routers en comparación con el equipo que estaba previamente instalado, lo cual establecerá una significante mejora en el servicio recibido.

5.2 Recomendaciones

En esta fase de proyecto dentro de la empresa Cable and Wireless Business, fui participe no solo del proyecto de COPEMSA, sino también de otros pequeños proyectos de renovación de equipo y en visitas a clientes por atención de fallas, debido a esto surgieron algunas recomendaciones, que se enlistan a continuación:

1. Es necesario que haya una mejor comunicación entre las personas que ofrecen los proyectos al cliente y los ingenieros a cargo de ellos, ya que al momento de hacer las visitas al cliente se tienen ciertas incertidumbres pues los ingenieros desconocen alguna información.
2. Se debe agilizar el proceso en la obtención de recursos, pues esto retrasa el tiempo que toma llevar a cabo un proyecto, como lo fue con el descrito en este informe que se mantuvo a la espera pues las configuraciones de los equipos tardaron en ser enviadas.
3. Publicitar más la empresa para que sea conocida en la zona, ya que hay muchas persona e incluso empresas que desconocen de Cable & Wireless Business y la gama de excelente servicios que brindan.

Capítulo VI. APLICABILIDAD

Cronología

La primera semana se tuvo una pequeña inducción sobre lo que la empresa C&W Business consistía, sus herramientas a utilizar y las actividades que realiza el equipo de trabajo. En la segunda semana se me fue asignado el proyecto descrito ya anteriormente en este informe.

Luego en las semanas 3 y 4 ya con un proyecto asignado, se recopilaron los datos como nodos al cual cada sucursal pertenecía, las vlans de MPLS y gestión asignadas, y el switch y puerto al que cada una pertenecía. Durante la semana 5 y 6 se hizo una investigación sobre cada una de las variables de análisis. Al tener ya todas las herramientas necesarias se prosiguió a la implementación del proyecto. Con todo el equipo instalada en la semana 9 se terminaron de hacer las pruebas RFC2544 para asegurar que la red siguiera funcionando de forma correcta. Y finalmente durante la semana 10 se hizo la culminación del proyecto, y entregando las conclusiones de ello a la empresa COPEMSA en la cual se realizó el proyecto previamente señalado.

En el proyecto se hizo la instalación de un nuevo equipo de routers en la zona norte, el modelo que al cual se renovó fue c881-k9 siempre de la marca Cisco. Las sucursales a las cual se hizo la renovación fueron: Texaco Hercules Puerto Cortés, Texaco David 7 Calle San Pedro Sula, Texaco Villa Olímplica San Pedro Sula, Texaco Expocento San Pedro Sula, Texaco Aerotex La Lima, Texaco Independecia y Metropolitana San Pedro Sula, Texaco La Victoria Choloma, Texaco La Curva y Milenium Puerto Cortes. Todas ellos fueron conectadas a la nube MPLS de Cable and Wireless Business tal y como se muestra en la tabla a continuación.

	1 semana	2 semana	3 semana	4 semana	5 semana	6 semana	7 semana	8 semana	9 semana	10 semana
Inducción										
Asignación de proyecto										
Recopilación de datos										
Investigación										
Implementación										
Realización de pruebas										
Conclusiones										

Tabla 5. Cronología de trabajo.

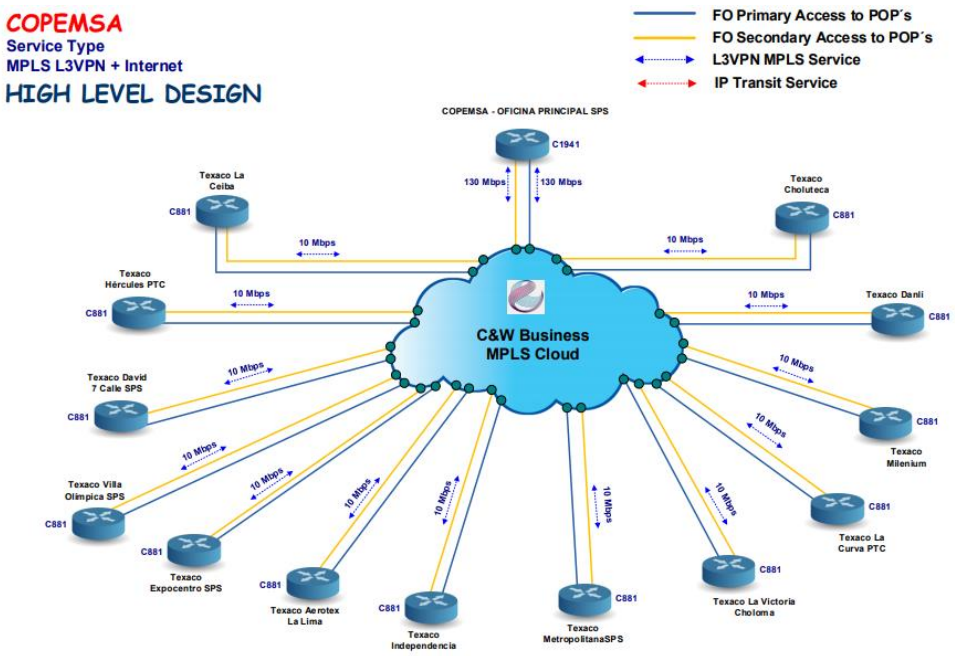


Ilustración 23. Muestra de red COPEMSA conectada a MPLS

Al hacerse una renovación y no una instalación el único costo monetario al que se incurrió fue en la compra de los routers cisco 881-k9 con un precio de $599.99 cada uno. La red ya estaba previamente instalada por lo cual no se obtuvo un gasto adicional en ello. Las demás mejoras fueron basadas en configuraciones lo cual no conllevo ningún costo adicional. Incluyendo la zona centro, la empresa hizo la instalación de 14 nuevos routers, lo cual lleva un total de $8,396.86 en gastos.

Bibliografía

Ahmad, A. (2012). *Data Communication Principles for Fixed and Wireless Networks*. Secaucus, US: Kluwer Academic Publishers. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10067399

Alarcón Aquino, V., & Martínez Suárez, J. C. (2008). *Introducción a Redes MPLS*. Córdoba, AR: El Cid Editor. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10232356

Alpern, N. J., Alpern, J., & Muller, R. (2011). *IT Career JumpStart: An Introduction to PC Hardware, Software, and Networking (1)*. Hoboken, US: Sybex. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10523275

Anand, K. (2010). *Networking Concepts and Netware*. Mumbai, IND: Himalaya Publishing House. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10415982

Ciccarelli, P., & Faulkner, C. (2006). *Networking Foundations: Technology Fundamentals for IT Success (1)*. Alameda, US: Sybex. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10131866

Cvijetic, M., & Djordjevic, I. B. (2012). *Advanced Optical Communication Systems and Networks*. Norwood, US: Artech House. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10857821

Gibson, D. (2011). *Microsoft Windows Networking Essentials (1)*. Hoboken, US: Sybex. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10513730

Muller, N. (2013). *LANs to WANs*. Norwood, US: Artech House Books. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10081915

Murthy, C. S. V. (2010). *Data Communication and Networking*. Mumbai, IND: Himalaya Publishing House. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10415883

Oki, E., Rojas-Cessa, R., & Tatipamula, M. (2012). *Advanced Internet Protocols, Services, and Applications (1)*. Hoboken, US: Wiley. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10538697

Shinde, S. S. (2009). *Computer Network*. Daryaganj, Delhi, IND: New Age International. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10367725

Singh, V. P. (2009). *Simplified Internet E-Mail and Web*. Delhi, IND: Computech Publications Limited. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10417314

Stavdas, A. (2010). *Wiley Series on Communications Networking & Distributed Systems: Core and Metro Networks (1)*. Hoboken, GB: Wiley. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10361246

Sun, Z. (2014). *Satellite Networking: Principles and Protocols (2)*. Somerset, GB: Wiley. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10849203

Thakur, V. (2010). *Digital Network*. Mumbai, IND: Himalaya Publishing House. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10416134

Toy, M. (2012). *Information and Communication Technology Series,: Networks and Services: Carrier Ethernet, PBT, MPLS-TP, and VPLS (1)*. Somerset, US: Wiley-Interscience. Recuperado a partir de http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10602107

Anexos

	A	B	C	D	E	F	G	H	I	J
1	PRODUCT	Site	CID	Name	VLAN	IP WAN	IP WAN CPE	IP LAN	NODE	SWITCH --PUERTO
2	C&W Managed WAN	La Lima AEROPUERTO	6012421.HN	Working	109				HND-LIM01-PE01-LIMA	HND-LIM01-SW-LIMA --FastEthernet1/0/2
3	C&W Managed WAN	La Lima AEROPUERTO	6012421.HN	Protectin	755					
4	C&W Managed WAN	Tegucigalpa	6012428.HN	Working	141				HND-TEG09-PE01-9001	HND-TEG09-SW01-4510 -- FastEthernet1/5
5	C&W Managed WAN	Tegucigalpa	6001328.HN	Protectin	975					
6	C&W Managed WAN	Danli	6012423.HN	Working	154				HND-DAN01-PE01-ME36	HND-DAN01-SW-DANLI-1-- FastEthernet0/28
7	C&W Managed WAN	Danli	6012423.HN	Protectin	162					
8	C&W Managed WAN	La Ceiba	6012431.HN	Working	230				HND-CHM01-PE01-9001	HND-CEI01-SW01-4510---FastEthernet2/3
9	C&W Managed WAN	La Ceiba	6012431.HN	Protectin	N					
10	C&W Managed WAN	La Lima -Estrella Este	6033987.HN	Working	110				HND-LIM01-PE01-LIMA	HND-LIM01-SW-LIMA--Fa1/0/5
11	C&W Managed WAN	La Lima -Estrella Este	6033987.HN	Protectin	N					
12	C&W Managed WAN	Puerto Cortes LA CURVA	6026196.HN	DISCONECTION						
13										
14	C&W Managed WAN	Choluteca	6012422.HN	Working	119				HND-CHO01-PE01-ME36	HND-CHO01-SW01-C4510 -- FastEthernet1/12
15	C&W Managed WAN	Choluteca	6012422.HN	Protectin	304					
16	C&W Managed WAN	San Pedro Sula TEXCO DAVID	6012424.HN	Working	511				HND-SPS01-PE02-ROMA	HND-SPS01-SW01-4510-ROMA--Fa1/13
17	C&W Managed WAN	San Pedro Sula TEXCO DAVID	6012424.HN	Protectin	722				HND-SPS01-PE02-ROMA	
18	C&W Managed WAN	Puerto Cortes LA CURVA	6026196.HN	Working	259				HND-PCO01-PE01-ME36	HND-PCO01-SW01-CORTES--FastEthernet1/0/42
19	C&W Managed WAN	Puerto Cortes LA CURVA	6026196.HN	Protectin	258					
20	C&W Managed WAN	San Pedro Sula Villa Olimpica	6012432.HN	Working	228				HND-SPS02-PE01-9006	HND-SPS02-SWI01-4510-- Fa1/15
21	C&W Managed WAN	San Pedro Sula Villa Olimpica	6012432.HN	Protectin	N					
22	C&W Managed WAN	San Pedro Sula OFICINA PPL	6012429.HN	Working	222				HND-SPS01-PE01-ROMA	HND-SPS01-SW01-4510 -- FastEthernet8/14
23	C&W Managed WAN	San Pedro Sula OFICINA PPL	6012429.HN	Protectin	721					
24	C&W Managed WAN	Choloma	6031045.HN	Working	263	10.215.235.202/31	10.215.235.203/31		HND-CHM01-PE01-9001	HND-CHM01-SW02-ME36 -- Gi0/11
25	C&W Managed WAN	Choloma	6031045.HN	Protectin	335					
26	C&W Managed UTM	San Pedro Sula OFICINA PPL	6030746.HN	Working	222	10.215.234.38/31	10.215.234.39/31		HND-SPS02-PE01-9006	HND-SPS02-SW03-3600 -- GigabitEthernet0/2
27				Protectin	337					
28	C&W Managed WAN	San Pedro Sula METROPOLITA	6012427.HN	Working	N				HND-SPS02-PE01-9006	HND-SPS02-SWI01-4510 -- FastEthernet1/9
29	C&W Managed WAN	San Pedro Sula METROPOLITA	6012427.HN	Protectin	N					
30	C&W Managed WAN	San Pedro Sula EXPOCENTRO	6012426.HN	Working	331				HND-SPS04-PE01-ASR	HND-SPS04-SWI01-4510 -- Fa1/13
31	C&W Managed WAN	San Pedro Sula EXPOCENTRO	6012426.HN	Protectin	374					
32										

Ilustración 24.Recurso Vlans de Gestión COPEMSA

	PRODUCT	Site	CID	Name	VLAN	IP WAN	IP WAN CPE	IP LAN	NODE	SWITCH	PUERTO
2	MPLS	La Lima AEROPUERTO	N	Working	VI28	172.16.0.36	172.16.0.37	192.168.9.0/24	HND-LIM01-PE01-LIMA	HND-LIM01-SW-LIMA	Fa1/0/2
3	MPLS	La Lima AEROPUERTO	6001338.HN	Protecting	VI754	172.16.0.38	172.16.0.39	192.168.10.0/24	HND-SPS03-PE01-9006	HND-SPS03-SW-4510-CEMCOL	Fa3/20
4	MPLS	Tegucigalpa	6001326.HN	Working	VI176	172.16.0.28	172.16.0.29	192.168.8.0/24	HND-TEG09-PE01-9001	HND-TEG09-SW01-4510	Fa1/5
5	MPLS	Tegucigalpa	6001328.HN	Protecting	VI181	172.16.0.30	172.16.0.31	192.168.8.0/24	HND-TEG09-PE01-9001	HND-TEG09-SW01-4510	Fa3/14
6	MPLS	Danli	6001324.HN	Working	VI61	172.16.0.20	172.16.0.21	192.168.6.0/24	HND-DAN01-PE01-ME38	HND-DAN01-SW-DANLI-1	Fa0/28
7	MPLS	Danli	6001345.HN	Protecting	VI63	172.16.0.22	172.16.0.23	192.168.6.0/24	HND-DAN01-PE01-ME38	HND-DAN01-SW-DANLI-2	Fa1/0/31
8	MPLS	La Ceiba	6001318.HN	Working	VI116	172.16.0.12	172.16.0.13	192.168.4.0/24	HND-CEI01-PE01-9006	HND-CEI01-SW01-4510	Fa2/3
9	MPLS	La Ceiba	6001341.HN	Protecting	VI237	172.16.0.14	172.16.0.15	192.168.4.0/24	HND-CEI01-PE01-9006	HND-CEI01-SW01-4510	Fa3/7
10	MPLS	La Lima -Estrella Este (Independe	6001340.HN	Working	VI30	172.16.0.32	172.16.0.33	192.168.9.0/24	HND-LIM01-PE01-LIMA	HND-LIM01-SW-LIMA	Fa1/0/5
11	MPLS	La Lima -Estrella Este	6001332.HN	Protecting	VI237	172.16.0.36	172.16.0.37	192.168.10.0/24	HND-LIM01-PE01-LIMA	HND-LIM01-SW-LIMA	Fa1/0/2
12	MPLS	Choluteca	6001320.HN	Working	VI84	172.30.16.1	172.30.16.2	192.168.5.0/24	HND-CHO01-PE01-ME38	HND-CHO01-SW01-C4510	Fa1/12
13	MPLS	Choluteca	6001319.HN	Protecting	VI115	172.16.0.18	172.16.0.19	192.168.5.0/24	HND-CHO01-PE01-ME38	HND-CHO01-SW01-C4510	Fa2/42
14	MPLS	San Pedro Sula TEXACO DAVID	6001314.HN	Working	VI931	172.16.0.8	172.16.0.9	192.168.3.0/24	HND-SPS01-PE01-ROMA	HND-SPS01-SW01-4510-ROMA	Fa1/13
15	MPLS	San Pedro Sula TEXACO DAVID	6001347.HN	Protecting	VI191	172.16.0.10	172.16.0.11	192.168.3.0/24	HND-SPS03-PE01-9006	HND-SPS03-SW-4510-CEMCOL	Fa2/12
16	MPLS	Puerto Cortes LA CURVA	6026194.HN	Working	VI130	172.16.0.48	172.16.0.49	192.168.13.0/24	HND-PCO01-PE01-ME38-CO	HND-PCO01-SW01-CORTES	Fa1/0/42
17	MPLS	Puerto Cortes LA CURVA	6026195.HN	Protecting	VI131	172.16.0.50	172.16.0.51	192.168.13.0/24	HND-PCO01-PE01-ME38-CO	HND-PCO01-SW01-CORTES	Fa2/0/26
18	MPLS	San Pedro Sula Villa Olimpica	6008769.HN	Working	vI227	172.16.0.40	172.16.0.41	192.168.11.0/24	HND-SPS02-PE01-9006	HND-SPS02-SWI01-4510	Fa1/15
19	MPLS	San Pedro Sula Villa Olimpica	6008770.H	Protecting	VI656	172.16.0.42	172.16.0.43	192.168.11.0/24	HND-SPS01-PE01-ROMA	HND-SPS01-SW01-4510-ROMA	Fa8/11
20	MPLS	Choloma La Victoria	6031043.HN	Working	VI334	172.16.0.52	172.16.0.53	192.168.14.0/24	HND-SPS05-CORE-CANAL7	HND-SPS05-SWI01-4510	Fa3/4
21	MPLS	Choloma La Victoria	6031044.HN	Portecting	VI264	172.16.0.54	172.16.0.55	192.168.14.0/24	HND-CHM01-PE01-9001	HND-CHM01-SW02-ME36	Gi0/11
22	MPLS	San Pedro Sula OFICINA PPL	6001342.HN	Working	VI220	172.16.0.0	172.16.0.1	192.168.1.0/24	HND-SPS02-PE01-9006	HND-SPS02-SW03-3600	Gi0/2
23	MPLS	San Pedro Sula OFICINA PPL	6001311.H	Protecting	VI656	172.16.0.2	172.16.0.3	192.168.1.0/24	HND-SPS01-PE01-ROMA	HND-SPS01-SW01-4510-ROMA	Fa8/14
24	MPLS	San Pedro Sula OFICINA PPL	6001312.H	Internet	VI221	190.5.91.124	190.5.91.125	192.168.1.0/24	HND-SPS02-PE01-9006	HND-SPS02-SW03-3600	Gi0/2
25	MPLS	San Pedro Sula METROPOLITANA	6010016.HN	Working	VI520	172.16.0.44	172.16.0.45	192.168.12.0/24	HND-SPS02-PE01-9006	HND-SPS02-SWI01-4510	Fa1/9
26	MPLS	San Pedro Sula METROPOLITANA	6010017.HN	Protecting	VI523	172.16.0.46	172.16.0.47	192.168.12.0/24	HND-SPS02-PE01-9006	HND-SPS02-SWI01-4510	Fa1/36
27	MPLS	San Pedro Sula EXPOCENTRO	6001316.HN	Working	VI44	172.16.0.24	172.16.0.25	192.168.7.0/24	HND-SPS04-PE01-ASR903	HND-SPS04-SWI01-4510	Fa1/13
28	MPLS	San Prdro Sula EXPOCENTRO	6001329.H	Protecting	VI135	172.16.0.26	172.16.0.27	192.168.7.0/24	HND-SPS05-PE02-CANAL7	HND-SPS05-SWI01-4510	Fa1/3

Ilustración 25. Recurso Vlans MPLS COMPEMSA

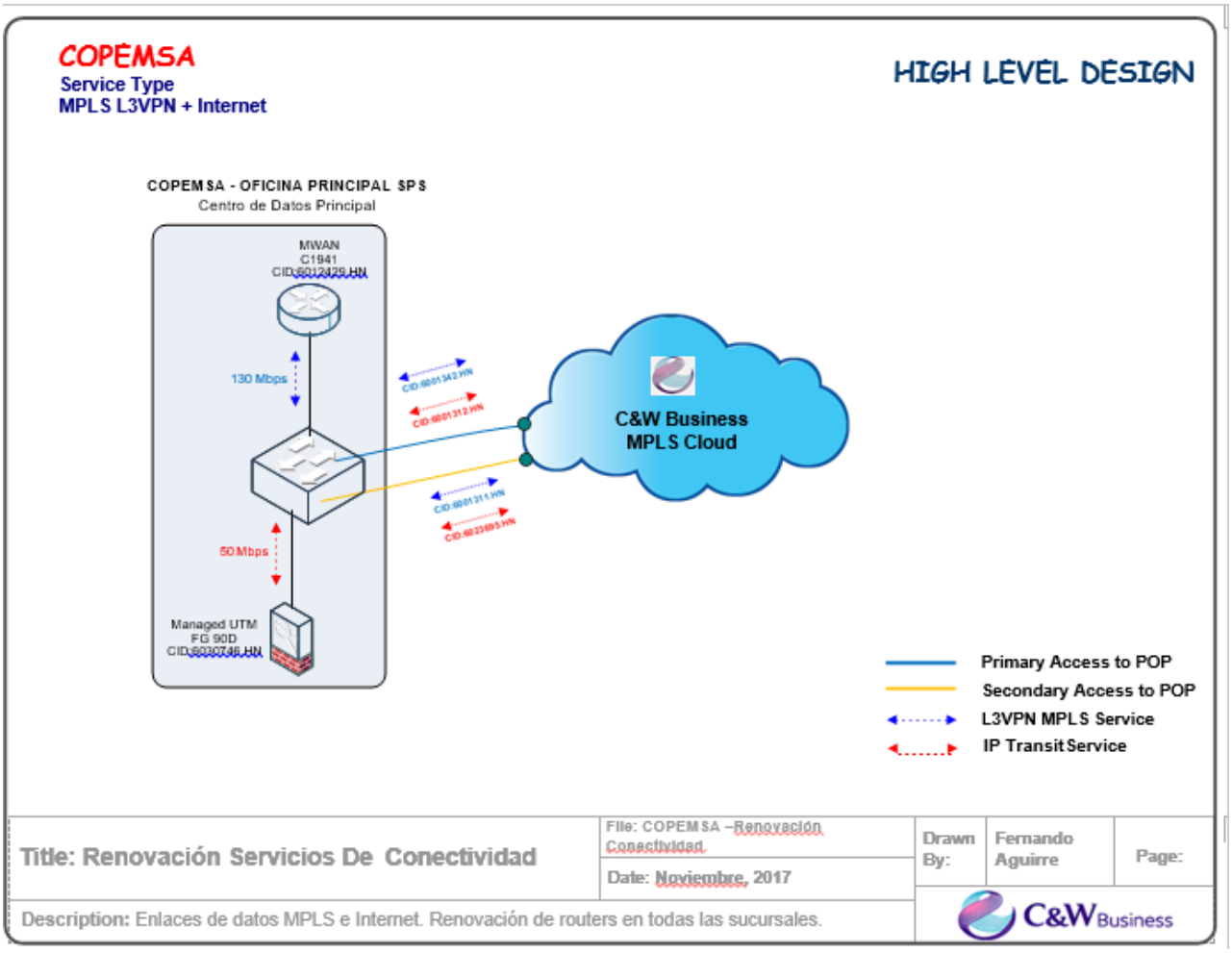


Ilustración 26. Nube MPLS de red COPEMSA

Product	Transaction	Location	Quantity	Notes (PON: | CID:8001341.HN)
C&W MPLS	Renewal	Texaco San Jose La Ceiba, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	N
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:8001318.HN)
C&W MPLS	Renewal	Texaco San Jose La Ceiba, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	Y
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:8012431.HN)
Cisco C881-K9	Disconnection	Texaco San Jose La Ceiba, Honduras	1	.

Product	Transaction	Location	Quantity	Notes (PON: | CID:8033987.HN)
Cisco C881-K9	Disconnection	texaco independencia la lima (Principal) La Lima, Honduras	1	.

Product	Transaction	Location	Quantity	Notes (PON: | CID:8033987.HN)
C&W Managed WAN	Renewal	texaco independencia la lima (Principal) La Lima, Honduras	1	.

	Product	Transaction	Location	Quantity	Notes (PON: | CID:)
Components	C881-K9	New Service	texaco independencia la lima(Principal) La Lima, Honduras	1	Reemplazo de equipo router de 1811 a 881

		Description	Value	Description	Value
Components	Attributes	Management Only	N	WAN Routing Protocol	BGP
		Service Availability	Normal		

Product	Transaction	Location	Quantity	Notes (PON: | CID:8012431.HN)
C&W Managed WAN	Renewal	Texaco San Jose La Ceiba, Honduras	1	.

	Product	Transaction	Location	Quantity	Notes (PON: | CID:)
Components	C881-K9	New Service	Texaco San Jose La Ceiba, Honduras	1	Reemplazo de equipo router Cisco 1811 por un router Cisco 881

		Description	Value	Description	Value
Components	Attributes	Management Only	N	WAN Routing Protocol	BGP
		Service Availability	Normal		

Ilustración 27. Formulario de Servicio de Orden Texaco La Ceiba

Product	Transaction	Location	Quantity	Notes (PON: | CID:6001347.HN)
C&W MPLS	Reconfiguration	texaco David 7 calle sps(Principal) San Pedro Sula, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	N
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:6001314.HN)
C&W MPLS	Renewal	texaco David 7 calle sps(Principal) San Pedro Sula, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	Y
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:6012424.HN)
Cisco C881-K9	Disconnection	texaco David 7 calle sps(Principal) San Pedro Sula, Honduras	1	.

Product	Transaction	Location	Quantity	Notes (PON: | CID:6012424.HN)
C&W Managed WAN	Renewal	texaco David 7 calle sps(Principal) San Pedro Sula, Honduras	1	.

	Product	Transaction	Location	Quantity	Notes (PON: | CID:)
Components	C881-K9	New Service	texaco David 7 calle sps(Principal) San Pedro Sula, Honduras	1	Reemplazo de equipo router Cisco 1811 por un router Cisco 881

		Description	Value	Description	Value
Components	Attributes	Management Only	N	WAN Routing Protocol	BGP
		Service Availability	Normal		

Ilustración 28. Formulario de Servicio de Orden Texaco David 7 Calle

Product	Transaction	Location	Quantity	Notes (PON: | CID:6001349.HN)
C&W MPLS	Renewal	Gasolinera Texaco Hercules puerto cortes(Principal) Puerto Cortes, Honduras	1	-

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	N
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	**False**	Type of MPLS Service	L3VPN
			WAN Routing Protocol	**BGP**
	Local Contact	**Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675**		

Product	Transaction	Location	Quantity	Notes (PON: | CID:6001322.HN)
C&W MPLS	Renewal	Gasolinera Texaco Hercules puerto cortes(Principal) Puerto Cortes, Honduras	1	-

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	Y
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	**False**	Type of MPLS Service	L3VPN
			WAN Routing Protocol	**BGP**
	Local Contact	**Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675**		

Product	Transaction	Location	Quantity	Notes (PON: | CID:6012430.HN)
Cisco C881-K9	Disconnection	Gasolinera Texaco Hercules puerto cortes(Principal) Puerto Cortes, Honduras	1	-

Product	Transaction	Location	Quantity	Notes (PON: | CID:6012430.HN)
C&W Managed WAN	Renewal	Gasolinera Texaco Hercules puerto cortes(Principal) Puerto Cortes, Honduras	1	-

	Product	Transaction	Location	Quantity	Notes (PON: | CID:)
Components	C881-K9	New Service	**Gasolinera Texaco Hercules puerto cortes(Principal) Puerto Cortes,** Honduras	1	Reemplazo de equipo router cisco 1811 por un router Cisco 881

Ilustración 29. Formato de Servicio de Orden Texaco Hércules, Puerto Cortes

Product	Transaction	Location	Quantity	Notes (PON: | CID:6008770.HN)
C&W MPLS	Renewal	villa olimpica por estadio olimpico (Principal) San Pedro Sula, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	N
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:6012432.HN)
C&W Managed WAN	Renewal	villa olimpica por estadio olimpico (Principal) San Pedro Sula, Honduras	1	.

	Product	Transaction	Location	Quantity	Notes (PON: | CID:)
Components	C881-K9	New Service	villa olimpica por estadio olimpico (Principal) San Pedro Sula, Honduras	1	Reemplazo de router 1811 por un router 881

		Description	Value	Description	Value
Components	Attributes	Management Only	N	WAN Routing Protocol	BGP
		Service Availability	Normal		

Product	Transaction	Location	Quantity	Notes (PON: | CID:6008769.HN)
C&W MPLS	Renewal	villa olimpica por estadio olimpico (Principal) San Pedro Sula, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	Y
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Ilustración 30. Formato de Servicio de Orden Texaco Villa Olimpica

Product	Transaction	Location	Quantity	Notes (PON: | CID:8012426.HN)
Cisco C881-K9	Disconnection	texaco expocentro las brisas (Principal) San Pedro Sula, Honduras	1	.

Product	Transaction	Location	Quantity	Notes (PON: | CID:8012426.HN)
C&W Managed WAN	Renewal	texaco expocentro las brisas (Principal) San Pedro Sula, Honduras	1	.

Components	Product	Transaction	Location	Quantity	Notes (PON: | CID:)
	C881-K9	New Service	texaco expocentro las brisas(Principal) San Pedro Sula, Honduras	1	Cambio de equipo router 1811 por un router 881

Components		Description	Value	Description	Value
	Attributes	Management Only	N	WAN Routing Protocol	BGP
		Service Availability	Normal		

Product	Transaction	Location	Quantity	Notes (PON: | CID:8001316.HN)
C&W MPLS	Renewal	texaco expocentro las brisas (Principal) San Pedro Sula, Honduras	1	.

	Description	Value	Description	Value
	Bandwidth (Mbps)	10	Primary	Y
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
Attributes				

	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:8001329.HN)
C&W MPLS	Renewal	texaco expocentro las brisas (Principal) San Pedro Sula, Honduras	1	.

	Description	Value	Description	Value
	Bandwidth (Mbps)	10	Primary	N
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
Attributes	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Name: Carlos Zelaya Email: carlos.zelaya@live.com			

Ilustración 31. Formato de Servicio de Orden Texaco Expocentro

Product	Transaction	Location	Quantity	Notes (PON: | CID:6012421.HN)
Cisco C881-K9	Disconnection	texaco aeropuerto antes de Jogo a La Lima(Principal) La Lima, Honduras	1	.

Product	Transaction	Location	Quantity	Notes (PON: | CID:6012421.HN)
C&W Managed WAN	Renewal	texaco aeropuerto antes de Jogo a La Lima(Principal) La Lima, Honduras	1	.

Components	Product	Transaction	Location	Quantity	Notes (PON: | CID:)
	C881-K9	New Service	texaco aeropuerto antes de Jogo a La Lima(Principal) La Lima, Honduras	1	Cambio de router cisco 1811 por un router 881

Components	Attributes	Description	Value	Description	Value
		Management Only	N	WAN Routing Protocol	BGP
		Service Availability	Normal		

Product	Transaction	Location	Quantity	Notes (PON: | CID:6001334.HN)
C&W MPLS	Renewal	texaco aeropuerto antes de Jogo a La Lima(Principal) La Lima, Honduras	1	.

Attributes	Description	Value	Description	Value
	Bandwidth (Mbps)	10	Primary	Y
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:6001338.HN)
C&W MPLS	Renewal	texaco aeropuerto antes de Jogo a La Lima(Principal) La Lima, Honduras	1	.

Attributes	Description	Value	Description	Value
	Bandwidth (Mbps)	10	Primary	N
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Ilustración 32. Formato de Servicio de Orden Texaco Aeropuerto

Product	Transaction	Location	Quantity	Notes (PON: | CID:8012427.HN)
Cisco C881-K9	Disconnection	texaco metropolitana entrada a sps por toyota(Principal) San Pedro Sula, Honduras	1	.

Product	Transaction	Location	Quantity	Notes (PON: | CID:8010016.HN)
C&W MPLS	Renewal	texaco metropolitana entrada a sps por toyota(Principal) San Pedro Sula, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	Y
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:8010017.HN)
C&W MPLS	Renewal	texaco metropolitana entrada a sps por toyota(Principal) San Pedro Sula, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	N
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:8012427.HN)
C&W Managed WAN	Renewal	texaco metropolitana entrada a sps por toyota(Principal) San Pedro Sula, Honduras	1	.

	Product	Transaction	Location	Quantity	Notes (PON: | CID:)
Components	C881-K9	New Service	texaco metropolitana entrada a sps por toyota(Principal) San Pedro Sula, Honduras	1	Cambio de Router 1811 a router 881

		Description	Value	Description	Value
Components	Attributes	Management Only	N	WAN Routing Protocol	BGP
		Service Availability	Normal		

Ilustración 33. Formato de Servicio de Orden Texaco Metropolitana

Product	Transaction	Location	Quantity	Notes (PON: | CID:8001326.HN)
C&W MPLS	Renewal	Gasolinera Texaco Milenium (Principal) San Pedro Sula, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	Y
	Circuit End Point	Local	CpS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:8001328.HN)
C&W MPLS	Renewal	Gasolinera Texaco Milenium (Principal) San Pedro Sula, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	N
	Circuit End Point	Local	CpS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
			Type of MPLS Service	L3VPN

	Demarcation Equipment : Accedian	False	WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:8012428.HN)
Cisco C881-K9	Disconnection	Gasolinera Texaco Milenium (Principal) San Pedro Sula, Honduras	1	.

Product	Transaction	Location	Quantity	Notes (PON: | CID:8001345.HN)
C&W MPLS	Renewal	dapil centro texaco(Principal) Dapil, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	N
	Circuit End Point	Local	CpS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation	False	Type of MPLS Service	L3VPN

Ilustración 34. Formato de Servicio de Orden Texaco Milenium

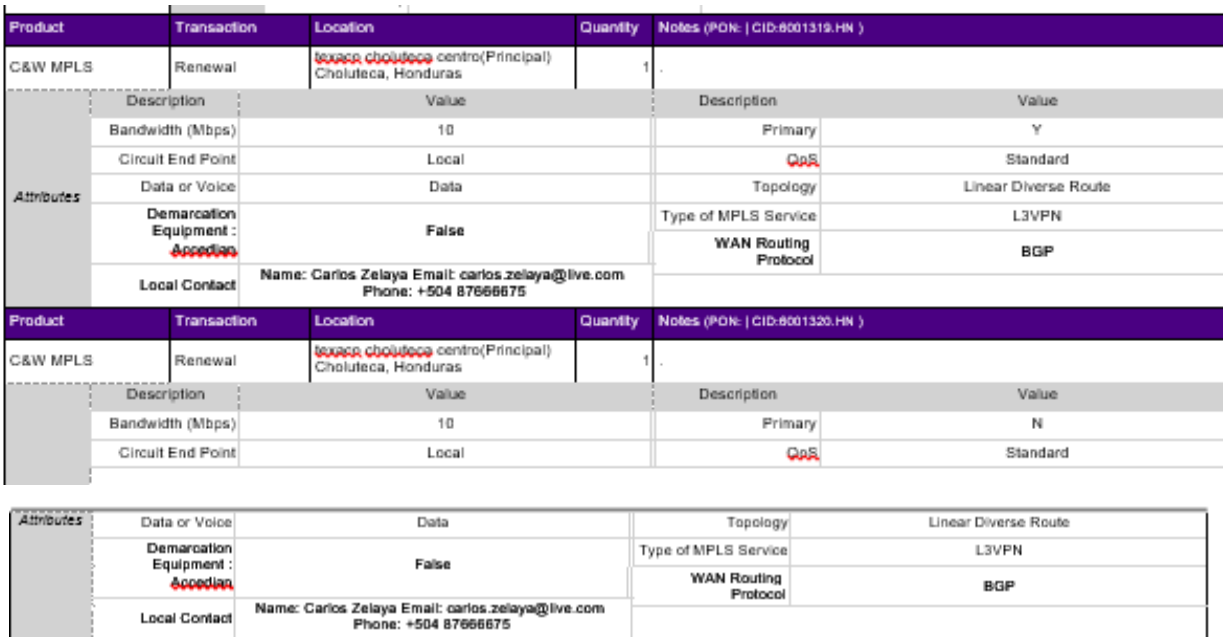
Product	Transaction	Location	Quantity	Notes (PON: | CID:6001345.HN)
C&W MPLS	Renewal	dapl centro texaco(Principal) Dapl, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	N
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	**False**	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	**Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675**		

Product	Transaction	Location	Quantity	Notes (PON: | CID:6001324.HN)
C&W MPLS	Renewal	dapl centro texaco(Principal) Dapl, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	Y
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	**False**	Type of MPLS Service	L3VPN
			WAN Routing Protocol	**BGP**
	Local Contact	**Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675**		

Ilustración 35. Formato de Servicio de Orden Texaco Danli



Product	Transaction	Location	Quantity	Notes (PON: | CID:8001319.HN)
C&W MPLS	Renewal	texaco choluteca centro(Principal) Choluteca, Honduras	1	.

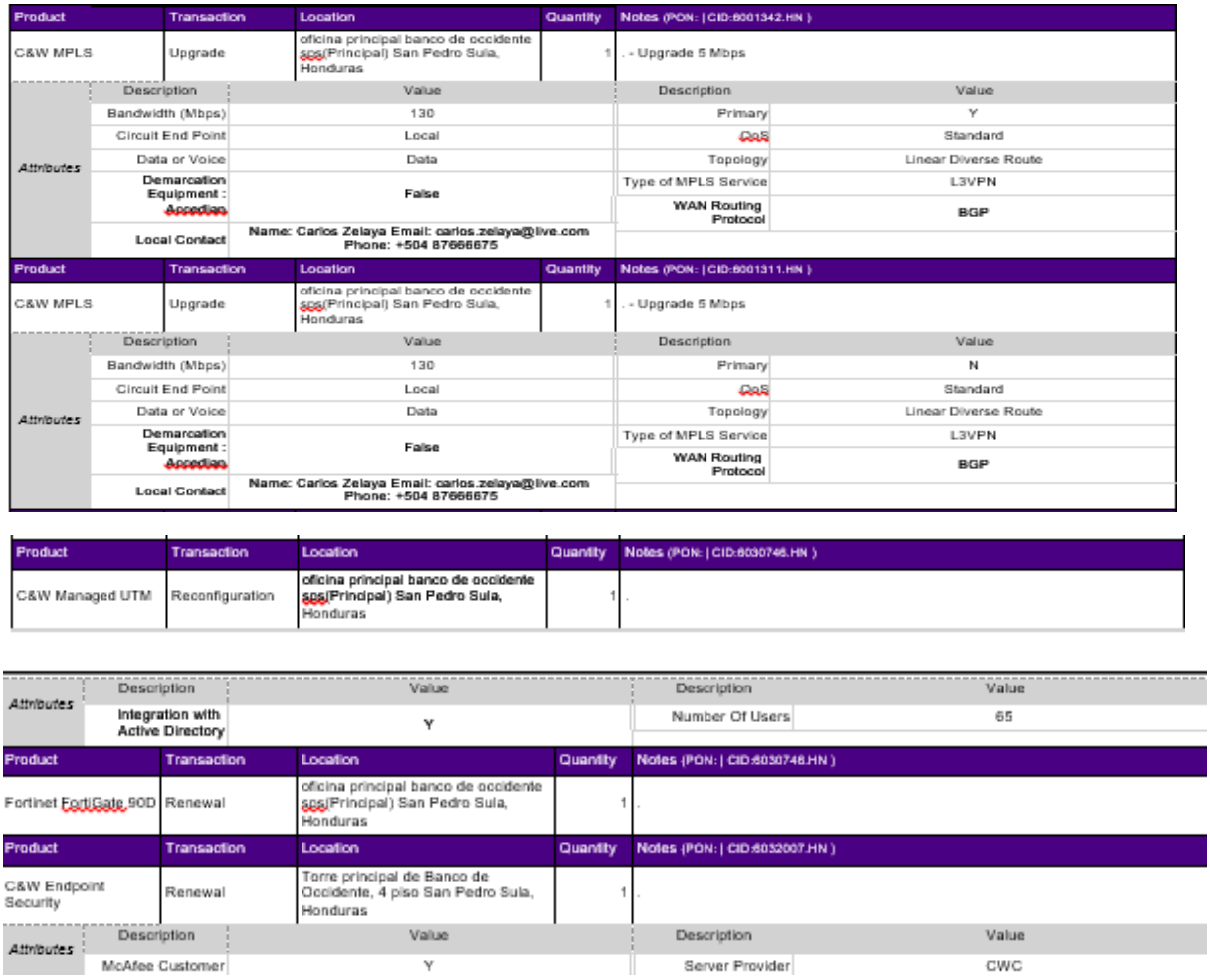
Attributes	Description	Value	Description	Value
	Bandwidth (Mbps)	10	Primary	Y
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	**False**	Type of MPLS Service	L3VPN
			WAN Routing Protocol	**BGP**
	Local Contact	**Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675**		

Product	Transaction	Location	Quantity	Notes (PON: | CID:8001320.HN)
C&W MPLS	Renewal	texaco choluteca centro(Principal) Choluteca, Honduras	1	.

	Description	Value	Description	Value
	Bandwidth (Mbps)	10	Primary	N
	Circuit End Point	Local	QoS	Standard

Attributes	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	**False**	Type of MPLS Service	L3VPN
			WAN Routing Protocol	**BGP**
	Local Contact	**Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675**		

Ilustración 36. Formato de Servicio de Orden Texaco Choluteca Principal



Product	Transaction	Location	Quantity	Notes (PON: | CID:8001342.HN)
C&W MPLS	Upgrade	oficina principal banco de occidente sps(Principal) San Pedro Sula, Honduras	1	- Upgrade 5 Mbps

Attributes	Description	Value	Description	Value
	Bandwidth (Mbps)	130	Primary	Y
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:8001311.HN)
C&W MPLS	Upgrade	oficina principal banco de occidente sps(Principal) San Pedro Sula, Honduras	1	- Upgrade 5 Mbps

Attributes	Description	Value	Description	Value
	Bandwidth (Mbps)	130	Primary	N
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:8030746.HN)
C&W Managed UTM	Reconfiguration	oficina principal banco de occidente sps(Principal) San Pedro Sula, Honduras	1	.

Attributes	Description	Value	Description	Value
	Integration with Active Directory	Y	Number Of Users	65

Product	Transaction	Location	Quantity	Notes (PON: | CID:8030746.HN)
Fortinet FortiGate 90D	Renewal	oficina principal banco de occidente sps(Principal) San Pedro Sula, Honduras	1	.

Product	Transaction	Location	Quantity	Notes (PON: | CID:8032007.HN)
C&W Endpoint Security	Renewal	Torre principal de Banco de Occidente, 4 piso San Pedro Sula, Honduras	1	.

Attributes	Description	Value	Description	Value
	McAfee Customer	Y	Server Provider	CWC

Ilustración 37. Formato de Servicio de Orden Oficina Principal, Banco de Occidente

Product	Transaction	Location	Quantity	Notes (PON: | CID:8026196.HN)
Cisco C881-K9	Disconnection	texaco la curva Puerto Cortes San Pedro Sula, Honduras	1	.

Product	Transaction	Location	Quantity	Notes (PON: | CID:8026196.HN)
C&W Managed WAN	Renewal	texaco la curva Puerto Cortes San Pedro Sula, Honduras	1	.

	Product	Transaction	Location	Quantity	Notes (PON: | CID:)
Components	C881-K9	New Service	texaco la curva Puerto Cortes San Pedro Sula, Honduras	1	Reemplazo de router 1811 por un equipo 881

		Description	Value	Description	Value
Components	Attributes	Management Only	N	WAN Routing Protocol	BGP
		Service Availability	Normal		

C&W MPLS	Renewal	texaco la curva Puerto Cortes San Pedro Sula, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	Y
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:8026195.HN)
C&W MPLS	Renewal	texaco la curva Puerto Cortes San Pedro Sula, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	N
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Ilustración 38. Formato de Servicio de Orden Texaco La Curva Puerto Cortés

Product	Transaction	Location	Quantity	Notes (PON: | CID:6001332.HN)
C&W MPLS	Renewal	texaco independencia la lima (Principal) La Lima, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	Y
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:6001340.HN)
C&W MPLS	Renewal	texaco independencia la lima (Principal) La Lima, Honduras	1	.

	Description	Value	Description	Value
Attributes	Bandwidth (Mbps)	10	Primary	N
	Circuit End Point	Local	QoS	Standard
	Data or Voice	Data	Topology	Linear Diverse Route
	Demarcation Equipment : Accedian	False	Type of MPLS Service	L3VPN
			WAN Routing Protocol	BGP
	Local Contact	Name: Carlos Zelaya Email: carlos.zelaya@live.com Phone: +504 87666675		

Product	Transaction	Location	Quantity	Notes (PON: | CID:6028194.HN)

Ilustración 39. Formato de Servicio de Orden Texaco La Lima