UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

APLICACIÓN DEL PROTOCOLO DE ENRUTAMIENTO BGP EN REDES DE ACCESO MPLS-VPN

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE TELECOMUNICACIONES

PRESENTADO POR:

CÉSAR JUAN BEAS VALDEZ

PROMOCIÓN

2007 - II

LIMA – PERÚ

2012

APLICACIÓN DEL PROTOCOLO DE ENRUTAMIENTO BGP EN REDES DE ACCESO MPLS-VPN

DEDICATORIA

A mis queridos padres, que han sido siempre una fuente constante de valores y compromiso, un ejemplo y modelo a seguir.

SUMARIO

El mundo de la integración de servicios de datos y voz a nivel corporativo hace que las empresas u organizaciones con oficinas distribuidas en el ámbito nacional tengan la necesidad de contar con un servicio que les permita la centralización del procesamiento y almacenamiento de la información que utilizan.

Para ello, establecen un socio tecnológico que en la mayoría de las veces es un proveedor de servicios de TI. Este último ofrece una infraestructura que le permite brindar servicios, tales como, un centro de cómputo con estructuras y espacios acondicionados, climatización, energía y una plataforma de red adecuada que permita la conectividad y alta disponibilidad de su información y aplicaciones.

Para lograr esto, es lograr habilitar la conectividad de red entre las oficinas distribuidas de la empresa y el centro de cómputo del proveedor de servicios de TI, para lo cual se establece un segundo socio tecnológico, quien por un factor económico es un proveedor de servicios de Telecomunicaciones. Este último ofrece una infraestructura de red de datos que brinda servicios y soluciones de conectividad. Lo más resaltante a través del uso de nuevas tecnologías de enrutamiento y conmutación de paquetes en la red del proveedor, tales como la MPLS y el protocolo BGP, es la capacidad de segmentar ésta red de transporte, permitiendo de forma segura lograr la conectividad extremo a extremo brindando niveles de calidad de servicio (QoS) y permitiendo la escalabilidad futura de la red.

INDICE GENERAL

INTRODUCCIÒN

Son muchas las plataformas utilizadas por los proveedores para permitir el transporte de los datos a través de su red, entre ellas: Frame Relay, ATM, ISDN, etc.
Dada la creciente necesidad de las empresas por contar con un servicio cada vez con mayores prestaciones en cuanto a velocidad y permita lograr una conectividad de todas las sucursales entre sí, sin depender de una sucursal principal y por el lado del proveedor de Telecomunicaciones que sea fácilmente administrable en cuanto a horas hombre, surge una tecnología de conmutación de paquetes llamada MPLS,
La implementación de una red MPLS requiere desde el punto de vista de proveedor el uso de un protocolo de enrutamiento con la escalabilidad necesaria, acorde con el requerimiento actual y futuro de nuevos clientes. Por este motivo se utiliza el protocolo de enrutamiento BGP, el cual permite el intercambio automático de información de enrutamiento entre la red del cliente y la red del proveedor.

CAPÌTULO I
PLANTEAMIENTO DE INGENIERÍA DEL PROBLEMA

1.1. Descripción del problema

Se presenta la necesidad de implementar los servicios de conectividad de red con el objeto de interconectar el centro de datos corporativo con las sedes de las empresas miembros de Fonafe.

El servicio requiere una política de calidad de servicio que permita la priorización y asignación de un determinado caudal de BW, de acuerdo al tipo de tráfico.

Para nuestro caso, se muestra el escenario con la sede principal donde se encuentra el centro de datos corporativo ubicado en IBM y la una de las sedes remotas ubicada en Arequipa, empresa Seal. Se tiene la necesidad de contar con enlaces de respaldo tanto en la sede principal como en la sede remota que permitan la conmutación automática del tráfico en casos de falla en el enlace principal.

De manera automática implica que esta conmutación será transparente para el cliente, el cual no percibirá eventos en sus servicios durante y después de la falla.

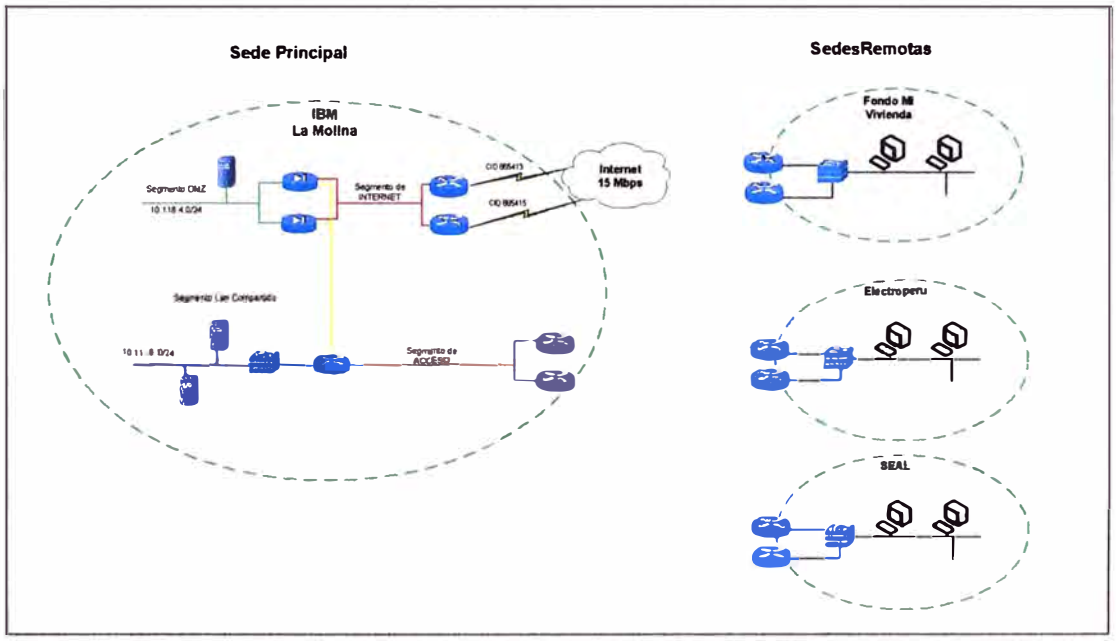


Figura 1.1 Diagrama de red de la sede principal y sedes remotas.

1.2. Objetivo del trabajo

Implementar una solución que permita la conectividad y la alta disponibilidad de

las comunicaciones entre la sede principal y las sedes remotas, de acuerdo a la necesidad de la empresa y utilizando las tecnologías actuales, tales como MPLS como protocolo de conmutación en la red backbone del proveedor y el uso del protocolo BGP para la configuración del enrutamiento dinámico que permita habilitar la comunicación entre el equipo ruteador del cliente y el equipo ruteador de borde del backbone MPLS del proveedor; asimismo esta solución debe permitir la alta disponibilidad en los enlaces de la sede principal y sedes remotas.

Finalmente, se mostrará las pruebas de alta disponibilidad realizadas.

1.3. Evaluación del Problema

En la actualidad, las necesidades de las empresas por contar con servicios de Telecomunicaciones es imprescindible, dado el requerimiento de contar de manera constante con el acceso a la información, servicios en tiempo real tales como la voz y acceso centralizado a internet. Es por este motivo que se tiene la necesidad de contar con servicios de transporte de la información que ofrezcan calidad de servicio y alta disponibilidad en sus enlaces.

1.4. Limitaciones del trabajo

Para el presente trabajo se ha utilizado BGP como protocolo de enrutamiento entre el router del cliente y el router del proveedor y ruteo estático dentro de la red LAN del cliente; sin embargo no se considera el uso de un protocolo de ruteo dinámico en la red LAN del cliente con el objeto de habilitar la redistribución automática de rutas, dado que ello depende de la administración de la red del cliente final.

1.5. Síntesis del Informe

En el primer capítulo se muestra el requerimiento de necesidad de conectividad de la empresa Fonafe (Fondo Nacional de Financiamiento de la Actividad Empresarial del Estado) cuya necesidad principal es la de comunicar las empresas miembro que la conforman con el centro de cómputo donde se encuentran los servicios de intranet, bases de datos, acceso a correo e internet.

Dentro de las empresas que conforman Fonafe, podemos mencionar:

- Corpac S.A.
- Electrocentro
- Electro Noroeste
- Electro Norte
- Hidrandina

- Electroperú S.A.
- Enapu S.A.
- Fonafe
- Seal
- Fondo Mi Vivienda S.A. (FMV o FONDO MiVivienda)
- Serpost S.A.

En el segundo capítulo nos centraremos en desarrollar y entender los conceptos que proporcionan la tecnología de enrutamiento y conmutación de paquetes utilizada en la red de proveedor, tales como son el protocolo BGP y el protocolo MPLS.

En el tercer capítulo se desarrollará el planteamiento de la solución a la necesidad indicada en el primer capítulo, mostrando la implementación realizada en una de las sedes remotas, tomando como modelo la empresa Seal. En esta implementación se muestra el esquema de red utilizado, tanto en la sede remota (Seal) como en el centro de datos corporativo instalado en el centro de cómputo del proveedor de TI, así como el tipo de equipos utilizados, el plan de direccionamiento, la implementación del protocolo BGP y las pruebas de alta disponibilidad realizadas en los enlaces de esta sede remota.

Finalmente, en el cuarto capítulo se muestran las conclusiones finales y recomendaciones.

CAPITULO II
MARCO TEÓRICO

2.1. Protocolos de enrutamiento Interior y Exterior

2.1.1. Sistemas Autónomos

Un Sistema Autónomo (AS) es un conjunto de redes y dispositivos de enrutamiento que cuenta con una política común de encaminamiento.

2.1.2. Protocolo de enrutamiento Interior (IGP)

Es aquel protocolo de enrutamiento que intercambia información de enrutamiento dentro de un Sistema Autónomo. Ejemplos : RIP, IGRP, EIGRP, OSPF, IS-IS.

2.1.3. Protocolo de enrutamiento Exterior (EGP)

Es aquel protocolo de enrutamiento que interconecta diferentes Sistemas Autónomos. Ejemplo: BGP.

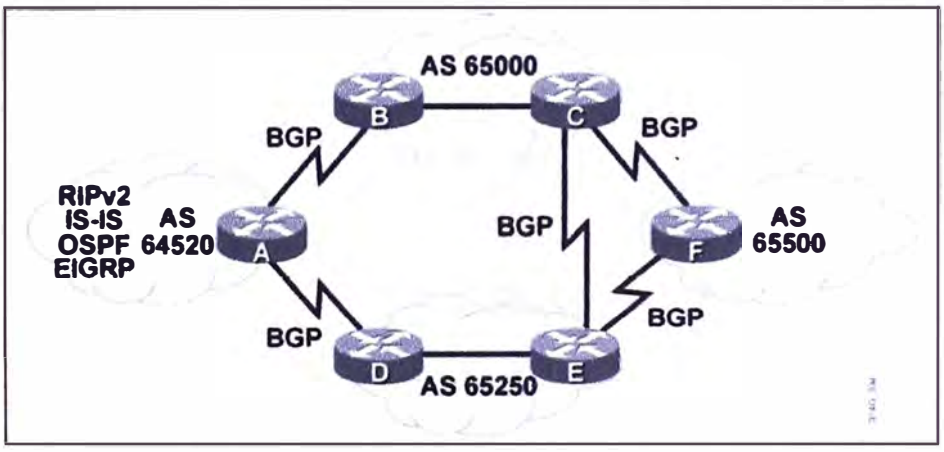


Figura 2.1 Red con protocolos de enrutamiento exterior (Fuente: www.cisco.com)

2.2. Protocolo de enrutamiento BGP

BGP es un protocolo de enrutamiento cuya principal función es la de proveer un sistema de enrutamiento entre-dominios que garantiza un intercambio de información de enrutamiento libre de loops entre Sistemas Autónomos.

BGP4 es la última versión de BGP, la cual se relaciona con los RFC 1771, 1772, 1773, 1774, 1863, 1930, 1965, 1966, 1997, 1998, 2042, 2283, 2385, and 2439.

La Internet utiliza BGP4 para conectar ISP's entre sí, y conectar las empresas a los ISP. BGP4 transporta una máscara de red por cada red anunciada, y soporta VLSM y CIDR. Los predecesores de BGP4 no soportaban estas capacidades, las cuales son obligatorias en la Internet de hoy.

Un protocolo de enrutamiento interno busca el menor camino para llegar desde un punto a otro dentro de una red corporativa; por ejemplo, RIP busca el menor número de dispositivos capa 3 (saltos) para alcanzar la red de destino. OSPF y EIGRP buscan el camino que tenga la mayor velocidad acorde con el BW asignado a la interfaz de red.

BGP es un protocolo de enrutamiento externo, el cual no ve la velocidad para elegir el mejor camino. BGP es un protocolo de enrutamiento basado en políticas que permite a un Sistema Autónomo controlar el flujo de tráfico que ingresa y sale de él, a través del uso de atributos de camino BGP.

2.2.1. BGP Path-vector Routing

Los routers BGP intercambian información de enrutamiento llamada "path-vector" los cuales están elaborados a partir de un conjunto de atributos, similares a las métricas en los protocolos de enrutamiento IGP.

Esta información "path-vector" incluye una lista del camino de Sistemas Autónomos necesarios para alcanzar a una red destino.

Los protocolos de enrutamiento IGP anuncian redes y describen en menor costo para alcanzar estas redes.

BGP anuncia el AS pathway a un Sistema Autónomo destino. BGP describe este pathway utilizando atributos, tales como la dirección IP para llegar al siguiente Sistema Autónomo (atributo next-hop), e indicar como las redes al final del pathway fueron introducidas en BGP (atributo origin code).

Muchos otros atributos BGP, además del next-hop y origin code, son también usados para describir el pathway y las redes al final del pathway.

Un AS sólo publicará el mejor camino para alcanzar una cierta red en un AS destino.

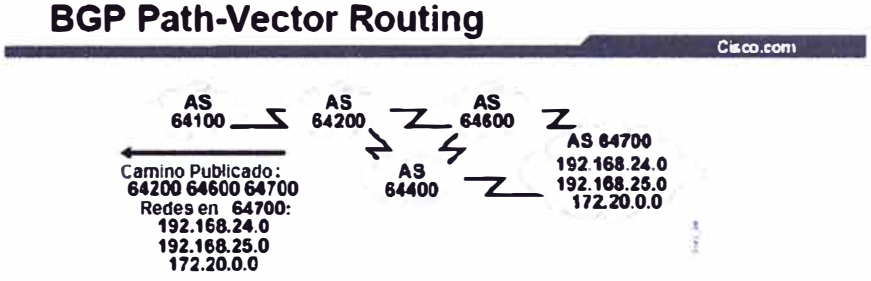


Figura 2.2 Enrutamiento BGP Vector-Camino (Fuente: www.cisco.com)

2.2.2. Características de BGP

BGP utiliza TCP (puerto 179) como protocolo de transporte el cual provee una entrega orientada a conexión.

Un router utilizando BGP forma una conexión TCP con el otro intercambiando mensajes para abrir y confirmar los parámetros de la conexión. Estos dos routers son llamados *peers* o *vecinos*.

Los peers BGP intercambian su tabla de enrutamiento completa luego que la conexión esta establecida; luego de esto envían sólo las actualizaciones cuando hay cambios, no de manera periódica. BGP envía mensajes *Keepalive*, similar a los mensajes *Hello* enviados por OSPF y EIGRP.

BGP es el único protocolo de enrutamiento IP que utiliza TCP como su protocolo de transporte. OSPF, IGRP y EIGRP residen directamente en la capa IP y RIPv1, RIPv2 utilizan UDP como su protocolo de transporte.

OSPF y EIGRP tienen su propia función interna para asegurar que los paquetes de actualización serán explícitamente reconocidos (*acknowledged*). Estos protocolos usan una ventana *one-for-one* tal que si cualquiera OSPF o EIGRP tienen múltiples paquetes que enviar, el siguiente paquete no puede ser enviado hasta que se ha recibido un acknowledgment del paquete anterior.

Este proceso puede ser muy ineficiente y causar latencia si miles de paquetes de actualización deben ser intercambiados sobre enlaces seriales de baja velocidad. OSPF y EIGRP raramente tienen miles de paquetes de actualización que enviar.

EIGRP puede contener más de 100 redes en un paquete de actualización EIGRP. Cien paquetes de actualización EIGRP pueden contener hasta 10,000 redes; la mayoría de organizaciones no tienen 10,000 redes en sus corporaciones .Por otra parte, BGP tiene más de 120,000 redes que actualizar.

TCP maneja la función de *acknowledgment* para BGP. TCP utiliza una ventana dinámica que permite una cantidad de 65,576 bytes ser enviados antes de parar y esperar y esperar para un *acknowledgment.*

Por tanto, si BGP envía paquetes de 1,000 bytes, no se tiene que esperar a que el primer paquete sea reconocido (*acknowledged)* antes de enviar el segundo paquete. Con paquetes de 1,000 bytes y una ventana de 65,000 bytes, se necesitaría que 65 paquetes no hayan sido reconocidos *(acknowledged)* para tener que parar y esperar por su reconocimiento.

TCP está diseñado para el uso de ventanas deslizantes, donde el receptor realizará el reconocimiento de los paquetes en el punto medio del tamaño de ventana que se está enviando. Este método permite a cualquier aplicación TCP continuar enviando paquetes

sin tener que parar y esperar como OSPF o EIGRP requieren.
BGP está diseñado para ser utilizado en grandes redes, tales como: Internet.

2.2.3. Bases de Datos BGP

BGP utiliza las siguientes tablas para almacenar la información que es enviada y recibida de otros routers.

-Tabla de vecinos

Es el listado de todos los vecinos BGP.

-Base de datos Topológica

Es el listado de todas las rutas que han sido aprendidas de cada vecino BGP.

-Tabla de Enrutamiento IP

Es el listado de las mejores rutas para cada red destino, las cuales han sido seleccionadas de la Base de datos Topológica.

Para establecer una adyacencia BGP, se configura ello explícitamente para cada vecino.

BGP forma una relación TCP con cada uno de los vecinos configurados y mantiene un seguimiento del estado de estas relaciones con el envío de mensajes periódicos *keepalive.*

Por defecto estos mensajes *keepalive* se envían cada 60 segundos.

Luego que se ha establecido la adyacencia, los vecinos (*neighbors*) intercambian las rutas BGP en su tabla de enrutamiento IP. Estas rutas son recolectadas de cada vecino con quien ha establecido una adyacencia, y son almacenadas en la *base de datos topológica* BGP. Las mejores rutas para cada red destino son seleccionadas de la *base de datos topológica* BGP utilizando el proceso de selección de rutas BGP y finalmente enviadas a la *tabla de enrutamiento* IP.

La *tabla de enrutamiento* IP compara las rutas BGP enviadas con otros caminos posibles a esas redes destino (si es que existen) y la mejor ruta, basada en la distancia administrativa es instalada finalmente en la *tabla de enrutamiento* IP.

Rutas BGP externas (rutas BGP aprendidas de un Sistema Autónomo externo) tienen una distancia administrativa de 20. Rutas BGP internas (rutas BGP aprendidas dentro del Sistema Autónomo) tienen una distancia administrativa de 200.

2.2.4. Tipos de Mensajes BGP

A continuación se muestran los tipos de mensajes BGP y sus funciones:

-Open

Luego de establecerse la conexión TCP, el primer mensaje enviado por cada lado es un mensaje *Open.* Luego que cada lado acepta este mensaje (a través de un mensaje

Keepalive) y establece la conexión BGP, los *neigbors* BGP pueden intercambiar los mensajes de tipo: *Update, Keepalive, y Notification.*

-Keepalive

Los mensajes *Keepalive* son intercambiados entre vecinos BGP de manera frecuente con el objeto de evitar que el temporizador *Hold Timer* expire.

-Update

Un mensaje *Update* cuenta con información de un *Path* (camino). La información acerca de atributos referidos a este *Path* y las redes que son alcanzables a través de él se encuentran dentro de éste mensaje.

-Notification

Un mensaje de tipo *Notification* es enviado cuando una condición de error es detectada y por tanto, la conexión BGP es cerrada inmediatamente.

Los *neighbors* (vecinos) BGP inicialmente intercambian su tabla de enrutamiento BGP completa. Luego, mensajes *Update* son enviados sólo cuando suceden cambios topológicos en la red. Los *neighbors* BGP envían mensajes *Keepalive* para asegurar que la conexión entre los *neighbors* todavía existe; en caso encontrar errores o condiciones especiales en la conexión, enviarán mensajes de tipo *Notification*.

2.2.5. BGP Conceptos y Terminología

Un solo router no puede manejar las comunicaciones con todos los routers que corren BGP.

Hay más de 20,000 routers que corren BGP y están conectados a la Internet, representando más de 10,000 Sistemas Autónomos. Un router forma una directa relación de vecindad con un número limitado de otros routers BGP. A través de estos *neighbors*, un router BGP aprende acerca de caminos a través de Internet para alcanzar cualquier red publicada.

Todo router que corre el protocolo BGP es conocido como BGP *speaker.*

El término *peer* o *neighbor* BGP se refiere a un BGP *speaker* que está configurado para formar una relación de vecindad con otro BGP *speaker* con el propósito de intercambiar información de enrutamiento BGP entre ellos.

Un BGP *speaker* tiene un número limitado de BGP *neighbors* con los cuales se enlaza y forma una relación basada en TCP.

Un *neighbor* o *peer* BGP es configurado a través del comando *bgp neighbor*, donde se le indica al router, establecer una relación de vecindad con la dirección IP indicada luego del comando *neighbor* e intercambiar actualizaciones de enrutamiento BGP con éste vecino.

Los *neighbors* o *peers* BGP son conocidos como *neighbors* y pueden ser Internos o

Externos al Sistema Autónomo.

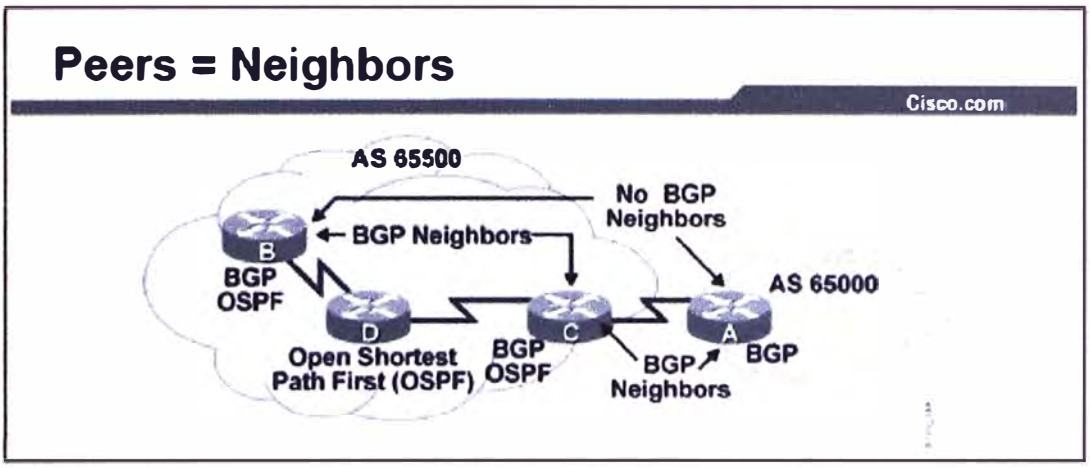


Figura 2.3 Neighbors BGP (Fuente: www.cisco.com)

a) External BGP Neighbors (EBGP)

BGP que corre en routers de diferentes Sistemas Autónomos es llamado External BGP (EBGP). Por defecto, estos routers deben estar directamente conectados entre sí.

No se admite algún protocolo de enrutamiento interno (RIP, OSPF, EIGRP, etc) corriendo entre los EBGP *neighbors*, por lo que las direcciones utilizadas en el comando *neighbor* deben ser alcanzables sin el uso de ellos.

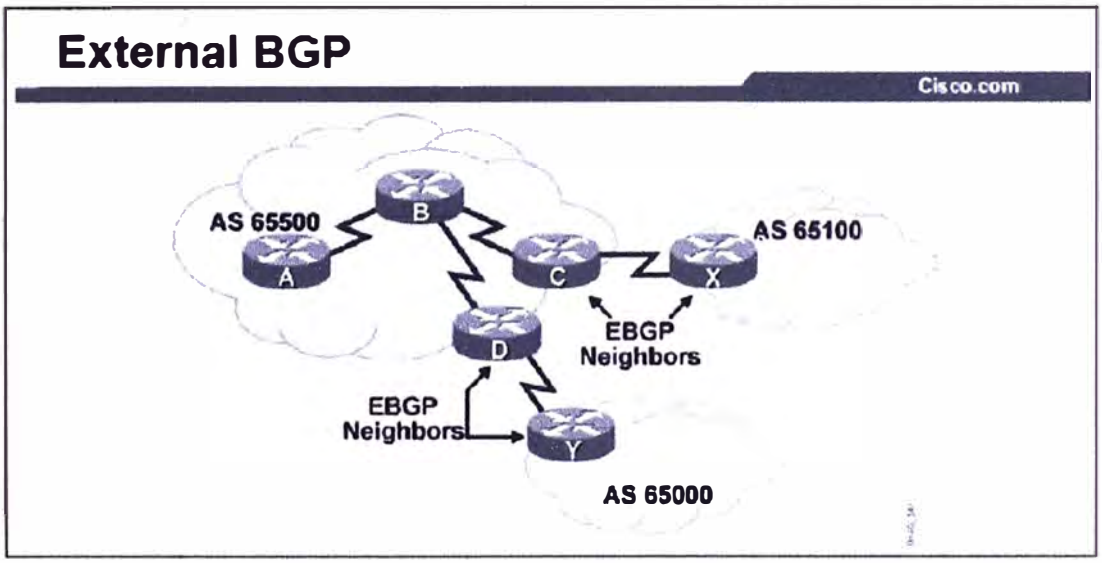


Figura 2.4 External BGP (Fuente: www.cisco.com)

b) Internal BGP Neighbors (IBGP)

BGP que corre en routers dentro del mismo Sistema Autónomo es llamado IBGP..

Luego de comando *neighbor* la dirección IP utilizada debe ser alcanzable por el *neighbor* IBGP. Esto puede lograrse a través del uso de rutas estáticas ó algún protocolo de enrutamiento interno (RIP, OSPF, EIGRP, etc).

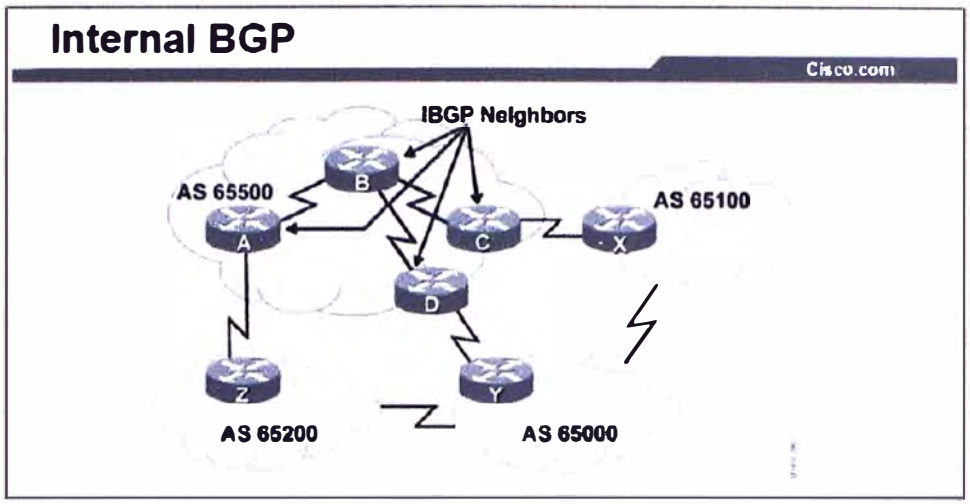


Figura 2.5 Internal BGP (Fuente: www.cisco.com)

- IBGP Full Mesh and Split Horizon rule

Dentro de un Sistema Autónomo es necesario que los *neighbors* IBGP estén habilitados de modo "*full mesh*" (todos contra todos) con el objeto de prevenir loops de enrutamiento.

La regla que gobierna el comportamiento de los *neighbors* IBGP es *Split Horizon*.

Para evitar loops de enrutamiento dentro de un Sistema Autónomo la regla *Split Horizon* especifica que las rutas aprendidas vía IBGP no podrán ser propagadas a otros *neighbors* IBGP.

Haciendo una habilitación del tipo *full mesh* en IBGP, cuando un cambio es recibido desde un Sistema Autónomo externo, el router BGP del Sistema Autónomo local es el responsable de informar a todos los *neighbors* IBGP del cambio.

Los *neighbors* IBGP que reciben este *Update* no lo envían a otro *neighbor* IBGP, porque ellos asumen que el *neighbor* del que recibieron este Update tiene una conexión *full mesh* con el resto de *neighbors* IBGP y por tanto, ha enviado a todos ésta actualización.

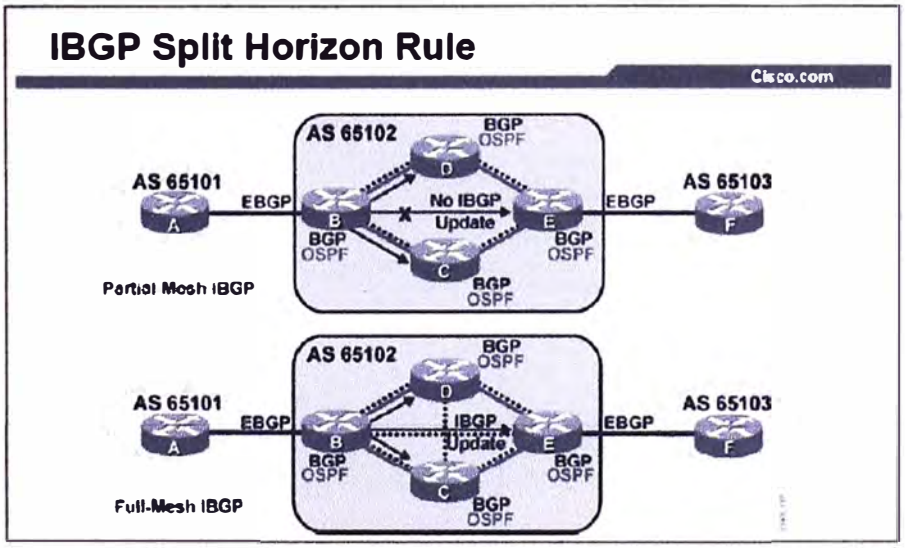


Figura 2.6 BGP Split Horizon (Fuente: www.cisco.com)

El resultado de tener una conexión del tipo *full mesh* es que un *Update* será enviado sólo una vez por el *neighbor* IBGP, reduciendo tráfico innecesario.

Las sesiones TCP no pueden ser enviadas por Multicast o Broadcast debido a que TCP debe garantizar la entrega de paquetes a cada receptor. Debido a ésto BGP no puede usar Multicast o Broadcast y por tanto debe utilizar sesiones TCP *full mesh.*

Como consecuencia de esto, todos los routers corriendo IBGP dentro de un Sistema Autónomo, mantienen una similar base de datos de enrutamiento, y por tanto, aplican una similar fórmula de selección de caminos hacia el exterior (acceso a Sistemas Autónomos remotos).

2.2.6. Configuración básica de BGP

La sintaxis de los comandos básicos de configuración BGP es similar a la sintaxis para la configuración de los protocolos de enrutamiento internos (RIP, OSPF, EIGRP, etc).

El comando *router BGP* identifica el proceso de enrutamiento BGP.

También, identifica el Sistema Autónomo local al cual pertenece este router.

```
Router(config)#
router bgp autonomous-system
```

El comando neighbor *ip-address* remote-as *autonomous-system* permite activar una sesión BGP e identificar el *neighbor* (externo ó interno) con el cual será establecida.

```
Router(config-router)#
neighbor {ip-address | peer-group-name}
remote-as autonomous-system
```

La dirección "*ip-address*" utilizada en este comando es la IP destino para todos los paquetes BGP dirigidos a este *neighbor*; por tanto esta IP debe ser alcanzable a fin de establecer la sesión BGP.

El "*peer-group-name*" identifica el nombre del peer group BGP.

El Sistema Autónomo indicado en "*autonomous-system*" es utilizado para identificar si este *neighbor* es IBGP (Sistema Autónomo similar) ó EBGP (Sistema Autónomo diferente).

a) BGP Neighbor Update Source Address

La opción *update-source* en el comando *neighbor* permite al proceso BGP, utilizar la dirección IP de una interfaz específica, como IP origen de todas las actualizaciones enviadas a un neighbor.

Si no se utiliza la opción *update-source* en el comando *neighbor,* una publicación a un *neighbor* utilizará la dirección IP de la interface de salida como dirección IP origen del paquete, por defecto.

Usualmente una interfaz loopback es utilizada debido a que ella siempre permanecerá activa mientras el router se mantenga operativo.

```
Router(config-router)#
neighbor {ip-address | peer-group-name} update-source
interface-type interface-number
```

La dirección IP utilizada luego del comando *neighbor*, será la IP destino de todas las actualizaciones BGP; y deberá ser la interfaz loopback del otro router.

Este comando es normalmente utilizado en configuraciones IBGP.

b) Peer Groups

En BGP, un grupo de routers pueden ser configurados con las mismas políticas.

Por ejemplo, éste grupo puede tener la misma política de filtrado de enrutamiento.

Por ello, éste grupo de routers con las mismas políticas pueden ser agrupados en "*peer-group*" para simplificar la configuración y hacer las actualizaciones de enrutamiento más eficientes. Para configuraciones de una gran cantidad de routers *neighbors* éste método es muy recomendado.

BGP "*peer-group*" es un grupo de *neighbors* BGP con las mismas políticas de actualización.

Es decir, los *neighbors* miembros del "*peer-group*" heredan todas las opciones de configuración que han sido previamente configuradas para este "*peer-group*", a diferencia de configurar cada

neighbor independientemente.

Los "*peer-group*" son más eficientes debido a que las actualizaciones de enrutamiento son generadas sólo una vez hacia el "*peer-group*" a diferencia de una vez hacia cada *neighbor*.

El nombre asignado al "*peer-group*" es local al router en el cual es configurado, y no enviado a algún otro router.

Los "*peer-group*" hacen la configuración de los routers más simple de administrar y mejoran la su performance.

Sin el uso de "*peer-group*", un router realiza las actualizaciones de enrutamiento de manera separada para router *neighbor*, aunque éstos neighbors tengan una idéntica política de salida.

Con el "*peer-group*", el router crea una sola actualización de enrutamiento para el "*peer-group*" y entonces la duplica para cada miembro.

Con el siguiente comando se crea un "*peer-group*" y se define el nombre que asociará a todos los routers *neighbors* en este grupo:

```
Router(config-router)#
neighbor [peer-group-name] peer-group
```

Con éste segundo comando, se enlaza la dirección IP del router *neighbor* al nombre específico del *"peer-group"* definido con el comando anterior.

```
Router(config-router)#
neighbor [ip-address] peer-group [peer-group-name]
```

Un router *neighbor* puede ser parte sólo de un "*peer-group*".

Todos los miembros de un "*peer-group*" heredan los parámetros de configuración del grupo al cual pertecenen.

Ejemplo: Peer Group

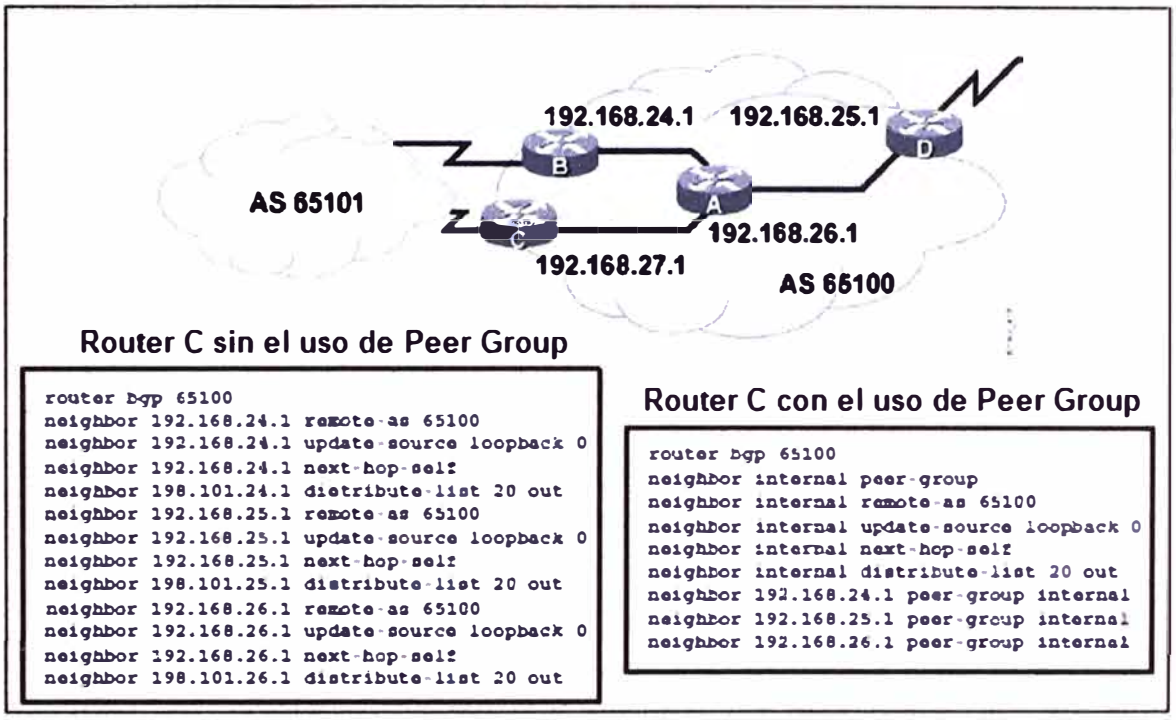


Figura 2.7 Configuración de Peer Group (Fuente: www.cisco.com)

En la figura el Sistema Autónomo 65100 tiene cuatro routers (A, B, C, D) corriendo IBGP. Todos éstos IBGP *neighbors* están utilizando su interfaz loopback 0 como dirección IP de origen; y la interfaz loopback 0 del resto de *neighbors* para el envío de paquetes BGP. Cada router utiliza su propia dirección IP como salto siguiente (comando *next-hop-self*) para toda red que publica a través de BGP.

También, se observa que el router C tiene una lista de distribución (comando *distribute-list*) asociada a cada IBGP *neighbor*, la cual indica no publicar a sus IBGP *neighbors* las redes privadas (10.0.0.0 /8, 172.16.0.0 /21 y 192.168.0.0 /16) que pudiera recibir del Sistema Autónomo 65101.

Para conseguir esto, se configura un access-list que filtre los segmentos de red deseados, tal como el mostrado:

```
access-list 20 deny 10.0.0.0 0.255.255.255
access-list 20 deny 172.16.0.0 0.31.255.255
access-list 20 deny 192.168.0.0 0.0.255.255
access-list 20 permit any
```

La figura 2.7 muestra la configuración del router C cuando el router no está utilizando un "*peer-group*". Todos los IBGP *neighbors* tienen el *distribute-list* 20 de salida asociado individualmente a cada uno de ellos. Si el router C recibe un cambio desde el Sistema Autónomo 65101, debe generar una actualización de enrutamiento individual para cada IBGP *neighbor* y aplicar el *distribute-list* 20 a cada actualización. Si el router C tiene un número largo de IBGP *neighbors,* la cantidad de procesamiento necesitada para informar a los IBGP *neighbors* acerca de los cambios en el Sistema Autónomo 65101 podría ser elevada.

La figura también muestra la salida del router C cuando está utilizando un "*peer-group*" llamado *internal*. Los comandos "*update-source*", "*next-hop-self*" y "*distribute-list 20 out*" son ahora asociados al peer-group *internal*. Entonces, si el router C recibe un cambio del Sistema Autónomo 65101, el router C elabora una única actualización de enrutamiento y la procesa a través del *distribute-list 20.* Esta actualización de enrutamiento es replicada para cada vecino que forma parte del "*peer-group*". Esta acción ahorra tiempo de procesamiento requerido para generar las actualizaciones para cada IBGP *neighbor*.

Por lo tanto, el uso de *peer-groups,* puede mejorar la eficiencia cuando se procesan actualizaciones de enrutamiento para neighbors BGP que tienen una política común de salida.

c) BGP comando Network

En BGP el comando *network* es utilizado para permitir una red a ser anunciada si ésta se encuentra en la tabla de enrutamiento.

```
Router(config-router)#
 network network-number [mask network-mask]
```

network-number: identifica la red IP que será anunciada por BGP.

network-mask: identifica la máscara de la red a ser anunciada por BGP.

Este comando tiene un concepto diferente al usado por los IGP, en los cuales es utilizado para iniciar el proceso de enrutamiento en una interfaz específica; a diferencia de BGP en el cual es utilizado para indicar que redes serán publicadas por el router.

La lista de comandos "*network*" deben incluir todas las redes en el Sistema Autónomo (aprendidas de manera estática, IGP, directamente conectadas) que se desea anunciar, no sólo las que están localmente conectadas al router.

Este comando *network network-number* permite a BGP anunciar una red IGP sólo si ésta

se encuentra en la tabla de enrutamiento. El comando *neighbor* indica a BGP a quien anunciar mientras que el comando *network* indica a BGP que anunciar.

Sin el uso del comando mask *network-mask,* el comando *network* anuncia sólo la red classful (clase A, B ó C).

d) BGP Synchronization

La regla de sincronización BGP indica que un router BGP no utilizará ni anunciará a un *neighbor* EBGP una red que ha aprendido de un *neighbor* IBGP a menos que esta ruta sea local al router ó aprendida vía un IGP (RIP, EIGRP, OSPF, etc).

Un router aprendiendo una ruta vía IBGP, deberá esperar hasta que el IGP que tiene habilitado propague esta ruta dentro del Sistema Autónomo y entonces podrá anunciarla a neighbors externos.

Esta regla asegura que todos los routers dentro del Sistema Autónomo están sincronizados y son capaces de rutear el tráfico que un Sistema Autónomo anuncia a otros Sistemas Autónomos.

Este aprovisionamiento asegura la consistencia de la información de enrutamiento dentro del Sistema Autónomo. La sincronización BGP está habilitada por defecto.

Utilize el comando *no synchronization* para deshabilitar la sincronización.

```
Router(config-router)#
no synchronization
```

Si se deshabilita la sincronización; BGP podrá utilizar y anunciar una red que ha aprendido vía un *neighbor* IGBP y que no ha sido aprendida vía un IGP o de manera local.

La sincronización no es es necesaria en ciertos casos. Si todos los routers dentro de un Sistema Autónomo se encuentran corriendo IBGP (full-mesh IBGP) la sincronización puede deshabilitarse.

En Sistemas Autónomos modernos, debido al gran tamaño de las tablas de enrutamiento de Internet, redistribuir redes de BGP hacia un IGP no es escalable; por tanto éstos Sistemas Autónomos corren full-mesh IBGP y tienen deshabilitada la sincronización.

Ejemplo: Sincronización BGP

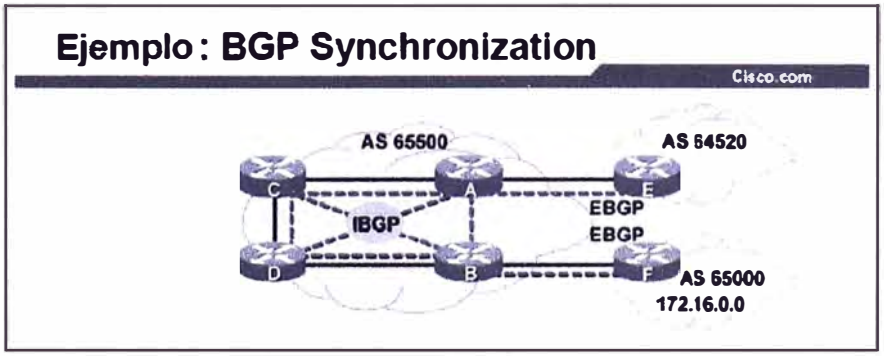


Figura 2.8 Syncronización BGP (Fuente: www.cisco.com)

En la figura, los routers A, B, C y D se encuentran corriendo IBGP e IGP con cada uno de ellos.

Los routers A y B no están redistribuyendo rutas BGP en IGP.

Los routers A, B, C y D tienen rutas IGP que pertenecen al Sistema Autónomo 65500, pero no tienen rutas a redes externas como por ejemplo: 172.16.0.0.

El router B publica la ruta 172.16.0.0 a los otros routers en el Sistema Autónomo 65500 utilizando IBGP. Por defecto (con la sincronización activa) los routers A, C y D no utilizan la ruta a la red 172.16.0.0; tampoco el router A publica esta ruta al router E en el Sistema Autónomo 64520. El router B utiliza esta ruta a 172.16.0.0 y la instala en su tabla de enrutamiento. Si el router E recibe tráfico destinado a la red 172.16.0.0, él no tendrá una ruta a esta red y no podrá enviar el tráfico.

Si la sincronización es deshabilitada en el Sistema Autónomo 65500; los routers A, C y D podrán utilizar la ruta a la red 172.16.0.0 e instalarla en sus tablas de enrutamiento, incluso si no hay una correspondencia entre las rutas IGP y las rutas BGP.

El router A publicará la ruta al router E. El router E entonces, tendrá una ruta a 172.16.0.0 y podrá enviar tráfico destinado a esta red. El router E enviará los paquetes al router A y el router A los enviará al router C. El router C aprenderá una ruta a 172.16.0.0 vía IBGP; por lo tanto, el router C enviará los paquetes al router D. El router D enviará éstos paquetes al router B. Finalmente, el router B enviará los paquetes al router F para alcanzar la red 172.16.0.0.

2.2.7. BGP Neighbor States

A continuación se muestran los estados por los que pasa el establecimiento de una sesión BGP:

1.- Idle: El router está buscando en la tabla de enrutamiento para ver si existe una ruta a fin de alcanzar al *neighbor*.

2.- Connect: El router encontró la ruta y ha completado el saludo three-way.

3.- Open sent: El router envía un mensaje "*Open*" el cual contiene los parámetros de la sesión BGP.

4.- Open confirm: El router recibe un *agreement* (confirmación) de los parámetros para establecer la sesión.

5.- Established: la sesión BGP está establecida, el proceso de enrutamiento entre los *neighbors* empieza.

Luego de ingresar el comando *neighbor,* BGP toma la dirección IP que está configurada en router y busca en la tabla de enrutamiento una ruta para ésta dirección. En este punto, BGP se encuentra en el estado Idle. Si BGP no encuentra una ruta a la dirección,

permanece en el estado Idle. Si encuentra una ruta, pasa al estado Connect luego que el proceso de sincronización de la conexión TCP ha terminado (paquete SYN ACK recibido).

Luego de ello, BGP genera un paquete *BGP Open* y lo envía fuera. Una vez transmitido este paquete, la sesión BGP cambia al estado Open sent. Si no se recibe respuesta durante los 5 siguientes segundos, el estado de la sesión cambia a Active.

Si se recibe respuesta dentro del tiempo, la sesión BGP pasa al estado Open confirm e inicia la evaluación de la tabla de enrutamiento en busca de *pathways* (información de enrutamiento) para enviar al nuevo *neighbor*. Cuando estos *pathways* han sido encontrados, la sesión BGP pasa al estado Established donde finalmente se inicia el proceso de actualización enrutamiento entre los *neighbors*.

2.2.8. BGP Path Selection Process

Después que BGP recibe las actualizaciones de enrutamiento desde diferentes Sistemas Autónomos, el protocolo tendrá que decidir que caminos escoger, a favor de alcanzar un destino específico.

BGP escogerá sólo un camino (el mejor) para alcanzar un destino.

Los routers BGP envían mensajes de actualización acerca de redes destino a otros routers BGP.

Este mensaje de actualización BGP contiene una o más rutas y un conjunto de atributos adjuntos a estas rutas.

El proceso de decisión BGP está basado en la comparación de estos diferentes atributos, tales como, "*next-hop*", "*weight*", "*local preference*", "*origin code*", "*metric*" entre otros.

Luego de escogido el mejor camino, BGP lo propagará a sus *neighbors*.

A continuación, se indica una descripción de cada uno de estos atributos BGP.

a) Atributo AS Path

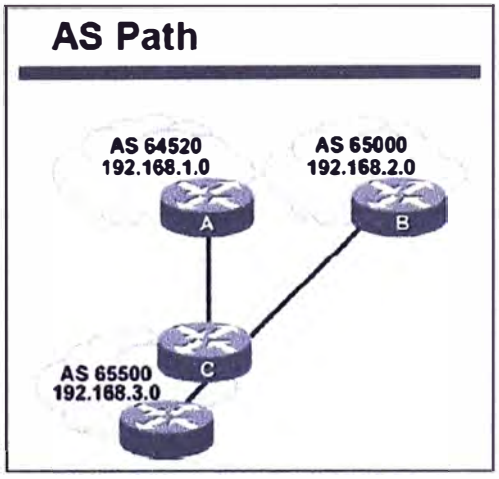


Figura 2.9 Atributo AS Path (Fuente: www.cisco.com)

Cada vez que una actualización de enrutamiento atraviesa un Sistema Autónomo. el número de Sistema Autónomo es añadido a ésta actualización cuando es publicada al siguiente *neighbor* EBGP.

El atributo "*AS path*" es la lista de Sistemas Autónomos que una ruta tiene que atravesar para alcanzar una red destino.

b) Atributo Origin

El atributo "*origin*" define el origen de la información del camino ("*AS path*"). Este atributo puede asumir uno de los siguientes tres valores:

IGP: Cuando la ruta es generada al interior del Sistema Autónomo. Esto normalmente sucede cuando utilizamos el comando "*network*" para publicar la ruta vía BGP ó cuando un protocolo IGP (RIP, OSPF, EIGRP, etc) es redistribuido en BGP. El origen IGP es indicado por con una "i" en la tabla de enrutamiento BGP.

EGP: Cuando la ruta ha sido aprendida vía EGP (Protocolo de Gateway Exterior). Esto es indicado con una "e" en la tabla de enrutamiento BGP.

Incomplete: Cuando el origen de la ruta es desconocido o ésta ha sido aprendida por otros medios.

Este valor usualmente ocurre cuando una ruta estática es redistribuida en BGP. El origen incompleto es indicado con un "?" en la tabla de enrutamiento BGP.

c) Atributo Next-Hop

El atributo *Next-Hop* indica la dirección IP del salto siguiente (next-hop) que es utilizada para alcanzar una red destino. BGP enruta Sistema Autónomo por Sistema Autónomo no router a router.

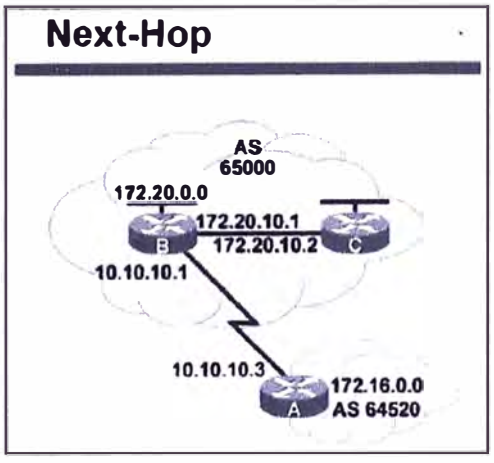


Figura 2.10 Atributo Next-Hop (Fuente: www.cisco.com)

El dirección Next-hop para una red destino ubicada en un Sistema Autónomo remoto será la dirección IP del punto de entrada al siguiente Sistema Autónomo a lo largo del camino a esta red destino.

Para EBGP, el *Next-Hop* es la dirección IP del *neighbor* EBGP, el cual envía la actualización de enrutamiento.

Para IBGP, el Next-Hop advertido por EBGP debe ser publicado vía IBGP.

d) Atributo Local Preference

Local preference es un atributo que provee un indicativo a los routers dentro del Sistema Autónomo acerca de que camino es preferido para dejar el Sistema Autónomo. Un camino con un valor alto de *local preference* es preferido respecto de otro con un menor valor.

El atributo *local preference* es configurado en un router e intercambiado sólo entre routers ubicados dentro del mismo Sistema Autónomo. El valor por defecto para el *local preference* en un router Cisco es 100.

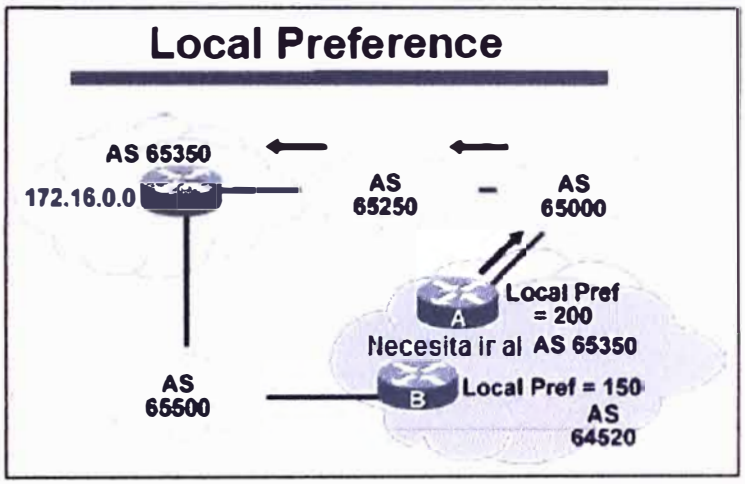


Figura 2.11 Atributo Local Preference (Fuente: www.cisco.com)

En la figura 2.11, el Sistema Autónomo recibe actualizaciones acerca de la red 172.16.0.0 a través de dos caminos. El *local preference* en el router A es fijado en 200 y el *local preference* en el router B es fijado en 150.

Esta información de *local preference* es intercambiada sólo dentro del Sistema Autónomo 64520. Todo el tráfico en el Sistema Autónomo 64520 destinado a la red 172.16.0.0 será enviado al router A como punto de salida de este Sistema Autónomo debido a mayor valor de *local preference* respecto al router B.

e) Atributo Med

El atributo *med* (métrica) es un indicativo a los *neighbors* EBGP acerca del camino preferido a un Sistema Autónomo. Este atributo es una manera dinámica de que un Sistema Autónomo con múltiples puntos de entrada pueda influenciar a otro Sistema Autónomo acerca de que camino debería escoger para acceder a él.

Un valor menor de *med* es preferido.

A diferencia del *local preference*, el *med* es intercambiado entre Sistemas Autónomos. El *med* es trasladado a otro Sistema Autónomo y usado ahí, pero no es enviado al siguiente Sistema Autónomo.

El *med* influencia el tráfico de entrada a un Sistema Autónomo, y el *local preference* influencia el tráfico de salida desde un Sistema Autónomo.

Por defecto, un router comparará el atributo *med* sólo para caminos provenientes de *neighbors* que se encuentran en el mismo Sistema Autónomo.

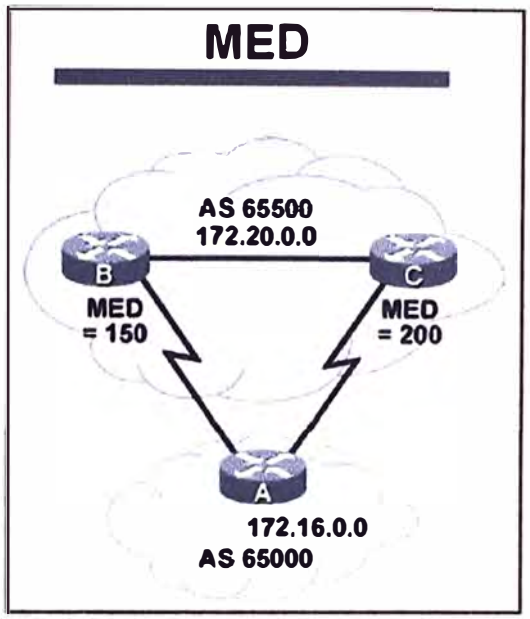


Figura 2.12 Atributo Med (métrica) (Fuente: www.cisco.com)

En la figura, el *med* del router B es fijado en 150 y el *med* del router C es fijado en 200. Cuando el router A reciba una actualización de enrutamiento de los routers B y C, escogerá al router B como el mejor camino debido a que el *med* 150 es menor que 200.

f) Atributo Weight

Weight es un atributo propietario de Cisco, el cual es configurado localmente en un router y no es propagado a ningún otro router.

Este atributo aplica cuando en un Sistema Autónomo se está utilizando un solo router con múltiples puntos de salida hacia el exterior, a diferencia del atributo *local preference* que es usado cuando dos o más routers proveen múltiples puntos de salida al exterior.

Este atributo puede tener un valor desde 0 a 65535. Caminos que el router origina tienen un *weight* de 32768 por defecto; y otros caminos tienen un *weight* de 0 por defecto.

Caminos con un alto valor de *weight* son preferidos cuando múltiples de estos existen al mismo destino.

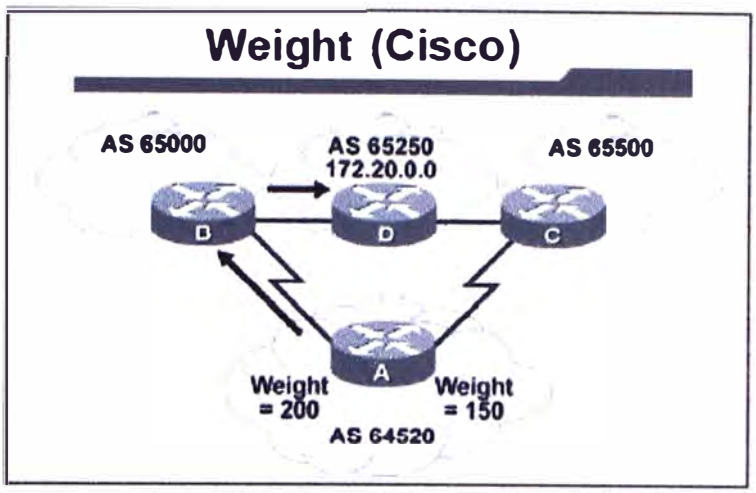


Figura 2.13 Atributo Weight (Fuente: www.cisco.com)

En la figura, los routers B y C aprended acerca de la red 172.20.0.0 del Sistema Autónomo 65250 y propagan esta actualización al router A. Entonces, el router A tendrá dos caminos para alcanzar la red 172.20.0.0, y por tanto, tendrá que decidir cuál de ellos tomar.

En este ejemplo, el router A configura el *weight* de las actualizaciones que provengan del router B en un valor de 200 y el *weight* de éstas actualizaciones que provengan del router C en un valor de 150. Debido a que el *weight* para el router B es mayor que el *weight* para el router C, el router A escogerá al router B como camino para alcanzar la red 172.20.0.0.

-Criterio de selección de caminos BGP

En este punto, se indica cómo el proceso BGP evalúa los diversos atributos para seleccionar el mejor camino (*pathway*) a una red destino.

BGP es un protocolo que no está diseñado para realizar balanceo de carga debido a dos motivos:

Los caminos son escogidos basados en políticas de enrutamiento.

Los caminos no son escogidos basados en parámetros de Bandwith.

Múltiples caminos pueden existir para alcanzar una red destino. Estos caminos son evaluados y se determina que los que no son el mejor, sean eliminados del criterio de selección, pero mantenidos en la base de datos topológica, a fin de ser utilizados en caso el mejor camino sea inaccesible.

Luego que BGP recibe actualizaciones de enrutamiento acerca de diferentes destinos a través de diversos Sistemas Autónomos, realiza un proceso de selección de caminos a fin de escoger el mejor camino para alcanzar una red destino específica.

El proceso de decisión está basado en los atributos BGP. Cuando un router se encuentra con múltiples rutas a un mismo destino, BGP escoge la mejor ruta para enrutar el tráfico

hacia el destino. BGP considera sólo rutas que no tienen loops a nivel Sistema Autónomo y un *next-hop* válido.

El siguiente proceso resume cómo BGP escoge la mejor ruta en un router Cisco:

Paso1: Si el camino es interno y la sincronización esta activa pero la ruta no está sincronizada (ruta aprendida por BGP y por un IGP o localmente) el router no considera esta ruta.

Paso2: Si la dirección de *next-hop* de una ruta no es alcanzable, el router no considera esta ruta.

Paso3: Se prefieren una ruta con el mayor valor de *weight.*

Paso4: Si múltiples rutas tienen el mismo valor de *weight*, se prefiere la ruta con el mayor valor de *local preference* (Recordar que el local preference es utilizado sólo dentro del Sistema Autónomo).

Paso5: Si múltiples rutas tienen el mismo valor de *local preference,* se prefiere la ruta originada en el router local. La ruta originada localmente tiene un next-hop de 0.0.0.0 en la tabla BGP.

Paso6: Si ninguna de las rutas fueron originadas localmente, se prefiere la ruta con el más corto *AS path.*

Paso7: Si la longitud de *AS path* es igual, se prefiere el menor valor de *origin code* (IGP < EGP < incomplete).

Paso8: Si todos los valores de *origin code* son iguales, se prefiere el camino con el menor valor de *med.* (Recordar que el atributo *med* es enviado desde otros Sistemas Autónomos).

La comparación del atributo *med* es realizada sólo si el Sistema Autónomo vecino es el mismo para todas las rutas consideradas, a menos que se habilite el comando *bgp always-compare-med*, con lo cual la comparación del atributo *med* se realizará en Sistemas Autónomos diferentes.

Paso9: Si las rutas tienen el mismo valor de *med,* se prefieren los caminos externos (aprendidos a través de un *neighbor* EBGP) que los caminos internos (aprendidos a través de un *neighbor* IBGP).

Paso10: Si la sincronización está deshabilitada y sólo se tienen caminos internos, se prefiere el camino a través del más cercano *neighbor* IGP. Esto significa que el router preferirá el camino interno más cercano dentro del Sistema Autónomo para alcanzar el destino (el camino más corto al BGP *next hop*).

Paso11: Para caminos EBGP, se seleccionan las rutas más antiguas para minimizar el efecto de rutas que puedan ser inestables (flapping en las rutas).

Paso12: Se prefiere la ruta con el menor valor de *neighbor* BGP router ID.

Sólo el mejor camino es ingresado en la tabla de enrutamiento y propagado a los *neighbors* BGP del router.

2.3. Tecnología MPLS – VPN

2.3.1. MPLS Características

En una red tradicional IP, el proceso de enrutamiento es realizado en cada router. Cada router en la red realiza una decisión independiente cuando envía los paquetes.

MPLS ayuda a reducir el número de procesos de enrutamiento y puede cambiar el criterio de envío de paquetes. Esta capacidad elimina la necesidad de correr un protocolo de enrutamiento particular en todos los routers.

Ejemplo básico de MPLS:

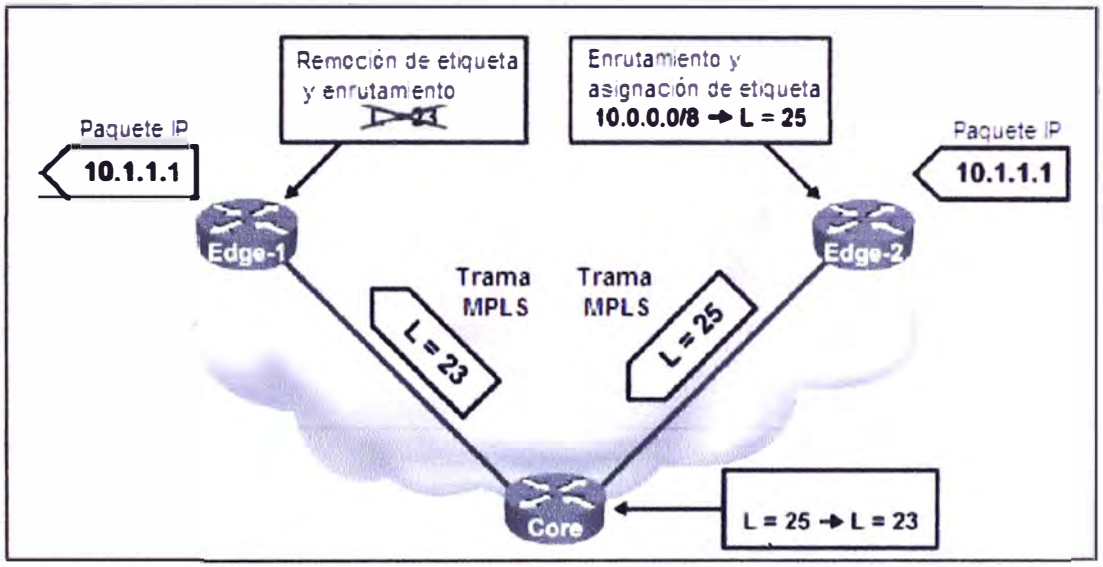


Figura 2.14 Conceptos básicos de MPLS (Fuente: www.cisco.com)

MPLS (Multiprotocol Label Switching) es un mecanismo de conmutación que asigna etiquetas a los paquetes, entonces usa estas etiquetas para el envío de los paquetes. Las etiquetas son asignadas en el borde de la red MPLS y el envío dentro de la red es únicamente basado en las etiquetas.

Estas etiquetas usualmente corresponden a direcciones IP destino, circuitos capa 2, interfaz de salida del router, QoS, entre otros.

MPLS habilita a los routers ubicados en el borde de esta red, aplicar una etiqueta a cada paquete recibido, permitiendo con esto que los routers de core puedan conmutar paquetes basados sólo en éstas etiquetas; lo cual se ve reflejado en una mayor velocidad de conmutación de paquetes a través de la red del proveedor de servicio.

La figura 2.14 muestra una situación en la que un router intermedio, o router core, no tiene que realizar un proceso de enrutamiento que le consuma tiempo. En cambio, el router de core conmuta una etiqueta con otra (etiqueta 25 es reemplazada por la 23) y envía el paquete al router *Edge-1*, basado en la etiqueta 23 recibida del router *Edge-1*.

En este ejemplo, se asume que el router *Edge-2* es informado que a favor de alcanzar la red 10.1.1.1, él debería asignar la etiqueta 25 al paquete y enviar éste paquete al router core. El router core es informado que cuando él reciba un paquete con una etiqueta de 25, él debería conmutar esa etiqueta con la etiqueta 23 y enviar el paquete al router *Edge-1*.

En redes extensas, el resultado del etiquetado MPLS es tal que sólo los routers ubicados en el borde de la red MPLS realizan el proceso de enrutamiento. Todos los routers core envían los paquetes basados en las etiquetas.

a) Mecanismos de conmutación de paquetes

La plataforma Cisco IOS soporta 3 mecanismos de conmutación de paquetes:

-Process switching

Es el primer y más antiguo mecanismo disponible en routers Cisco.

El router realiza una búsqueda en la tabla de enrutamiento y construye un encabezado Capa 2 por cada paquete. Este método es lento y actualmente no utilizado.

-Fast switching

El router utiliza una caché para almacenar los destinos recientemente utilizados. Esta caché utiliza un mecanismo de búsqueda rápida y almacena el encabezado Capa 2 completo para mejorar la performance de encapsulación. El primer paquete cuyo destino no es encontrado en la caché, es conmutado por process-switching y una entrada es creada en la caché. Los sub-siguientes paquetes serán conmutados usando la caché para mejorar la performance.

-CEF

El último y preferido mecanismo de conmutación de paquetes es CEF, el cual incorpora lo mejor de los mecanismos Process y Fast switching.

CEF soporta un balanceo de carga por paquete (soportado previamente sólo por Process switching), balanceo de carga por origen ó por destino y muchas otras características no soportadas por otros mecanismos de conmutación de paquetes.

Basado en la tabla de enrutamiento, CEF crea su propia tabla de envío, llamada FIB (Forward Information Base) y es la que utiliza para definir a que interfaz enviar un paquete.

Esta tabla FIB, es en esencia, un reemplazo de la tabla de enrutamiento standart.

b) Arquitectura MPLS

La arquitectura de un router MPLS puede ser dividida en dos componentes:

-Control Plane:

Es el encargado de realizar las funciones de intercambio de información de enrutamiento e intercambio de etiquetas MPLS.

Para realizar el intercambio de información de enrutamiento utiliza un amplio número de protocolos de enrutamiento tales como OSPF, IGRP, RIP, BGP entre otros.

Para realizar el intercambio de etiquetas utiliza los protocolos LDP (Label Distribution Protocol), BGP (usado por MPLS VPN) y RSVP (Resourse Reservation Protocol, Usado por MPLS TE).

-Data Plane:

Es el encargado de realizar las funciones de envío de paquetes basado en la dirección IP destino ó en la etiqueta MPLS.

Es independiente del tipo de protocolo de enrutamiento ó protocolo de intercambio de etiquetas.

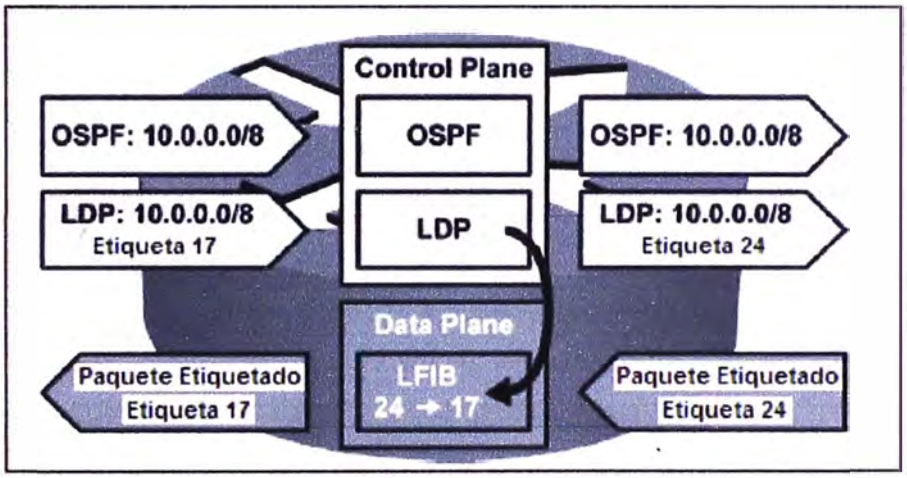


Figura 2.15 Control Plane y Data Plane (Fuente: www.cisco.com)

La tabla LFIB (Label Forwarding Information Base) es usada para almacenar la información de etiquetas utilizadas para el envío de los paquetes. La tabla LFIB es llenada por el protocolo de intercambio de etiquetas utilizado (LDP, BGP ó RSVP).

La figura 2.15 muestra los dos componentes del Control Plane:

El protocolo OSPF, quien recibe y envía una actualización de enrutamiento para la red 10.0.0.0/8.

El protocolo LDP, quien recibe la etiqueta 17 para ser usada con los paquetes con dirección IP destino 10.X.X.X. Una etiqueta local de 24 es generada y enviada a los routers vecinos cuando el paquete es destinado a la red 10.X.X.X. LDP añade una entrada a la tabla LFIB cuando la etiqueta entrante 24 es mapeada con una etiqueta saliente 17.

El Data Plane envía todos los paquetes con etiqueta 24 a través de la interfaz apropiada después de conmutar la etiqueta 24 por la 17.

Para realizar el envío de paquetes, utiliza 2 tablas:

-Tabla LIB: Es la tabla utilizada por LDP (Label Distribution Protocol), donde un prefijo IP es asociado a una etiqueta asignada localmente, la cual es mapeada con otra etiqueta de tipo next-hop que ha sido aprendida de un router vecino.

-Tabla FIB: Contiene la información de envío IP. Esta información puede ser creada manualmente (rutas estáticas, entradas arp) ó dinámicamente (protocolo de enrutamiento).

Esta tabla dinámicamente mantiene una copia de la información de envío contenida en la tabla de enrutamiento IP.

-Tabla LFIB: Es utilizada para almacenar la información de etiquetas necesaria para realizar el envío de paquetes. Esta tabla es llenada por el protocolo de intercambio de etiquetas utilizado (LDP, BGP ó RSVP).

c) Etiquetas MPLS

MPLS está diseñado para ser utilizado en cualquier medio (capa 1) y protocolo de red (capa 2).

MPLS utiliza una etiqueta de 32 bits, la cual es insertada entre la cabecera de capa 2 y capa 3 del paquete.

Esta etiqueta contiene los siguientes cuatro campos:

-Campo Etiqueta (20 bits): Indica el valor de la etiqueta MPLS

-Campo Exp (3 bits): No se encuentra definido por la RFC. Sin embargo es utilizado por Cisco para manejar Calidad de Servicio (CoS, IP Precedence).

-Campo Bottom-of-Stack (1 bit): indica si ésta etiqueta es la última insertada en el paquete. Si este bit tiene el valor de 1, indica que ésta es la última etiqueta.

-Campo TTL (8 bits): Indica la cantidad de saltos restantes al paquete (similar al campo TTL en la cabecera IP).

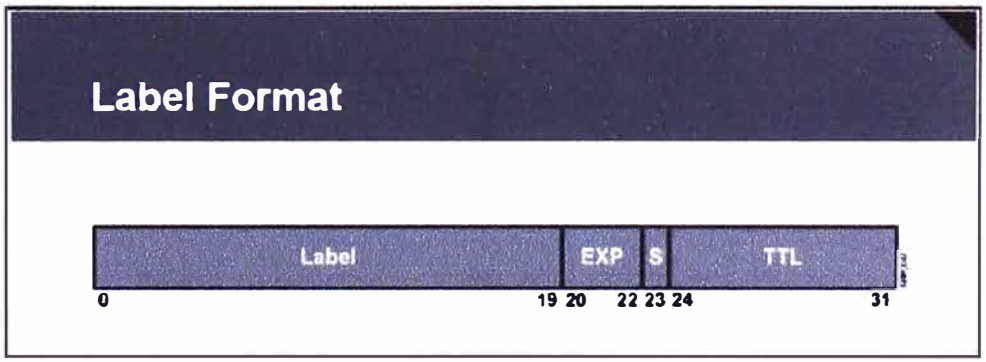


Figura 2.16 Formato de Etiqueta MPLS (Fuente: www.cisco.com)

d) Label Switch Routers

Dentro de la red MPLS se tienen 2 tipos de routers:

-LSR:

Este tipo de router tiene todas sus interfaces habilitadas para MPLS y se encuentra dentro del dominio MPLS.

Realiza la conmutación de paquetes basado en etiquetas.

Este router tiene las siguientes funciones:

*Se encarga de realizar el intercambio de información de enrutamiento.

*Se encarga de realizar el intercambio de etiquetas.

*Realiza el envío de paquetes basado en la etiqueta de 32 bits.

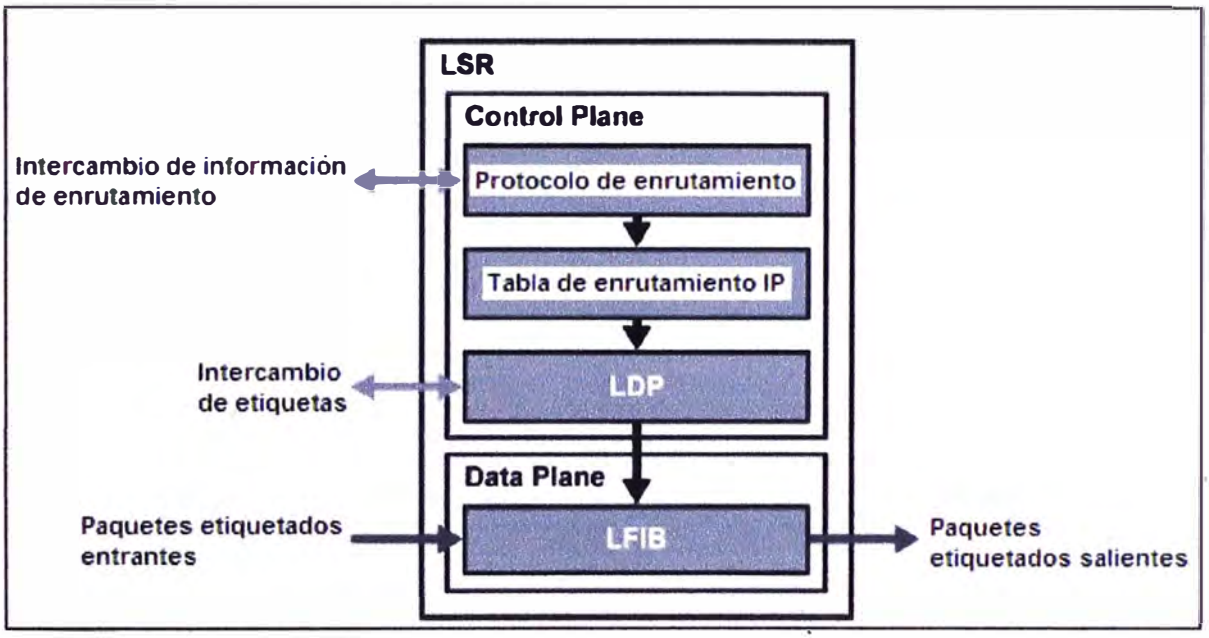


Figura 2.17 Arquitectura de un router LSR (Fuente: www.cisco.com)

-ELSR:

Este tipo de router tiene algunas interfaces no habilitadas para MPLS y se encuentra en el borde del dominio MPLS.

Este router tiene las siguientes funciones:

*Se encarga de realizar el intercambio de información de enrutamiento.

*Se encarga de realizar el intercambio de etiquetas.

*Realiza el envío de paquetes basado en la dirección IP destino ó etiqueta de 32 bits.

*Se encarga de realizar el etiquetado y des-etiquetado de paquetes dependiendo si la interfaz de salida del paquete se encuentra habilitada ó deshabilitada para MPLS, respectivamente.

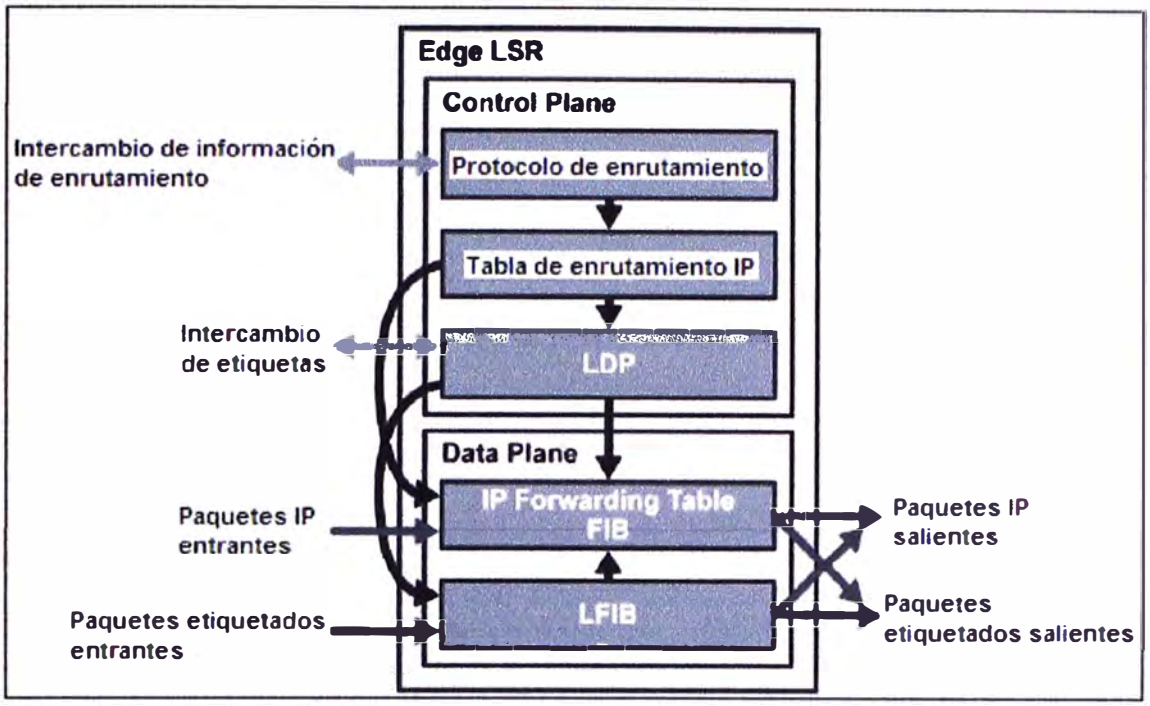


Figura 2.18 Arquitectura de un router ELSR (Fuente: www.cisco.com)

Ejemplo:

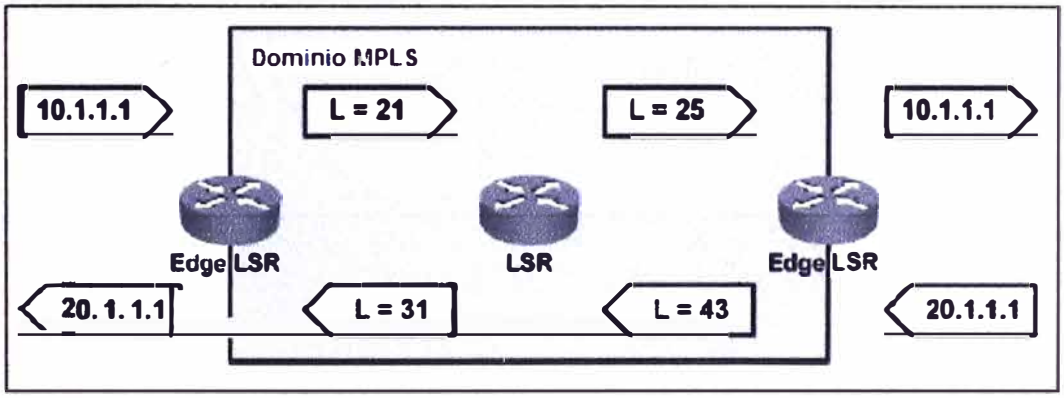


Figura 2.19 routers LSR y ELSR (Fuente: www.cisco.com)

Del ejemplo mostrado en la figura 2.19, se observa que un ELSR recibe un paquete con IP destino 10.1.1.1, le asigna la etiqueta 21 y envía el paquete al LSR en el backbone MPLS. LSR conmuta la etiqueta 21 con la etiqueta 25 y envía el paquete. El ELSR remueve la etiqueta 25 y envía el paquete basado en la dirección IP destino 10.1.1.1.

En el sentido inverso, el comportamiento es similar.

e) Asignación de etiquetas MPLS

La asignación y distribución de etiquetas en una red MPLS puede ser dividida en los siguientes pasos:

Los routers construyen la tabla de enrutamiento IP basados en la información de enrutamiento compartida vía los protocolos de enrutamiento, de esta manera, cada router determina el camino más corto a las redes destino IP.

Cada router genera localmente una etiqueta y la asigna a cada red destino IP encontrado en la tabla de enrutamiento. Estas etiquetas son almacenadas en la tabla LIB (Label Information Base).

Las etiquetas locales son anunciadas a los routers adyacentes, donde estas etiquetas pueden ser utilizadas como etiquetas next-hop y almacenadas por éstos en las tablas FIB (Forwarding Information Base) y LFIB (Label Forwarding Information Base), con el objeto de habilitar la conmutación de etiquetas.

Todos los routers LSR's construyen sus tablas LIB, LFIB y FIB basados en las etiquetas recibidas.

Las siguientes tablas contienen información de etiquetas:

-Tabla LIB: Ubicada en el Control Plane, es la tabla utilizada por LDP (Label Distributlon Protocol), donde un prefijo IP es asociado a una etiqueta asignada localmente, la cual es mapeada con otra etiqueta de tipo next-hop que ha sido aprendida de un router vecino con dirección al destino.

-Tabla LFIB: Ubicada en el Data Plane, es la tabla utilizada para el envío de paquetes etiquetados. Las etiquetas locales previamente anunciadas a los routers vecinos con dirección al origen, son mapeadas con las etiquetas de next-hop, previamente recibidas de los routers vecinos con dirección al destino.

-Tabla FIB: Ubicada en el Data Plane, es la tabla utilizada para el envío de paquetes no etiquetados. Un paquete es etiquetado si una etiqueta de next-hop está disponible para una dirección IP destino específica; de otra forma el paquete a enviar no es etiquetado.

Ejemplo: Asignación de etiquetas

Como punto de inicio se observa que el protocolo de enrutamiento IGP ha convergido.

Se puede ver la tabla FIB del router A, la cual contiene una entrada para la red X, asignando como next-hop la dirección IP del router B.

Sin embargo, en estos momentos una etiqueta next-hop no está disponible, lo cual significa que el paquete será enviado en la forma tradicional (como paquete no etiquetado).

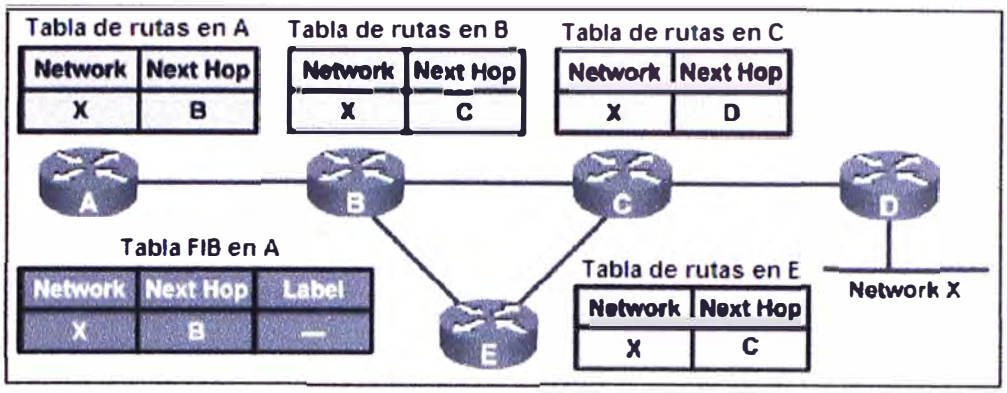


Figura 2.20 Llenado de la tabla de enrutamiento IP (Fuente: www.cisco.com)

-Asignando etiquetas:

Cada router genera una etiqueta de significado local.

Para el ejemplo, el router B genera la etiqueta (25) y la asigna a la red X.

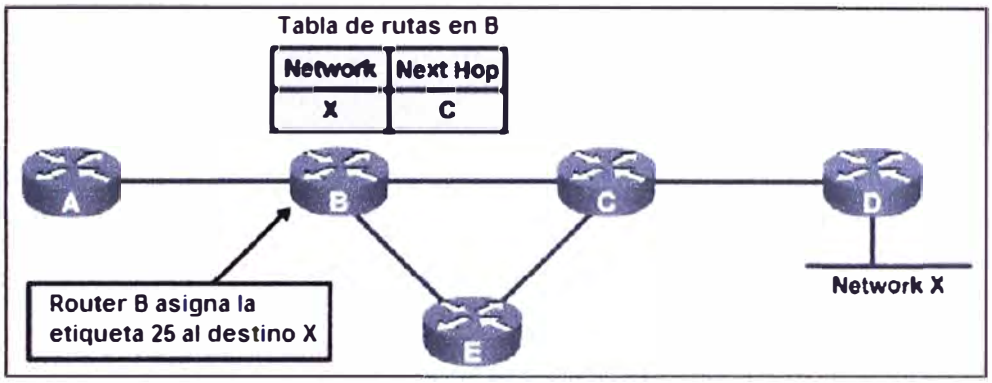


Figura 2.21 Asignación de Etiquetas (Fuente: www.cisco.com)

Cuando una etiqueta es asignada a un prefijo IP, ésta es almacenada en las tablas LIB y LFIB.

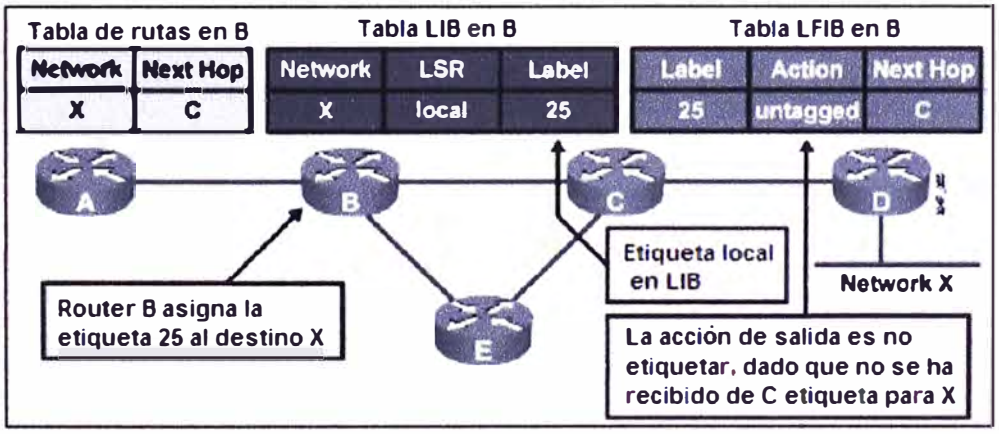


Figura 2.22 Llenado de Tablas LIB y LFIB en router B (Fuente: www.cisco.com)

La tabla LIB contiene el mapeo entre la red X, la etiqueta asignada (25) y el router que ha asignado ésta etiqueta (local).

La tabla LFIB es modificada para contener la etiqueta local mapeada a la acción de envío. En este caso la acción en *untagged* (des-etiquetar) debido a que no se ha recibido de ningún vecino una etiqueta para la red X.

El router que ha asignado la etiqueta de manera local, propaga ésta etiqueta a todos sus vecinos adyacentes donde esta etiqueta puede ser utilizada como etiqueta next-hop.

Para el ejemplo, el router B propaga la etiqueta (25).

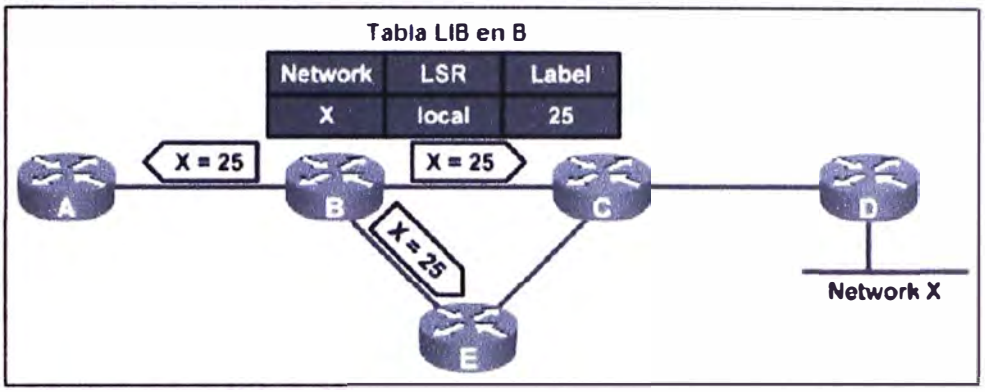


Figura 2.23 Distribución de Etiquetas del router B (Fuente: www.cisco.com)

Luego de recibir un update (actualización) LDP, los routers A, C y E pueden llenar la información de etiqueta en sus tablas LIB, LFIB y FIB.

Estos routers reciben la etiqueta (25) vía el protocolo LDP.

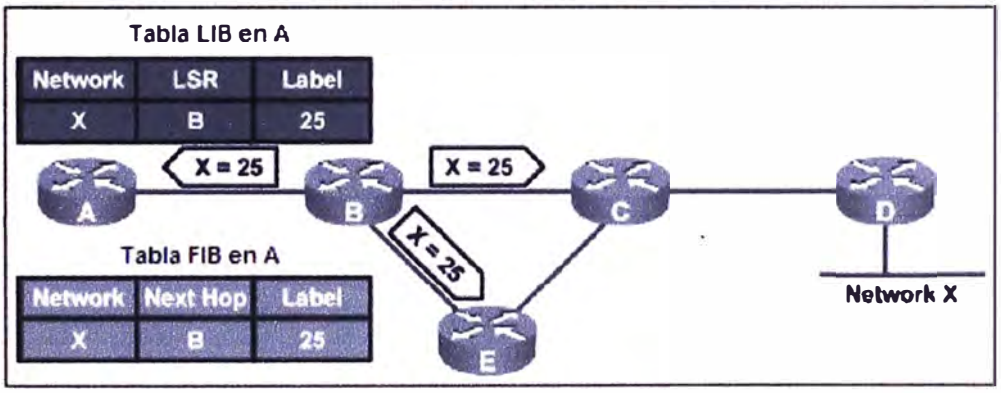


Figura 2.24 Llenado de tablas LIB y FIB en router A (Fuente: www.cisco.com)

De manera similar, el router C asigna la etiqueta (47) a la red X y la publica vía LDP a sus routers adyacentes, incluyendo el router B.

El router D también publica una etiqueta para la red X.

Debido a que el router D se encuentra en el límite del dominio MPLS (router ELSR) asigna la etiqueta "null" lo cual significa que para esta red X el router C realizará la acción POP (quitar la etiqueta) y enviará el paquete sin etiquetar al router D.

Esta acción de des-etiquetar el paquete en el penúltimo salto se denomina PHP (Penultimate Hop Popping).

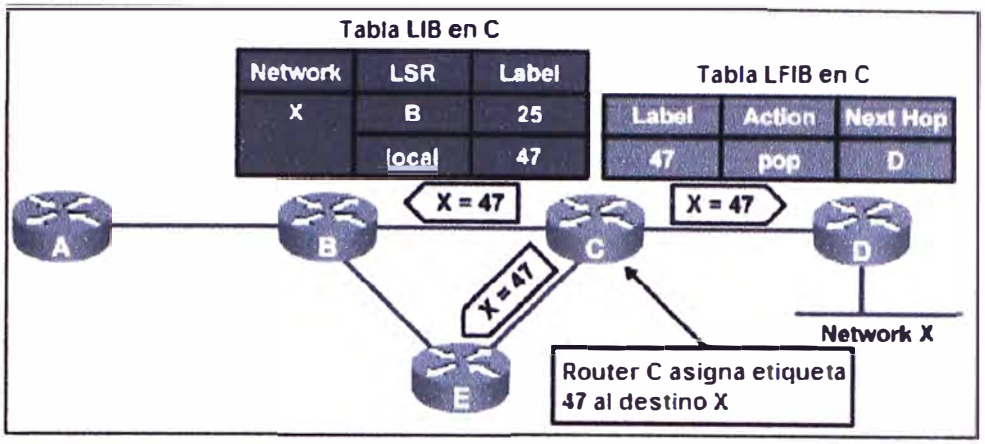


Figura 2.25 Distribución de Etiquetas del router C (Fuente: www.cisco.com)

El router B puede ahora mapear una entrada para la red X en su tabla FIB y con la etiqueta local (25) y la etiqueta de next-hop (47) recibida del router C en la tabla LFIB.

El router E ha asignado la etiqueta (26) para la red X y ha recibido la etiqueta (25) del router B y la etiqueta (47) del router C para esta misma red.

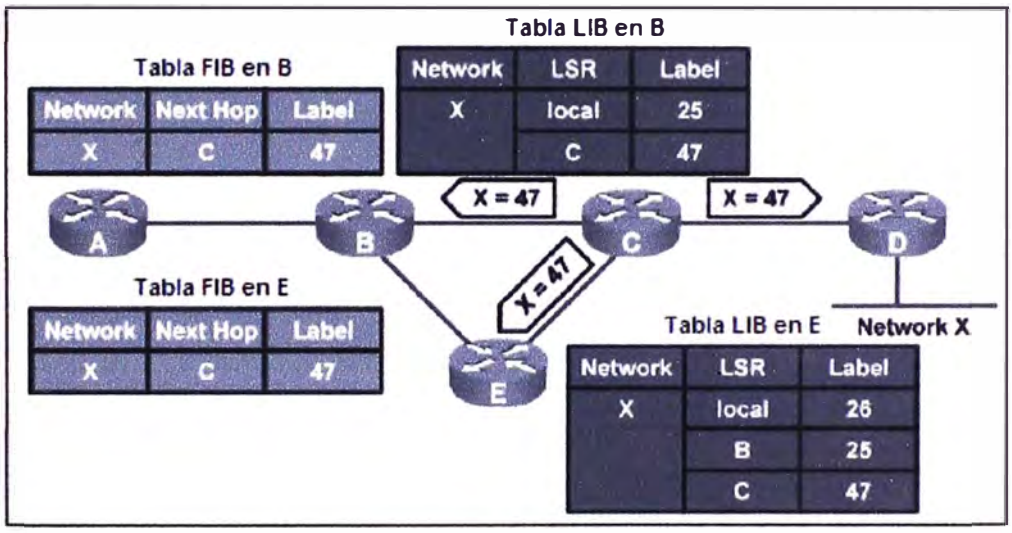


Figura 2.26 Llenado de Tablas LIB y FIB en los routers B y E (Fuente: www.cisco.com)

-Llenado de la tabla LFIB:

El protocolo IGP es utilizado para llenar las tablas de enrutamiento en todos los routers del dominio MPLS. Con ello cada router determina su camino más corto a las redes destino vía IGP.

LDP, quien propaga las etiquetas asociadas a las redes, añade éstas etiquetas en las tablas FIB y LFIB. Sólo las etiquetas que provienen del router next-hop son insertadas en la tabla LFIB.

Para el ejemplo, el router B ha asignado una etiqueta para la red X y creado una entrada en la tabla LFIB. La etiqueta de salida es insertada en la tabla LFIB después que dicha etiqueta es recibida del next-hop LSR.

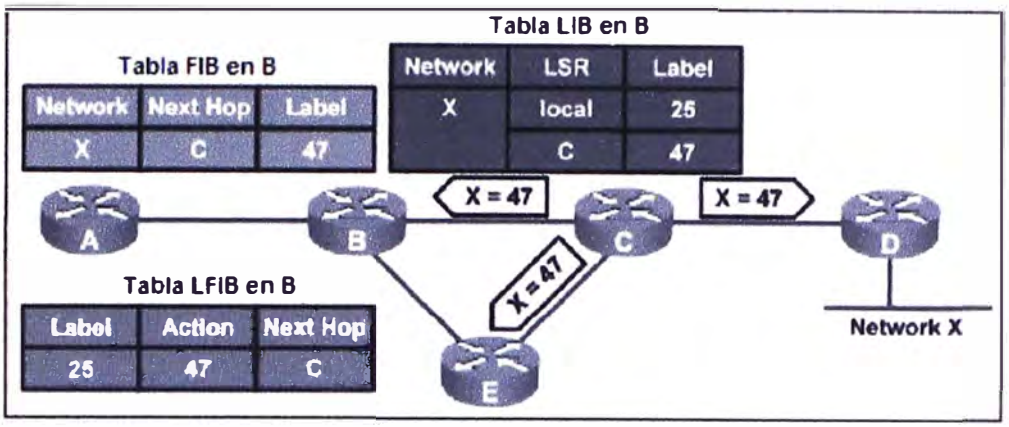


Figura 2.27 Llenado de Tabla LFIB en el router B (Fuente: www.cisco.com)

f) Penultimate Pop Popping (PHP)

Cuando un router determina que es el nodo final en el LSP, éste distribuye una etiqueta de tipo "null" la cual tiene un valor de 3 (valor reservado), en el momento en el que el LSP es establecido.

Esta etiqueta instruye al penúltimo router del LSP de remover la actual etiqueta (acción "POP" en la tabla LFIB) que tiene el paquete y enviarlo sin etiquetar al último router del LSP.

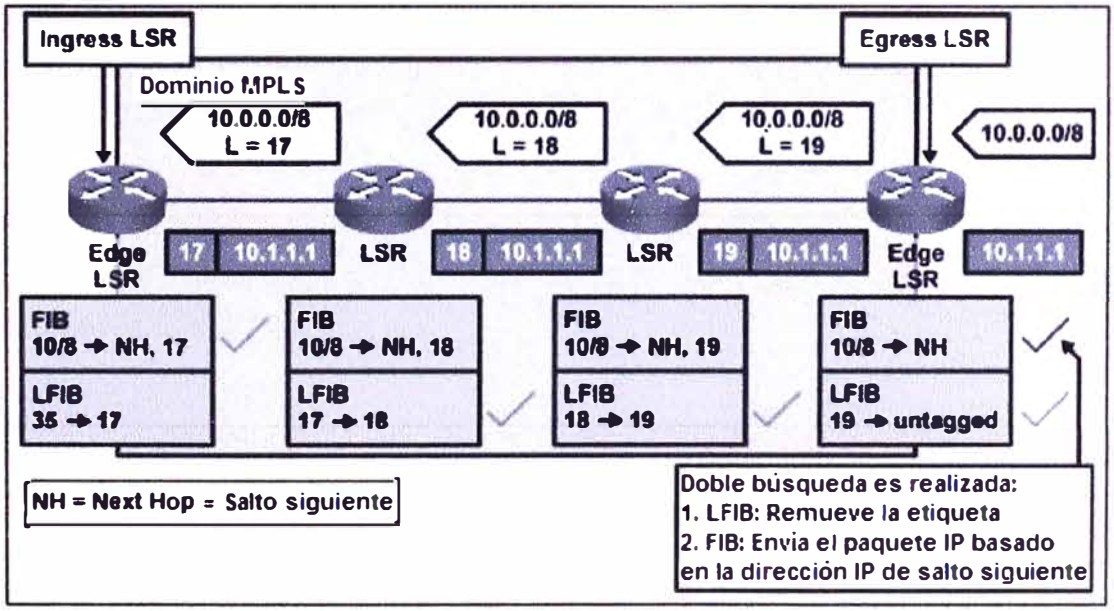


Figura 2.28 Comportamiento del Egress ELSR sin PHP (Fuente: www.cisco.com)

Finalmente, el último router del LSP, recibirá el paquete y éste será procesado usando la tabla FIB.

PHP elimina el requerimiento de realizar un doble proceso del paquete, en el cual el último router del LSP tendría que analizar la tabla LFIB para determinar si la etiqueta debe ser removida y luego, analizar la tabla FIB para enviar el paquete al next-hop.

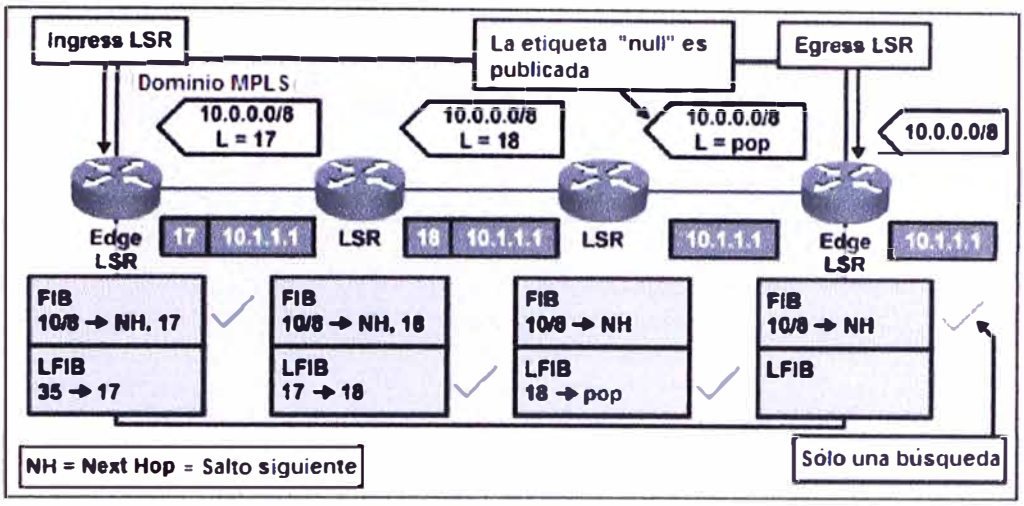


Figura 2.29 Compotamiento del Egress ELSR con PHP (Fuente: www.cisco.com)

La figura 2.28 muestra como los paquetes son propagados antes del uso de PHP.

El check muestra cuales tablas son utilizadas en routers individuales. El router de salida en el ejemplo debería realizar una búsqueda en la tabla LFIB para determinar si la etiqueta debería ser removida y si una búsqueda futura en la tabla FIB es requerida.

La figura 2.29 muestra como los paquetes son propagados utilizando PHP.

Esta figura muestra cómo una etiqueta predefinida, la cual corresponde a la acción POP en la tabla LFIB, es propagada desde el primer salto al último salto.

El término POP significa remover la etiqueta superior en el stack de etiquetas MPLS, en lugar de conmutar ésta etiqueta con la etiqueta next-hop. El último router antes del router de salida, por lo tanto, remueve la etiqueta superior.

PHP optimiza levemente la performance de MPLS, eliminando una búsqueda en la tabla LFIB del router de salida MPLS.

-Propagación del paquete dentro de la red MPLS

Un paquete IP de entrada al dominio MPLS es procesado utilizando la tabla FIB y puede ser etiquetado ó enviado como paquete IP.

Asimismo, un paquete etiquetado de entrada es procesado utilizando la tabla LFIB y es enviado como paquete etiquetado. Si en la tabla LFIB no se encuentra una etiqueta para el router next-hop la etiqueta es removida y el paquete no etiquetado es enviado.

Ejemplo:

La figura muestra como un paquete IP es propagado a través de un dominio MPLS.

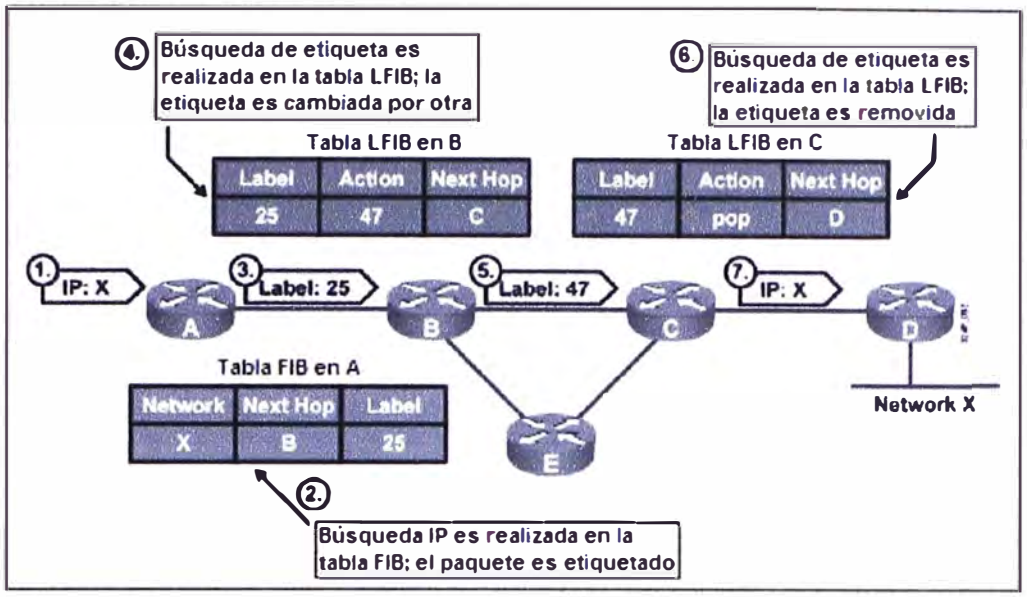


Figura 2.30 Propagación de un paquete a través de la MPLS (Fuente: www.cisco.com)

Los pasos son los siguientes:

-Paso1: Un paquete IP destinado a la red X es recibido por el router A.

-Paso2: El router A etiqueta el paquete destinado para la red X, utilizando la etiqueta de next-hop (25).

-Paso3: El router A envía el paquete hacia la red X, el cual se encuentra etiquetado con la etiqueta (25).

-Paso4: El router B conmuta la etiqueta (25) por la etiqueta (47) utilizando la tabla LFIB.

-Paso5: El router B envía el paquete al router C.

-Paso6: El router C remueve la etiqueta (acción POP).

-Paso 7: El router C envía el paquete no etiquetado al router D (la etiqueta es removida utilizando la tabla LFIB).

g) Implementación de MPLS modo Frame

Para la configuración de MPLS modo Frame en un router Cisco, realizar los siguientes pasos:

-Paso1

Configurar CEF: CEF debe ser habilitado en el router como prerrequisito para la habilitación de MPLS.

Para habilitar CEF, utilizar el comando *ip cef* en el modo de configuración global.

```
Router(config)#
ip cef [distributed]
```

El comando *distributed* configura CEF en modo distribuído, el cual distribuye la información CEF a las *line cards*.

Utilizado por ejemplo, en routers de la serie 6500, 12000.

Para habilitar la operación de CEF en una interfaz individual, utilizar el comando *ip route-cache* cef en el modo de configuración de interfaz.

```
Router(config-if)#
ip route-cache cef
```

OBS: Cuando el modo estándar o distribuído de CEF son habilitados en modo global, todas las interfaces que soportan CEF son habilitadas por defecto.

-Paso2

Habilitar MPLS modo Frame en la interfaz:

Para habilitar el soporte de MPLS en un router, utilizar el comando *mpls ip* en el modo de configuración global, aunque este comando se encuentra habilitado por defecto.

MPLS puede ser deshabilitado utilizando el comando *no mpls ip* en el modo de configuración global. También, puede ser habilitado individualmente en una determinada interfaz utilizando el comando *mpls ip* en el modo de configuración de interfaz.

```
Router(config-if)#
mpls ip
```

Luego de habilitar MPLS en una interfaz, se debe seleccionar el protocolo de distribución de etiquetas utilizando el comando *mpls label protocol* en el modo de configuración de interfaz.

El protocolo de distribución de etiquetas por defecto es LDP. Por tanto, si no es configurado explícitamente un protocolo, LDP será habilitado por defecto.

Los protocolos de distribución de etiquetas que pueden ser habilitados con este comando son LDP y TDP.

```
Router(config-if)#
mpls label protocol [tdp | ldp | both]
```

La opción *both* de este comando, permite habilitar el soporte para LDP y TDP en la interfaz.

-Paso3

Configurar el tamaño de MTU en la conmutación de etiquetas (opcional):

Debido a la etiqueta adicional añadida, es posible cambiar el tamaño máximo de los paquetes etiquetados, con el objeto de prevenir la fragmentación IP.

El MTU en interfaces WAN es automáticamente incrementado, pero no en interfaces LAN.

Debido a que el MTU no es automáticamente incrementado en interfaces LAN, se debe realizar el incremento de manera manual utilizando el comando *mpls mtu bytes* en el modo de configuración de interfaz.

```
Router(config-if)#
mpls mtu bytes
```

Este incremento del tamaño de MTU en los paquetes etiquetados debe realizarse en todos los segmentos a lo largo del túnel LSP.

El tamaño de MTU en un segmento LAN, es 1500 bytes. El tamaño del MPLS MTU depende de la aplicación que se tenga habilitada en MPLS. Cuando se está utilizando MPLS puro en el backbone, el tamaño de MTU deberá incrementarse para una sola etiqueta añadida a un valor de 1504 bytes. Cuando se está implementando MPLS VPN, el tamaño de MTU deberá incrementarse para dos etiquetas añadidas a un valor de 1508 bytes. Con MPLS VPN y TE (Ingeniería de Tráfico), el tamaño de MTU deberá incrementarse para tres etiquetas a un valor de 1512 bytes.

OBS: El valor mínimo de MTU es 64 bytes. El valor máximo depende del tipo de medio de la interfaz.

2.3.2. Tecnología MPLS VPN

a) Overlay y Peer-to-Peer VPN

Los servicios VPN pueden ser ofrecidos basados en 2 modelos mayores:

-Overlay VPN: En el cual el proveedor de servicio provee enlaces vituales punto-a-punto entre las sedes del cliente.

*Overlay VPN de Capa1: Es el modelo en el cual el proveedor de servicio proporciona circuitos capa 1 implementados con tecnologías tales como ISDN, E1, T1, SDH, entre otros. El cliente es responsable de realizar la encapsulación de Capa2 entre los routers de las sedes remotas y del transporte de la data IP a través de la infraestructura.

*Overlay VPN de Capa2: Es el tradicional modelo wan conmutado, implementado con tecnologías tales como X.25, Frame Relay, ATM entre otros. El proveedor de servicio es responsable por el transporte de las tramas capa 2 entre las sedes del cliente, y el cliente es responsable por todas las capas de nivel superior.

*Overlay VPN de Capa3: Es el modelo en el cual La VPN está implementada a través de un túnel IP-sobre-IP. Utiliza los protocolos GRE, IPSEC para el establecimiento del túnel.

-Peer-to-peer VPN: En el cual el proveedor de servicio participa en el proceso de enrutamiento de las redes pertenecientes a las sedes del cliente.

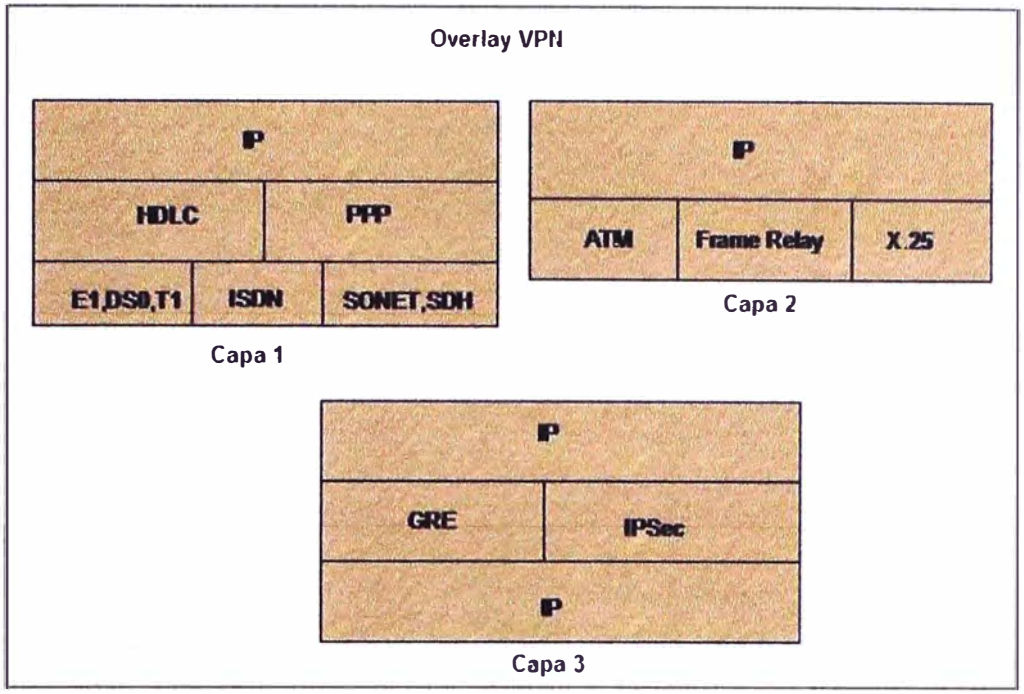


Figura 2.31 Overlay VPN

Ejemplo: Overlay VPN de Capa2:

El cliente necesita conectar tres sedes con la sede A (sede central) y ordena la conectividad entre la sede A (hub) y la sede B (spoke), entre la sede A y la sede C (spoke) y entre la sede A y la sede D (spoke). El proveedor de servicio realiza este requerimiento con la provisión de tres circuitos virtuales permanentes (PVCs) a través de la red Frame Relay.

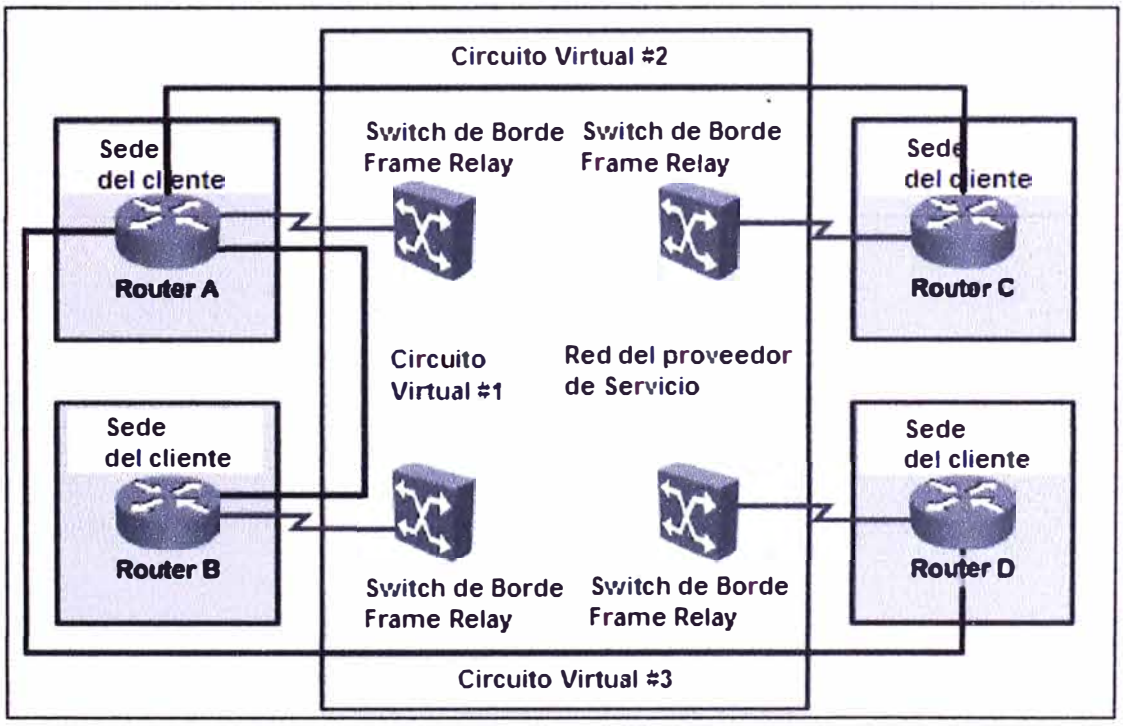


Figura 2.32 Overlay VPN de Capa2, ejemplo: Frame Relay (Fuente: www.cisco.com)

La figura 2.32 muestra un típico modelo de Overlay VPN de Capa2 implementado a través de una red Frame Relay.

La implementación realizada en este ejemplo no provee full-conectividad, el flujo de datos entre las sedes "*spoke*" es a través de la sede "hub".

-Ventajas de implementaciones VPN:

*Overlay VPN:

El proveedor de servicio no participa en el proceso de enrutamiento del cliente.

La red del cliente y la red del proveedor se encuentran claramente delimitadas.

*Peer-to-peer VPN:

Óptimo enrutamiento entre los sites del cliente sin realizar un diseño o esfuerzo adicional.

Fácil aprovisionamiento de VPN's o nuevas sedes para el cliente, debido a que el proveedor de servicio adiciona sedes individuales no los enlaces entre ellas.

-Desventajas de implementaciones VPN:

*Overlay VPN:

Overlay VPN de Capa 2 requiere conectividad "full mesh" (todos contra todos) de los VC's entre las sedes del cliente para proveer un óptimo enrutamiento entre ellas.

Todos los VC's entre las sedes del cliente tienen que ser provistos manualmente.

Overlay VPN de Capa 3 (IPSEC o GRE) incurre en un sobre-encabezado; entre 20 y 80 bytes por paquete.

*Peer-to-peer VPN:

El proveedor de servicio viene a ser responsable por el correcto enrutamiento y rápida convergencia de las redes del cliente.

El proveedor de servicio necesita tener un detallado conocimiento de enrutamiento IP, lo cual no es fácilmente alcanzable para un proveedor de servicio.

2.3.3 Arquitectura MPLS VPN

MPLS VPN ofrece a los proveedores de servicio una arquitectura que combina las mejores características de Overlay VPN (soporte de traslapo de direccionamiento IP de los clientes) con las mejores características de Peer-to-peer VPN.

Estas características son las siguientes:

Los routers PE participan en el enrutamiento del cliente, garantizando un óptimo enrutamiento entre las sedes del cliente.

Los routers PE utilizan una tabla de enrutamiento virtual para cada cliente, garantizando un proceso de enrutamiento independiente para cada cliente.

Los clientes pueden utilizar un direccionamiento IP traslapado.

a) Terminología MPLS VPN

La terminología MPLS VPN divide a la totalidad de la red en dos partes: una parte controlada por el cliente (C-Network) y una parte controlada por el proveedor (P-Network).

Las sedes del cliente están enlazadas con la P-Network vía el router CE (Customer Edge router) los cuales están conectados con los routers PE (Provider Edge routers) quienes actúan como dispositivos de borde de la P-Network.

Los dispositivos core en la P-Network proveen transporte a través del backbone del proveedor.

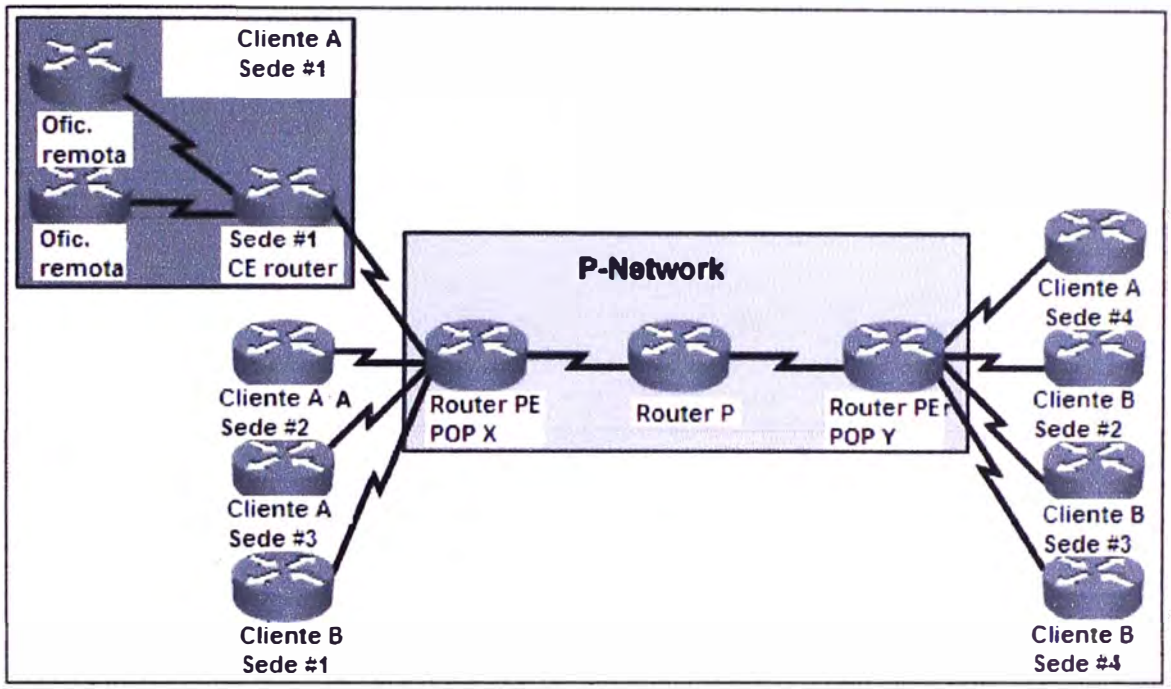


Figura 2.33 Arquitectura de la red MPLS VPN (Fuente: www.cisco.com)

2.3.4. Propagación de la información de enrutamiento a través de la P-Network

Aunque las VRF's proveen aislamiento entre los clientes, la información de éstas tablas de enrutamiento todavía necesita ser cambiada entre los routers PE para habilitar la transferencia de datos entre las sedes conectadas a los diferentes routers PE.

Por tanto, un protocolo de enrutamiento es necesitado para transportar todas las redes del cliente a través de la P-Network, mientras se mantiene la independencia del espacio de direccionamiento de cada cliente.

La mejor solución para la propagación de rutas del cliente, es habilitar un protocolo de enrutamiento entre los routers PE que intercambiará todas las rutas del cliente sin involucrar a los routers P. Esta solución es escalable.

Se muestran algunos de los beneficios de esta solución:

El número de protocolos de enrutamiento corriendo entre los routers PE no se incrementa con un incremento del número de clientes.

Los routers P no transportan redes de clientes.

Dado que es esperado un número muy elevado de redes de clientes, el único protocolo de enrutamiento con la escalabilidad requerida es BGP.

Por tanto, BGP es utilizado en la arquitectura de MPLS VPN para el transporte de las redes del cliente directamente entre los routers PE.

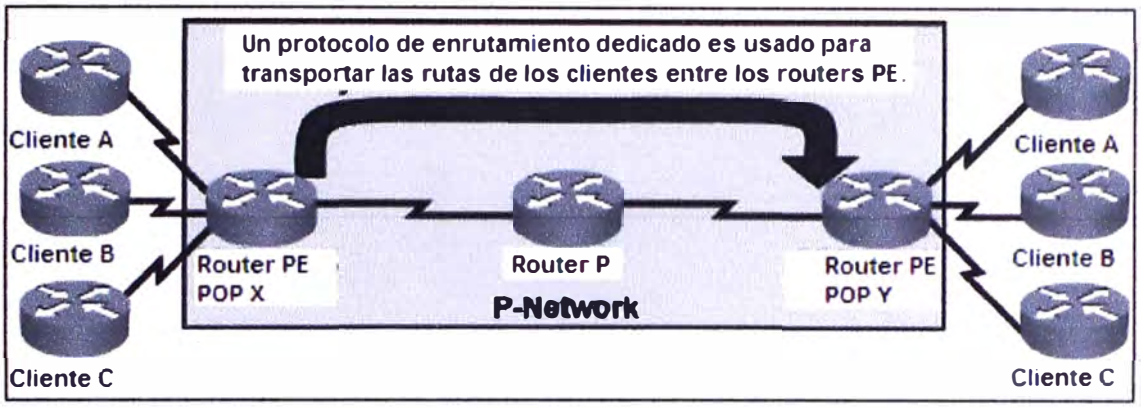


Figura 2.34 Propagación de información de enrutamiento a través de la P-Network (Fuente: www.cisco.com)

a) Route Distinguishers (RD)

Con el desarrollo de un único protocolo de enrutamiento (BGP) para intercambiar todas las redes de los clientes entre los routers PE, un observación importante aparece: como puede BGP propagar segmentos de red idénticos, perteneciendo a diferentes clientes entre los routers PE.

La solución a este inconveniente es realizar la expansión de los segmentos de red del cliente con un nuevo prefijo que los haga únicos.

Un prefijo de 64 bits llamado RD es utilizado en MPLS VPN para convertir las direcciones no únicas IPv4 de 32 bits en direcciones únicas de 96 bits que pueden ser transportadas entre los routers PE.

El prefijo RD es utilizado para convertir las direcciones no únicas del cliente IPv4 de 32 bits en direcciones únicas de 96 bits VPN versión 4 (VPNv4).

Las direcciones VPNv4 son intercambiadas sólo entre los routers PE; ellas nunca son utilizadas entre los routers CE.

La sesión BGP entre los PE routers debe soportar el intercambio de los prefijos de red tradicionales IPv4 y el intercambio de los prefijos VPNv4.

Una sesión BGP entre los routers PE debe soportar múltiples protocolos, a fin de ésto, una sesión MP-BGP es establecida.

La propagación de rutas del cliente a través de una red MPLS VPN es realizado a través del siguiente proceso:

-Paso1: El router CE envía una actualización IPv4 al router PE.

-Paso2: El router PE adiciona el prefijo RD (64 bits) a la actualización de enrutamiento IPv4, resultando en un prefijo globalmente único VPNv4 de 96 bits.

-Paso3: El prefijo VPNv4 es propagado vía una sesión MPBGP a otro PE router.

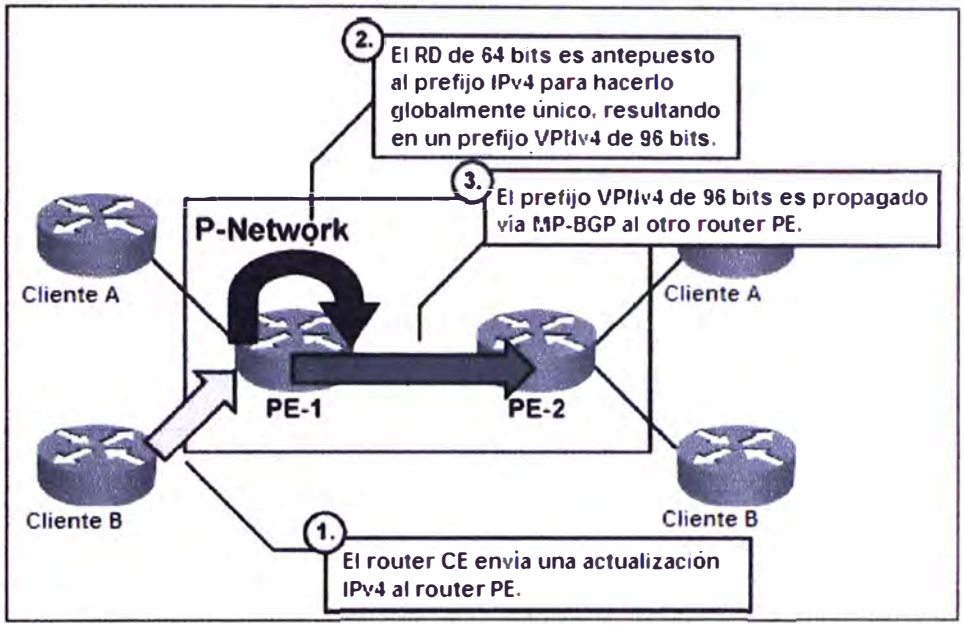


Figura 2.35 Propagación de las redes del cliente a través de la red MPLS VPN (Fuente: www.cisco.com)

-Paso4: Los routers PE que reciben la actualización quitan el RD del prefijo VPNv4, resultando en un prefijo IPv4.

-Paso5: El prefijo IPv4 es reenviado a otros routers CE dentro de la actualización de enrutamiento.

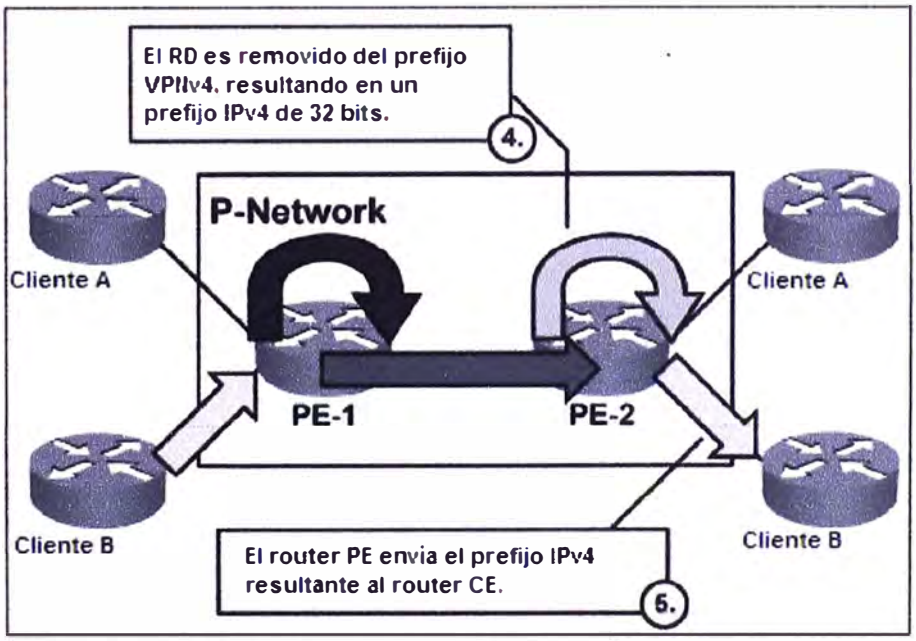


Figura 2.36 Propagación de las redes del cliente a través de la red MPLS VPN (continuación) (Fuente: www.cisco.com)

-Observaciones:

El prefijo RD no tiene un significado especial. Su única función es convertir las direcciones IPv4 con un riesgo potencial de ser traslapadas entre los clientes, en direcciones globalmente únicas.

El prefijo RD es configurado en los routers PE como parte de la implementación de aprovisionamiento de un nuevo cliente.

Este prefijo no es configurado en los routers CE y es invisible para el cliente.

Topologías VPN simples requieren sólo un RD por cliente, dando la posibilidad que el RD pueda servir como un identificador VPN. Este diseño, sin embargo, podría no permitir implementaciones más complejas de topologías VPN, tales como, cuando un cliente pertenece a múltiples VPNs.

b) Route Targets (RT)

Para ilustrar la necesidad de un indicador más completo que el RD, consideremos el siguiente ejemplo:

Se tiene el siguiente servicio de VoIP:

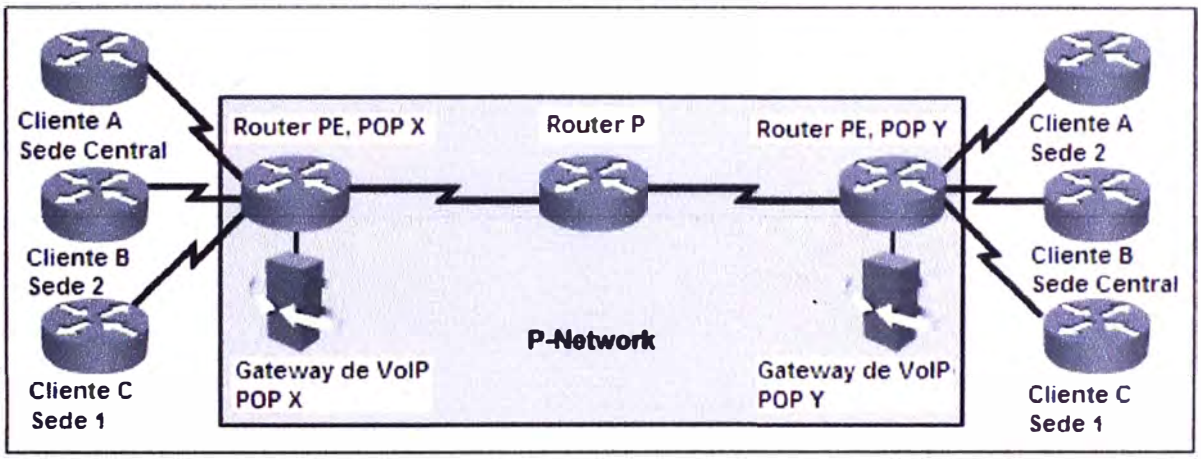


Figura 2.37 Ejemplo: Necesidad de utilizar el RT (Fuente: www.cisco.com)

Los requerimientos de conectividad de este servicio de VoIP son los siguientes:

Todos los sites de un cliente necesitan comunicarse entre sí.

Las sedes centrales (Central Sites) de diferentes clientes suscritos al servicio de VoIP necesitan comunicarse con los VoIP Gateways para originar y recibir llamadas en la red de voz pública; también necesitan comunicarse con otras sedes centrales para intercambiar llamadas entre empresas.

Estos requerimientos son ilustrados en la siguiente figura:

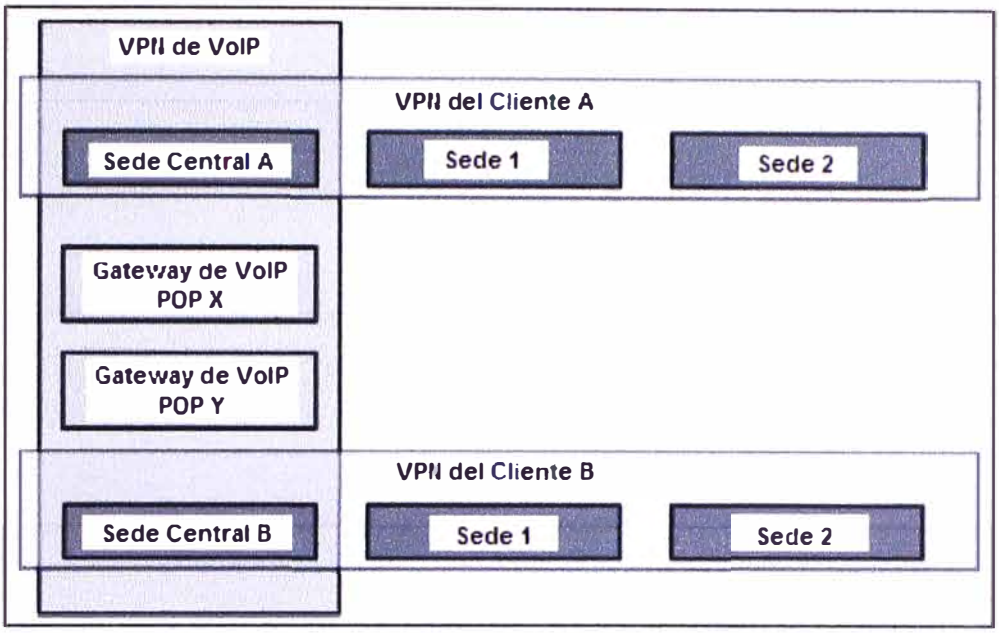


Figura 2.38 Requerimiento de conectividad del ejemplo (Fuente: www.cisco.com)

Para implementar esta conectividad requerida son necesitadas 3 VPNs: 2 VPNs para los clientes (A y B) y una VPN compartida para VoIP, de acuerdo a lo siguiente:

Central Site A participa en la VPN A y en la VPN de VoIP.

Central Site A participa en la VPN B y en la VPN de VoIP.

Customer Sites A-1 y A-2 participan en la VPN A.

Customer Sites B-1 y B-2 participan en la VPN B.

-Route Target (RT):

El RD (prefijo añadido a una red IPv4) no puede indicar si una sede del cliente pertenece a más de una VPN.

El concepto de RT fué introducido en la arquitectura MPLS VPN para soportar los requerimientos de pertenencia a varias VPN.

RTs son atributos, que son adjuntados a una ruta VPNv4 BGP para indicar la pertenencia de ésta a una o varias VPNs.

Las MPLS VPN RTs son adjuntadas a una ruta del cliente en el momento que es convertida una ruta IPv4 a una ruta VPNv4 por el router PE.

Los atributos MPLS VPN RTs se dividen en Export RT e Import RT.

*Export RT:

Los atributos MPLS VPN RTs son adjuntados a una ruta de cliente en el momento que son convertidas de una ruta IPv4 a una ruta VPNv4 por el router PE.

Estos RTs adjuntos a la ruta son llamados export RTs y son configurados separadamente para cada tabla de enrutamiento virtual en el router PE.

Estos export RTs identifican el grupo de VPNs al cual la ruta será publicada.

*Import RT:

Cuando las rutas VPNv4 son propagadas a otros routers PE, éstos routers necesitan seleccionar qué rutas importar a sus tablas de enrutamiento virtuales. Esta selección es basada en el atributo import RT. Cada tabla de enrutamiento virtual en un router PE puede tener un número de import RT configurados que identifican el grupo de VPNs desde el cual la tabla de enrutamiento virtual aceptará las rutas.

2.3.5. Flujo de información de enrutamiento end-to-end

Los diseñadores de la tecnología MPLS VPN hicieron frente a los siguientes requerimientos de enrutamiento:

Los routers CE no deberían estar configurados / habilitados para MPLS VPN; ellos deberían correr un protocolo de enrutamiento standart.

Los routers PE deberían estar configurados / habilitados para MPLS VPN.

Para hacer la solución MPLS VPN escalable, los routers P no deberían transportar rutas VPN.

a) Perspectiva del router CE:

Los routers CE corren un protocolo de enrutamiento estándar e intercambian actualizaciones de enrutamiento con los routers PE quienes aparecen ante ellos como los encargados de realizar la redistribución de rutas entre las sedes del cliente.

Los routers P están escondidos para la vista del cliente; la topología interna del backbone BGP es, por lo tanto, transparente para el cliente.

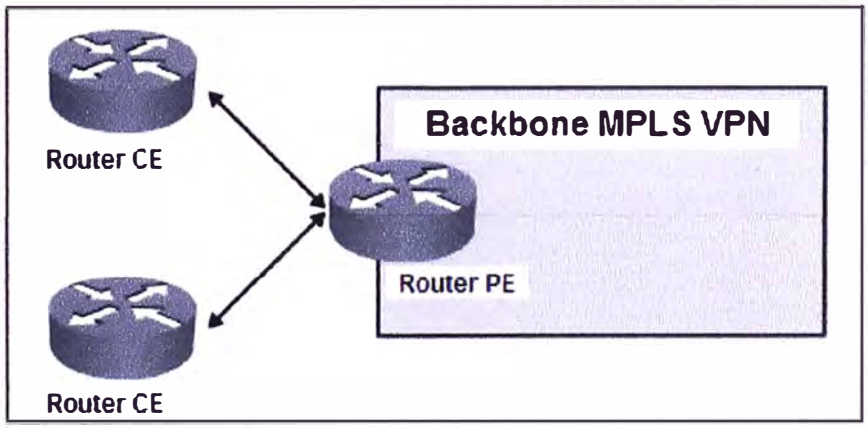


Figura 2.39 Enrutamiento MPLS VPN: Perspectiva del router CE (Fuente: www.cisco.com)

-Protocolo de enrutamiento PE-CE

Después de configurar las VRFs y establecer la conectividad MPBGP entre los routers PE; se tiene que configurar los protocolos de enrutamiento entre el router PE y los routers CE conectados a él.

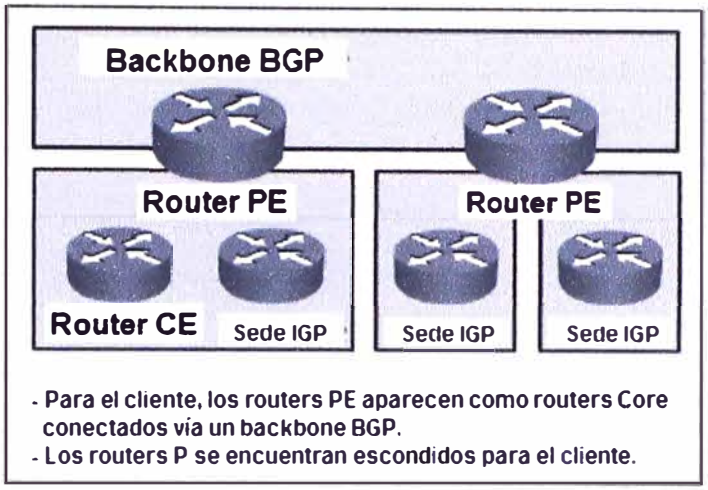


Figura 2.40 Enrutamiento MPLS VPN: Protocolos de enrutamiento en los routers CE y PE (Fuente: www.cisco.com)

Procolos de enrutamiento soportados incluyen BGP, OSPF, ruteo estático, RIP y EIGRP entre otros.

Los protocolos de enrutamiento PE-CE en el router PE necesitan ser configurados para cada VRF de manera individual.

La configuración del protocolo de enrutamiento en el router CE es muy simple, debido a que el cliente no tiene información de las VRFs configuradas en el lado del proveedor.

La configuración del lado cliente es la misma configuración como si el enrutamiento tuviera lugar entre dos routers de la C-Network.

b) Perspectiva del router P:

Desde la perspectiva del router P, el backbone MPLS VPN se observa simple. Los routers P no participan en el enrutamiento MPLS VPN, lo cual significa que no transportan rutas VPN.

Los routers P sólo corren un protocolo de Gateway interior (IGP) con otros routers P y routers PE para intercambiar información de redes de core y loopbacks.

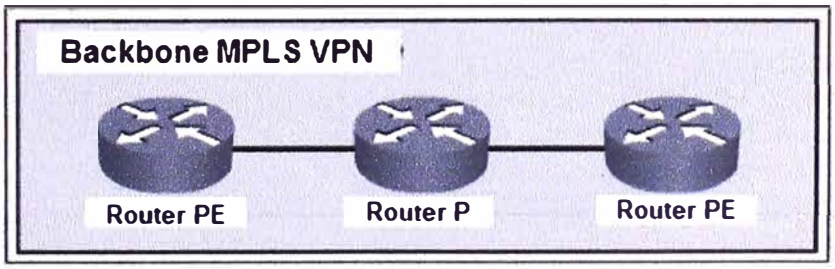


Figura 2.41 Enrutamiento MPLS VPN: Perspectiva del router P (Fuente: www.cisco.com)

c) Perspectiva del router PE:

Los routers PE son los únicos en la arquitectura MPLS VPN que participan en todos los aspectos de enrutamiento de la red MPLS VPN.

Los routers PE son capaces de intercambiar lo siguiente:

*Las rutas IPv4 VPN con los routers CE vía los protocolos de enrutamiento que se encuentran corriendo en las tablas VRF.

*Las rutas VPNv4 vía las sesiones MPBGP con otros routers PE.

*Rutas de core con los routers P y otros routers PE vía IGP.

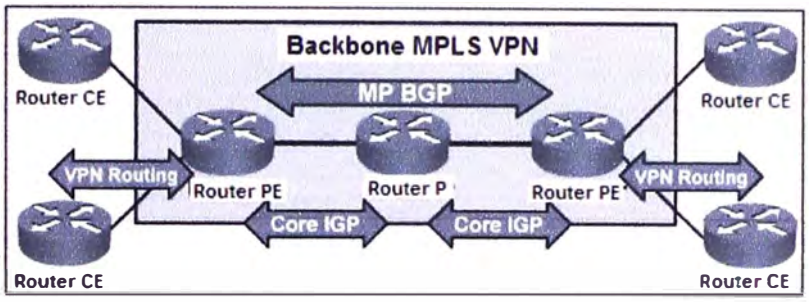


Figura 2.42 Enrutamiento MPLS VPN: Perspectiva del router PE (Fuente: www.cisco.com)

-Flujo de actualización de enrutamiento end-to-end

La siguiente figura muestra un resumen del flujo de información de enrutamiento end-to-end en una red MPLS VPN.

Los siguientes pasos describen las etapas por las que pasa el flujo de información de enrutamiento desde la actualización de enrutamiento como paquete IPv4, ingresando al backbone MPLS VPN y propagándose a través de él como rutas VPNv4.

-Paso1: Los routers PE reciben actualizaciones IPv4 desde los routers CE e instalan éstas en la tabla VRF apropiada.

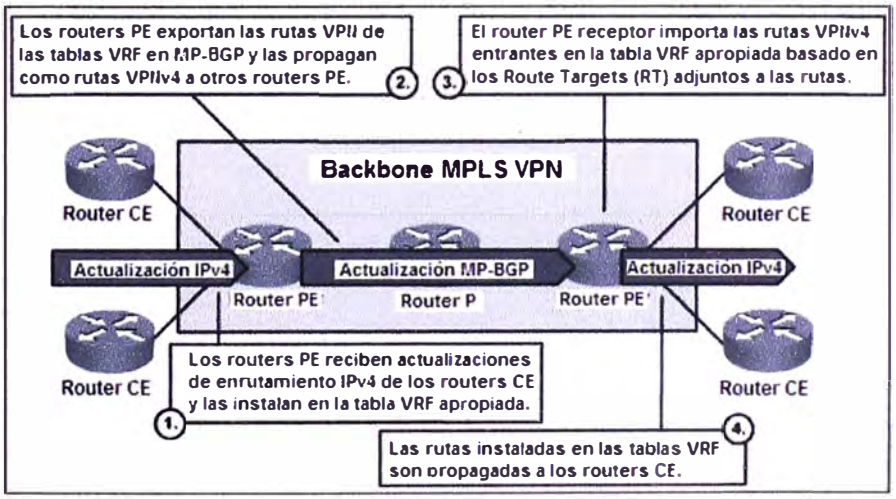


Figura 2.43 Flujo de información de enrutamiento extremo-a-extremo (Fuente: www.cisco.com)

-Paso2: Las rutas de clientes son exportadas desde la tabla VRF como rutas VPNv4 a través de MP-BGP y propagadas a otros routers PE.

-Paso3: Los routers PE reciben las actualizaciones MP-BGP e importan las rutas VPNv4 entrantes en sus tablas VRF basados en los RTs adjuntos a éstas rutas entrantes y en los import RTs configurados en las tablas VRF.

-Paso4: Las rutas VPNv4 instaladas en las tablas VRF son convertidas en rutas IPv4 y finalmente propagadas a los routers CE del otro extremo.

2.3.6. Envío de paquetes en MPLS VPN

Es posible utilizar el apilamiento de etiquetas MPLS para indicar al egress (salida) router PE que hacer con el paquete VPN. Al utilizar el apilamiento de etiquetas, el ingress (entrada) router PE etiqueta los paquetes IP entrantes con dos etiquetas:

La etiqueta externa del apilamiento es la etiqueta LDP (protocolo Label Distribution Protocol) para el egress router PE. Esta etiqueta garantiza que el paquete atravesará el backbone MPLS VPN y arribará al egress router PE.

La segunda etiqueta del apilamiento es asignada por el egress router PE e indica a éste router como forwardear los paquetes VPN entrantes. Esta segunda etiqueta podría apuntar directamente hacia una interfaz de salida en cuyo caso el egress router PE realizaría una búsqueda de etiquetas, ó hacia una tabla VRF, en cuyo caso el egress router PE realizaría primero una búsqueda de etiquetas para encontrar la tabla VRF y entonces realizar una búsqueda IP dentro de la tabla VRF.

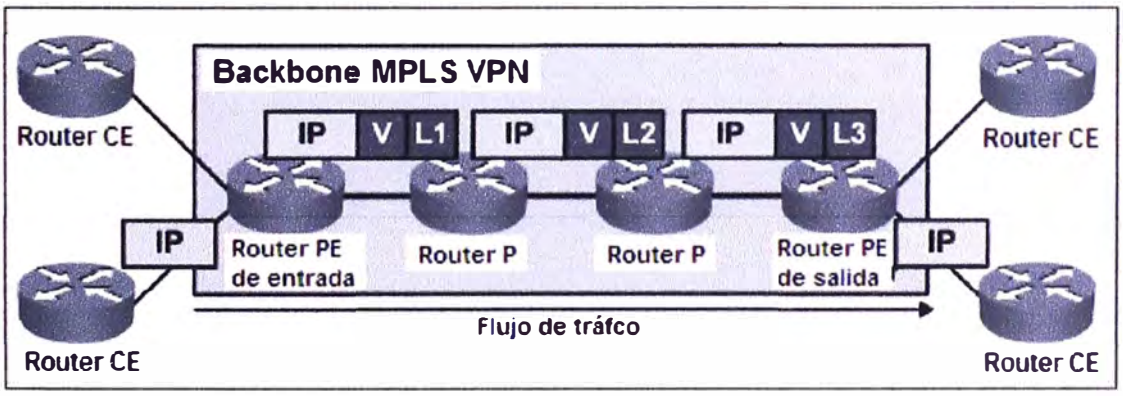


Figura 2.44 Envío de paquetes en el backbone MPLS VPN (Fuente: www.cisco.com)

Esta segunda etiqueta en el apilamiento apunta hacia una interfaz de salida siempre que el router CE sea el next-hop (salto siguiente) de la ruta VPN. La segunda etiqueta en el apilamiento apunta a una tabla VRF para la adición de rutas VPN, rutas VPN apuntando a la interfaz null y rutas para interfaces VPN directamente conectadas.

Estos dos niveles de apilamiento de etiquetas MPLS satisfacen los siguientes requerimientos de envío MPLS VPN:

*Los routers P realizan una conmutación de etiqueta en la etiqueta asignada por LDP hacia el egress router PE.

*El egress router PE realiza una conmutación de la segunda etiqueta (la cual fue previamente asignada por él) y envía el paquete IP hacia el router CE ó realiza otra búsqueda IP en la tabla VRF basado en ésta segunda etiqueta del apilamiento.

-MPLS VPN PHP (Penultimate Hop Popping)

Penúltimamente Hop Popping (PHP), la remoción de la primera etiqueta (top) del apilamiento en el salto hacia el egress router PE, puede ser realizado en este tipo de redes MPLS.

En estas redes, el último router P en el túnel LSP (Label Switch Path) quita la etiqueta LDP de acuerdo a lo requerido previamente por el router PE (envío de etiqueta de tipo "null") a través de LDP; por tanto el router PE recibe un paquete etiquetado que contiene sólo la etiqueta VPN. Por tanto, una única búsqueda de etiquetas es suficiente en este paquete para ser enviado hacia el router CE.

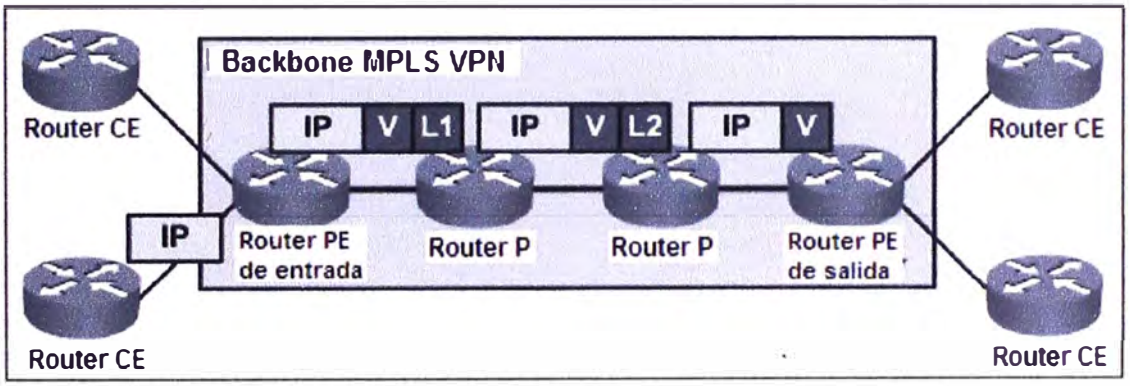


Figura 2.45 MPLS VPN con PHP (Fuente: www.cisco.com)

CAPITULO III
PLANTEAMIENTO DE LA SOLUCIÓN

3.1. Análisis de la solución:

Se realizará un análisis de la topología del cliente, de acuerdo a los requerimientos de conectividad y servicios a ser instalados en el centro de datos corporativo.

En el segmento LAN del centro de datos corporativo, serán instalados servidores de Directorio Activo, Bases de Datos, etc.

En el segmento DMZ del centro de datos corporativo, serán instalados servidores para publicaciones web hacia internet, el proxy para navegación de los usuarios de las sedes remotas y el relay de correos de los usuarios de las sedes remotas.

En el lado de las sedes remotas, se encuentran habilitados los servidores de Directorio Activo, quienes deben constantemente sincronizar con los servidores de Directorio Activo del centro de datos corporativo.

El protocolo utilizado para la conexión LAN y DMZ en el centro de datos corporativo y en las sedes remotas es Ethernet.

En el lado del centro de datos corporativo, debido a la gran demanda de uso de los servicios de Directorio Activo, Bases de Datos, se ha considerado utilizar tarjetas de red y switches de acceso con velocidades Gigabit Ethernet (1000 Mbps),

En el lado de las sedes remotas, para el acceso de los usuarios a la red local y a los servicios del centro de datos corporativo se utilizan switches con velocidades FastEthernet (100 Mbps).

Finalmente, para la conectividad a nivel WAN, se ha contratado los servicios de un proveedor de Telecomunicaciones, quien realizará las funciones de transporte de los datos desde las sedes remotas hacia el centro de datos corporativo en IBM.

Este servicio de transporte que realiza el proveedor, incluye la aplicación de políticas de Calidad de Servicio (QoS) lo cual implica realizar la clasificación de los paquetes de datos en el router CE de las sedes remotas, basado en las direcciones IP origen y destino del tráfico; y asignar un caudal de ancho de banda a cada Clase correspondiente.

Estos caudales de ancho de banda son mantenidos por el proveedor hasta llegar al router CE ubicado en el centro de datos corporativo, el cual, entregará la información al switch

Core de esta sede.

En cada sede remota, así como en la sede IBM, se tienen dos equipos ruteadores, los cuales han sido configurados en modo activo-pasivo, a través del protocolo HSRP.

En este escenario, se contempla el uso del protocolo BGP, el cual es utilizado para habilitar el intercambio de rutas de manera dinámica entre el router PE (proveedor) y el router CE (cliente).

Por ello, cada uno de los dos routers CE ubicados en las sedes remotas y sede en IBM, mantendrá una sesión BGP con su correspondiente router PE.

La alta disponibilidad consiste en que si se presenta la condición de caída de la sesión BGP entre el router CE principal y su correspondiente router PE, ó la caída física del enlace (última milla) hacia el router CE principal ó la caída misma del router CE principal, el tráfico originado en la sede remota sea ruteado a través del router CE de respaldo y a través del éste, poder llegar hacia su correspondiente router PE y finalmente a la sede en IBM.

En la sede de IBM, el tráfico es enviado desde el router CE hacia el switch Core, el cual enviará el tráfico al segmento LAN o DMZ a través del uso de enrutamiento estático.

Finalmente, para el acceso a internet se cuenta con un enlace de 15 Mbps para los servicios de navegación y correo de las sedes remotas.

3.1.1. Características de los equipos de red utilizados

Es importante definir previamente los servicios que utilizará el cliente sobre la red del proveedor (BW por cada servicio), tener en cuenta el nivel de escalabilidad, es decir, que los equipos a instalar permitan el crecimiento de la red con el mínimo de cambios necesarios. De acuerdo a esto, en la tabla B.2 se indican las características de los equipos de red utilizados en el lado remoto y en la sede en IBM.

3.2. Topología de la red:

Para el caso de la sede remota la topología física es de tipo estrella, donde se tienen estaciones de trabajo (sede Seal, Arequipa) y servidores (sede IBM, Lima) conectados a un switch; el cual se conecta directamente al router del proveedor.

Para el caso de la sede en IBM, la topología física es de tipo estrella, donde se tienen los servidores de (BD, Directorio Activo, Correo.) los cuales se encuentran conectados a un switch blade marca Cisco, modelo WS-CBS3110X-S-I.

A este switch blade, se conecta un switch Core modelo WS-C6506-E que realiza las funciones de inter vlan routing, (segmentos lan de las empresas pertenecientes al grupo grupo FONAFE).

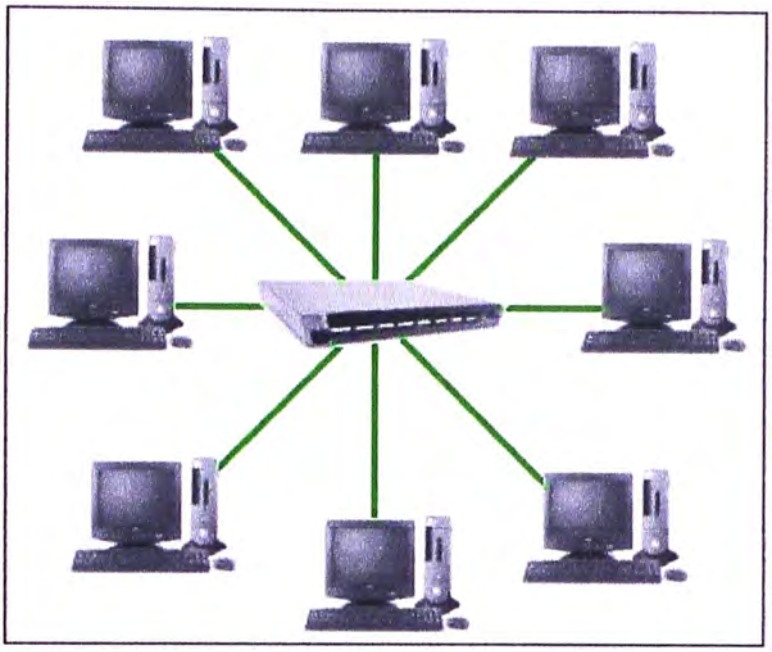


Figura 3.1 Topología de red de la sede remota del cliente

Finalmente, este switch Core, se interconecta a los routers CE principal y respaldo, modelos 7206VXR para el envío del tráfico a través del proveedor de servicios hacia la sede remota.

Para el acceso a internet de las sedes remotas se tienen 2 firewalls marca Cisco, modelo ASA5540 configurados en alta disponibilidad, los cuales se interconectan a 2 routers Cisco, configurados también, en alta disponibilidad.

Revisando la topología en modo global, debemos considerar la infraestructura de red del proveedor de servicios, la cual consta de una red de acceso basado en enlaces con tecnología Metro Ethernet; con última milla de fibra óptica que llega a las sedes del cliente donde se interconecta a los equipos ruteadores del cliente a través de un conversor de medios.

Tanto la sede en IBM como la sede en Seal, tendrán dos enlaces (principal y respaldo) de fibra óptica como última milla.

De manera similar se tendrá en cada sede dos ruteadores con una configuración a nivel de protocolo de enrutamiento dinámico que les permita redireccionar automáticamente el tráfico a través del enlace de respaldo ante una situación de falla en alguno de los componentes (ruteo a nivel del proveedor, enlace de última milla, media converter, router principal) del enlace principal.

Finalmente, el enlace entre las sedes IBM y Seal a nivel capa enlace de datos y capa de red serán realizados a través del proveedor de servicios quien será el responsable del transporte de los datos desde el router CE de la sede remota hacia el router CE de la sede en IBM.

3.3. Plan de direccionamiento IP:

Se realiza una distribución de las direcciones IP de la siguiente forma:

Tabla 3.1 Distribución de direcciones IPs.

Sedes	Redes LAN	Redes WAN
Sede IBM (Lima)	LAN: 10.116.1.0/24 DMZ: 10.116.4. 0/24 INTERNET:	WAN Enlace RPVN Principal: 10.15.24.236/30 WAN Enlace RPVN Respaldo: 10.10.94.100/30
Sede Seal (Arequipa)	LAN: 192.168.50.0/24	WAN Enlace RPVN Principal: 10.225.68.184/30 WAN Enlace RPVN Respaldo: 10.225.68.192/30

3.3.1. Plan de direccionamiento para la red LAN y DMZ:

IPs red LAN de IBM: 10.116.1.0, con máscara de red: 255.255.255.0

IPs red DMZ de IBM: 10.116.4.0, con máscara de red: 255.255.255.0

IPs red LAN sede Seal (Arequipa): 192.168.50.0, con máscara de red: 255.255.255.0

3.3.2. Plan de direccionamiento para las redes WAN:

IPs red WAN sede IBM: 10.15.24.236, con máscara de red: 255.255.255.252

IPs red WAN sede IBM Respaldo: 10.10.94.100, con máscara de red: 255.255.255.252

IPs red WAN sede Seal: 10.225.68.184, con máscara de red: 255.255.255.252

IPs red WAN sede Seal Respaldo: 10.225.68.192, con máscara de red: 255.255.255.252

Cabe mencionar que tanto en la sede IBM (Lima) como en la sede Seal (Arequipa) se tienen 2 ruteadores para transportar el tráfico de los enlaces Principal y Respaldo.

Sede IBM:

Router Principal: PLM-CF-FNF-1

Router Respaldo: PLM-CF-FNF-2

Sede Seal:

Router Principal: fnf-seal-cf-1

Router Respaldo: fnf-seal-cf-2

3.4. Implementación del protocolo BGP

Configuraciones:

En el lado de la sede remota:

Para la implementación de esta red se ha utilizado un router Cisco modelo 2921 con interfaces Gigabit Ethernet y FastEthernet como router principal y un router Cisco modelo 2921 con interfaces Gigabit Ethernet y FastEthernet como router de Respaldo.

Ambos routers CE se encuentran habilitados con el protocolo HSRP, el cual permite la alta disponibilidad de los equipos, permitiendo que ante una situación de caída de la interfaz WAN, LAN ó del propio router principal, de manera automática el router de respaldo tome control del proceso de enrutamiento del tráfico de datos.

A nivel de BGP, los dos routers CE tanto de las sedes remotas como de la sede en IBM, presentan una configuración en la cual el router principal y el de respaldo mantienen cada uno tres sesiones BGP: una sesión con su correspondiente router PE para el servicio RPVL, otra sesión con este router PE para el servicio RPVN y una tercera sesión a través de la interfaz LAN para la comunicación entre ambos router CE.

Para el caso del router CE principal de una sede remota, la sesión BGP que mantiene con su correspondiente router PE para el servicio RPVL, le permite el intercambio de redes pertenecientes a los segmentos de red LAN del resto de sedes remotas ubicadas localmente en la misma zona geográfica (ciudad). La sesión BGP que mantiene con su correspondiente router PE para el servicio RPVN, le permite el intercambio de redes pertenecientes a los segmentos de red LAN del resto de sedes remotas ubicadas geográficamente en diversas zonas, ciudades del exterior. Por ejemplo, para el caso de la sede Seal (Arequipa), a través de esta sesión BGP para el servicio RPVN, son recibidas las redes que pertenecen al segmento LAN y DMZ de la sede ubicada en IBM (Lima).

Finalmente, el router CE principal mantiene con su correspondiente router CE de respaldo, una sesión BGP a través de su interfaz lan para el intercambio de redes entre ambos routers, con el objeto que en caso se presente una falla en la nube MPLS del proveedor que impida que el router CE principal deje de recibir las redes remotas a través de la interfaz WAN, éstas sean recibidas a través de la interfaz LAN, de su router CE de respaldo.

En el lado de la sede en IBM:

Para la implementación de esta red se ha utilizado un router Cisco modelo 7206 con interfaces Gigabit Ethernet y FastEthernet como router principal y un router Cisco modelo 7206 con interfaces Gigabit Ethernet y FastEthernet como router de Respaldo.

De manera similar a las sedes remotas, ambos routers CE ubicados en la sede de IBM se encuentran habilitados con el protocolo HSRP, que permite la alta disponibilidad de los mismos de manera automática.

Similarmente a como se tiene habilitado para las sedes remotas, ambos routers CE de la sede en IBM presentan una configuración en la cual mantienen cada uno de ellos, tres sesiones BGP: una sesión con su correspondiente router PE para el servicio RPVL, otra sesión con el mismo router PE para el servicio RPVN y una tercera sesión a través de la interfaz LAN para la comunicación entre ambos router CE.

Como red de acceso se tiene la red MetroEthernet (red del proveedor) la cual provee el transporte a nivel capa 2 desde el router CE de la sede remota (ó sede en IBM) hacia el router PE del backbone MPLS.

Esta red de acceso transporta la data de los servicios de conectividad local y nacional (RPVL y RPVN) contratados por el cliente.

El enlace Principal es el encargado de transportar la data del cliente a través de esta red de acceso y transporte, desde el router CE de la sede remota hasta el router PE de la red MPLS en Arequipa.

Sólo cuando éste enlace presente una falla (caída de la interfaz wan del router CE, interfaz LAN del router CE, enlace de última milla, etc) la data del cliente será transportada a través del enlace de Respaldo.

Las siguientes tablas muestran la configuración de las políticas de calidad de servicio en el router CE principal (y respaldo) de la sede remota.

La configuración en la interfaz WAN se aplicará en modo troncal para pasar las vlan's de la red privada virtual nacional (RPVN) y la red privada virtual local (RPVL).

Se observa las políticas de QoS aplicadas a cada sub-interfaz "Shape8192N" y "Shape8192L" para la red red privada virtual nacional (RPVN) y la red privada virtual local (RPVL), respectivamente.

3.4.1. Configuración del router principal (activo) de la sede remota Seal, ubicada en Arequipa.

```
interface GigabitEthernet0/0
 description Enlace WAN IBM SEAL AREQUIPA
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 load-interval 30
 duplex full
 speed 100
interface GigabitEthernet0/0.10
```

```
 description Enlace WAN RPVN IBM SEAL AREQUIPA - CID:1056709
 encapsulation dot1Q 1334
 ip address 10.225.68.186 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip flow egress
 ip nat outside
 ip virtual-reassembly in
 service-policy output Shape8192N

interface GigabitEthernet0/0.20
 description Enlace WAN RPVL IBM SEAL AREQUIPA - CID:1056710
 encapsulation dot1Q 1333
 ip address 10.225.68.182 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip flow egress
 service-policy output Shape8192L
```

La interfaz G0/1 es la que recibirá el tráfico proveniente de la Lan del cliente.

```
#####Se observa la política de QoS "SetDscpLan"
interface GigabitEthernet0/1
 description Enlace LAN Cliente
 ip address 10.0.10.120 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip flow egress
 ip nat inside
 ip virtual-reassembly in
 standby 1 ip 10.0.10.122
```

```
 standby 1 priority 110
 standby 1 preempt
 standby 1 track 1 decrement 20
 load-interval 30
 duplex auto
 speed auto
 service-policy input SetDscpLan
```

3.4.2. Configuración del protocolo BGP en el router CE principal

```
router bgp 64516
 bgp router-id 10.233.5.197
 bgp log-neighbor-changes
 neighbor RPVN.IBM.SEAL peer-group
 neighbor RPVN.IBM.SEAL remote-as 12252
 neighbor RPVN.IBM.SEAL password 7 13170704055D426E686B
 neighbor RPVN.IBM.SEAL timers 10 30
 neighbor RPVL.IBM.SEAL peer-group
 neighbor RPVL.IBM.SEAL remote-as 12252
 neighbor RPVL.IBM.SEAL password 7 01011612575A404B6203
 neighbor RPVL.IBM.SEAL timers 10 30
 neighbor LAN_SEAL_PRI peer-group
 neighbor LAN_SEAL_PRI remote-as 64516
 neighbor LAN_SEAL_PRI password 7 000847084148580703650F01
 neighbor LAN_SEAL_PRI timers 10 30
 neighbor 10.0.10.121 peer-group LAN_SEAL_PRI
 neighbor 10.0.10.121 description Enlace LAN CE principal
 neighbor 10.225.68.181 peer-group RPVL.IBM.SEAL
 neighbor 10.225.68.181 description Enlace WAN Prin IBM-SEAL
 neighbor 10.225.68.185 peer-group RPVN.IBM.SEAL
 neighbor 10.225.68.185 description Enlace WAN Principal IBM-SEAL

 address-family ipv4
  network 10.233.5.197 mask 255.255.255.255
  redistribute connected
  redistribute static
  neighbor RPVN.IBM.SEAL send-community both
```

```
 neighbor RPVN.IBM.SEAL soft-reconfiguration inbound
 neighbor RPVN.IBM.SEAL route-map FROM_VPN_CLARO_NACIONAL in
 neighbor RPVN.IBM.SEAL route-map SET_VPN_CLARO_NACIONAL out
 neighbor RPVL.IBM.SEAL send-community both
 neighbor RPVL.IBM.SEAL soft-reconfiguration inbound
 neighbor RPVL.IBM.SEAL route-map FROM_VPN_CLARO_LOCAL in
 neighbor RPVL.IBM.SEAL route-map SET_VPN_CLARO_LOCAL out
 neighbor LAN_SEAL_PRI send-community both
 neighbor LAN_SEAL_PRI next-hop-self
 neighbor LAN_SEAL_PRI soft-reconfiguration inbound
 neighbor 10.0.10.121 activate
 neighbor 10.225.68.181 activate
 neighbor 10.225.68.185 activate
 no auto-summary
exit-address-family

ip bgp-community new-format
```

Rutas estáticas para acceso a los segmentos Lan del cliente:

```
ip route 10.22.11.0 255.255.255.0 10.0.10.1
ip route 10.23.11.0 255.255.255.0 10.0.10.1
ip route 100.10.10.0 255.255.255.0 10.0.10.1
ip route 192.116.40.0 255.255.255.0 10.0.10.1
ip route 192.116.60.0 255.255.255.0 10.0.10.1
ip route 192.116.100.0 255.255.255.0 10.0.10.1
ip route 192.116.120.0 255.255.255.0 10.0.10.1
ip route 192.116.140.0 255.255.255.0 10.0.10.1
ip route 192.168.10.0 255.255.255.0 10.0.10.1
ip route 192.168.30.0 255.255.255.0 10.0.10.1
ip route 192.168.40.0 255.255.255.0 10.0.10.1
ip route 192.168.50.0 255.255.255.0 10.0.10.1
ip route 192.168.60.0 255.255.255.0 10.0.10.1
ip route 192.168.61.0 255.255.255.0 10.0.10.1
ip route 192.168.70.0 255.255.255.0 10.0.10.1
ip route 192.168.100.0 255.255.255.0 10.0.10.1
ip route 192.168.130.0 255.255.255.0 10.0.10.1
ip route 192.169.11.0 255.255.255.0 10.0.10.1
```

ip route 192.169.14.0 255.255.255.0 10.0.10.1

Access-list para las políticas de Calidad de Servicio (QoS):

ip access-list extended qos2

permit ip 10.10.0.0 0.0.255.255 10.110.6.0 0.0.0.255

permit ip 10.10.0.0 0.0.255.255 host 10.112.1.4

permit ip 10.10.0.0 0.0.255.255 host 10.112.1.5

permit ip 10.10.0.0 0.0.255.255 host 10.112.1.6

permit ip 10.10.0.0 0.0.255.255 host 10.112.1.7

permit ip 10.10.0.0 0.0.255.255 host 10.112.1.8

permit ip 10.10.0.0 0.0.255.255 host 10.112.1.9

permit ip 10.10.0.0 0.0.255.255 host 10.112.4.3

ip access-list extended qos5

permit ip 10.10.0.0 0.0.255.255 10.110.100.0 0.0.0.255

Creación de filtros (prefix-list) para implementación de alta disponibilidad:

ip prefix-list Redes.IBM.SEAL seq 10 permit 10.225.68.184/30

ip prefix-list Redes.IBM.SEAL seq 20 permit 10.225.68.180/30

ip prefix-list Redes.IBM.SEAL seq 30 permit 10.233.5.197/32

ip prefix-list Redes.IBM.SEAL seq 40 permit 10.22.11.0/24

ip prefix-list Redes.IBM.SEAL seq 50 permit 10.23.11.0/24

ip prefix-list Redes.IBM.SEAL seq 60 permit 100.10.10.0/24

ip prefix-list Redes.IBM.SEAL seq 70 permit 192.168.40.0/24

ip prefix-list Redes.IBM.SEAL seq 80 permit 192.168.50.0/24

ip prefix-list Redes.IBM.SEAL seq 110 permit 192.168.70.0/24

ip prefix-list Redes.IBM.SEAL seq 120 permit 192.168.100.0/24

ip prefix-list Redes.IBM.SEAL seq 130 permit 192.169.11.0/24

ip prefix-list Redes.IBM.SEAL seq 140 permit 192.169.14.0/24

ip prefix-list Redes.IBM.SEAL seq 150 permit 10.0.10.0/24

ip prefix-list Redes.IBM.SEAL seq 160 permit 192.168.10.0/24

ip prefix-list Redes.IBM.SEAL seq 170 permit 192.168.30.0/24

ip prefix-list Redes.IBM.SEAL seq 190 permit 192.168.130.0/24

ip prefix-list Redes.IBM.SEAL seq 200 permit 192.116.40.0/24

ip prefix-list Redes.IBM.SEAL seq 210 permit 192.116.60.0/24

ip prefix-list Redes.IBM.SEAL seq 220 permit 192.116.100.0/24

ip prefix-list Redes.IBM.SEAL seq 230 permit 192.116.120.0/24

ip prefix-list Redes.IBM.SEAL seq 240 permit 192.116.140.0/24

ip prefix-list Redes_all seq 10 permit 0.0.0.0/0 le 32

```
route-map SET_VPN_CLARO_NACIONAL permit 10
 description Envia solo redes Lan internas de esta sede remota
 match ip address prefix-list Redes.IBM.SEAL
 set community 12252:1200
route-map FROM_VPN_CLARO_LOCAL deny 10
 description Deniega las redes anunciadas por esta sede
 match ip address prefix-list Redes.IBM.SEAL
route-map FROM_VPN_CLARO_LOCAL permit 20
 description Recibe Todas las redes por la WAN de claro
 match ip address prefix-list Redes_all
route-map SET_VPN_CLARO_LOCAL permit 10
 description Envia solo redes Lan internas de esta sede remota
 match ip address prefix-list Redes.IBM.SEAL
 set community 12252:1200
route-map FROM_VPN_CLARO_NACIONAL deny 10
 description Deniega las redes anunciadas por esta sede
 match ip address prefix-list Redes.IBM.SEAL
route-map FROM_VPN_CLARO_NACIONAL permit 20
 description Recibe Todas las redes por la WAN de claro
 match ip address prefix-list Redes_all
```

3.4.3. Configuración del router de respaldo (pasivo) de la sede en Arequipa

```
interface GigabitEthernet0/0
 description Enlace WAN IBM SEAL AREQUIPA CONTINGENCIA
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 load-interval 30
 duplex full
 speed 100
interface GigabitEthernet0/0.10
 description Enlace WAN RPVN IBM SEAL AREQUIPA - CID:1056708
 encapsulation dot1Q 1337
 ip address 10.225.68.194 255.255.255.252
 no ip redirects
```

```
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip flow egress
 ip nat outside
 ip virtual-reassembly in
 service-policy output Shape2048N
interface GigabitEthernet0/0.20
 description Enlace WAN RPVL IBM SEAL AREQUIPA - CID:1056711
 encapsulation dot1Q 1336
 ip address 10.225.68.190 255.255.255.252
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip flow egress
 service-policy output Shape2048L
interface GigabitEthernet0/1
 description Enlace LAN Cliente
 ip address 10.0.10.121 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 ip flow ingress
 ip flow egress
 ip nat inside
 ip virtual-reassembly in
 standby 1 ip 10.0.10.122
 standby 1 preempt
 load-interval 30
 duplex auto
 speed auto
 service-policy input SetDscpLan
```

3.4.4. Configuración del protocolo BGP en el router CE de respaldo

```
router bgp 64516
```

```
bgp router-id 10.233.5.199
bgp log-neighbor-changes
neighbor RPVN.IBM.SEAL peer-group
neighbor RPVN.IBM.SEAL remote-as 12252
neighbor RPVN.IBM.SEAL password rpvn1&$#/
neighbor RPVN.IBM.SEAL timers 10 30
neighbor RPVL.IBM.SEAL peer-group
neighbor RPVL.IBM.SEAL remote-as 12252
neighbor RPVL.IBM.SEAL password rpvl1&$#/
neighbor RPVL.IBM.SEAL timers 10 30
neighbor LAN_SEAL_PRI peer-group
neighbor LAN_SEAL_PRI remote-as 64516
neighbor LAN_SEAL_PRI password l4n%s3al$#/
neighbor LAN_SEAL_PRI timers 10 30
neighbor 10.0.10.120 peer-group LAN_SEAL_PRI
neighbor 10.0.10.120 description Enlace LAN CE principal
neighbor 10.225.68.189 peer-group RPVL.IBM.SEAL
neighbor 10.225.68.189 description Enlace WAN Prin IBM-SEAL
neighbor 10.225.68.193 peer-group RPVN.IBM.SEAL
neighbor 10.225.68.193 description Enlace WAN Principal IBM-SEAL

address-family ipv4
 network 10.233.5.199 mask 255.255.255.255
 redistribute connected
 redistribute static
 neighbor RPVN.IBM.SEAL send-community both
 neighbor RPVN.IBM.SEAL soft-reconfiguration inbound
 neighbor RPVN.IBM.SEAL route-map FROM_VPN_CLARO_NACIONAL in
 neighbor RPVN.IBM.SEAL route-map SET_VPN_CLARO_NACIONAL out
 neighbor RPVL.IBM.SEAL send-community both
 neighbor RPVL.IBM.SEAL soft-reconfiguration inbound
 neighbor RPVL.IBM.SEAL route-map FROM_VPN_CLARO_LOCAL in
 neighbor RPVL.IBM.SEAL route-map SET_VPN_CLARO_LOCAL out
 neighbor LAN_SEAL_PRI send-community both
 neighbor LAN_SEAL_PRI next-hop-self
 neighbor LAN_SEAL_PRI soft-reconfiguration inbound
```

```
  neighbor 10.0.10.120 activate
  neighbor 10.225.68.189 activate
  neighbor 10.225.68.193 activate
  no auto-summary
 exit-address-family

ip bgp-community new-format
ip route 10.22.11.0 255.255.255.0 10.0.10.1
ip route 10.23.11.0 255.255.255.0 10.0.10.1
ip route 100.10.10.0 255.255.255.0 10.0.10.1
ip route 192.116.40.0 255.255.255.0 10.0.10.1
ip route 192.116.60.0 255.255.255.0 10.0.10.1
ip route 192.116.100.0 255.255.255.0 10.0.10.1
ip route 192.116.120.0 255.255.255.0 10.0.10.1
ip route 192.116.140.0 255.255.255.0 10.0.10.1
ip route 192.168.10.0 255.255.255.0 10.0.10.1
ip route 192.168.30.0 255.255.255.0 10.0.10.1
ip route 192.168.40.0 255.255.255.0 10.0.10.1
ip route 192.168.50.0 255.255.255.0 10.0.10.1
ip route 192.168.60.0 255.255.255.0 10.0.10.1
ip route 192.168.61.0 255.255.255.0 10.0.10.1
ip route 192.168.70.0 255.255.255.0 10.0.10.1
ip route 192.168.100.0 255.255.255.0 10.0.10.1
ip route 192.168.130.0 255.255.255.0 10.0.10.1
ip route 192.169.11.0 255.255.255.0 10.0.10.1
ip route 192.169.14.0 255.255.255.0 10.0.10.1
ip access-list extended qos2
 permit ip 10.10.0.0 0.0.255.255 10.110.6.0 0.0.0.255
 permit ip 10.10.0.0 0.0.255.255 host 10.112.1.4
 permit ip 10.10.0.0 0.0.255.255 host 10.112.1.5
 permit ip 10.10.0.0 0.0.255.255 host 10.112.1.6
 permit ip 10.10.0.0 0.0.255.255 host 10.112.1.7
 permit ip 10.10.0.0 0.0.255.255 host 10.112.1.8
 permit ip 10.10.0.0 0.0.255.255 host 10.112.1.9
 permit ip 10.10.0.0 0.0.255.255 host 10.112.4.3
ip access-list extended qos5
```

```
 permit ip 10.10.0.0 0.0.255.255 10.110.100.0 0.0.0.255
ip prefix-list Redes.IBM.SEAL seq 10 permit 10.233.5.199/32
ip prefix-list Redes.IBM.SEAL seq 20 permit 10.225.68.192/30
ip prefix-list Redes.IBM.SEAL seq 30 permit 10.225.68.188/30
ip prefix-list Redes.IBM.SEAL seq 40 permit 10.22.11.0/24
ip prefix-list Redes.IBM.SEAL seq 50 permit 10.23.11.0/24
ip prefix-list Redes.IBM.SEAL seq 60 permit 100.10.10.0/24
ip prefix-list Redes.IBM.SEAL seq 70 permit 192.168.40.0/24
ip prefix-list Redes.IBM.SEAL seq 80 permit 192.168.50.0/24
ip prefix-list Redes.IBM.SEAL seq 90 permit 192.168.60.0/24
ip prefix-list Redes.IBM.SEAL seq 100 permit 192.168.61.0/24
ip prefix-list Redes.IBM.SEAL seq 110 permit 192.168.70.0/24
ip prefix-list Redes.IBM.SEAL seq 120 permit 192.168.100.0/24
ip prefix-list Redes.IBM.SEAL seq 130 permit 192.169.11.0/24
ip prefix-list Redes.IBM.SEAL seq 140 permit 192.169.14.0/24
ip prefix-list Redes.IBM.SEAL seq 150 permit 10.0.10.0/24
ip prefix-list Redes.IBM.SEAL seq 160 permit 192.168.10.0/24
ip prefix-list Redes.IBM.SEAL seq 170 permit 192.168.30.0/24
ip prefix-list Redes.IBM.SEAL seq 190 permit 192.168.130.0/24
ip prefix-list Redes.IBM.SEAL seq 200 permit 192.116.40.0/24
ip prefix-list Redes.IBM.SEAL seq 210 permit 192.116.60.0/24
ip prefix-list Redes.IBM.SEAL seq 220 permit 192.116.100.0/24
ip prefix-list Redes.IBM.SEAL seq 230 permit 192.116.120.0/24
ip prefix-list Redes.IBM.SEAL seq 240 permit 192.116.140.0/24

ip prefix-list Redes_all seq 10 permit 0.0.0.0/0 le 32
route-map SET_VPN_CLARO_NACIONAL permit 10
 description Envia solo redes Lan internas de esta sede remota
 match ip address prefix-list Redes.IBM.SEAL
 set community 12252:1201

route-map FROM_VPN_CLARO_LOCAL deny 10
 description Deniega las redes anunciadas por esta sede
 match ip address prefix-list Redes.IBM.SEAL

route-map FROM_VPN_CLARO_LOCAL permit 20
```

```
 description Recibe Todas las redes por la WAN de claro
 match ip address prefix-list Redes_all

route-map SET_VPN_CLARO_LOCAL permit 10
 description Envia solo redes Lan internas de esta sede remota
 match ip address prefix-list Redes.IBM.SEAL
 set community 12252:1201

route-map FROM_VPN_CLARO_NACIONAL deny 10
 description Deniega las redes anunciadas por esta sede
 match ip address prefix-list Redes.IBM.SEAL

route-map FROM_VPN_CLARO_NACIONAL permit 20
 description Recibe Todas las redes por la WAN de claro
 match ip address prefix-list Redes_all
```

3.4.5. Configuración en el router PE de la sede remota

```
interface GigabitEthernet1/1/6.101334
 description CID 1056709  Ibm Del Peru S.A.C. Seal-Arequipa
 encapsulation dot1Q 1334
 ip vrf forwarding 40120
 ip address 10.225.68.185 255.255.255.252
 no ip directed-broadcast
 no cdp enable
 service-policy input Shape8192
 service-policy output Shape8192_1024_4096_3072

interface GigabitEthernet1/1/6.101337
 description CID 1069830  Ibm Del Peru S.A.C. Seal-Arequipa
 encapsulation dot1Q 1337
 ip vrf forwarding 40120
 ip address 10.225.68.193 255.255.255.252
 no ip directed-broadcast
 no cdp enable
 service-policy input Shape2048
```

```
 service-policy output Shape2048_512_1024_512
end
router bgp 12252

address-family ipv4 vrf 40120
 redistribute connected
 neighbor IBM_RPVN_FONAFE peer-group
 neighbor IBM_RPVN_FONAFE remote-as 64516
 neighbor IBM_RPVN_FONAFE password 7 071D315A40585F41545D
 neighbor IBM_RPVN_FONAFE timers 10 30
 neighbor IBM_RPVN_FONAFE activate
 neighbor IBM_RPVN_FONAFE send-community both
 neighbor IBM_RPVN_FONAFE as-override
 neighbor IBM_RPVN_FONAFE soft-reconfiguration inbound
 neighbor IBM_RPVN_FONAFE route-map dualhome in
 neighbor 10.225.68.186 peer-group IBM_RPVN_FONAFE
 neighbor 10.225.68.186 description CID 1056709
 neighbor 10.225.68.194 peer-group IBM_RPVN_FONAFE
 neighbor 10.225.68.194 description CID 1069830
 no synchronization
 exit-address-family
```

3.4.6. Configuración del router principal (activo) de la sede en IBM

```
interface GigabitEthernet0/1
 description Enlace WAN IBM PRINCIPAL
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 load-interval 30
 duplex full
 speed 1000
 media-type rj45
 negotiation auto

interface GigabitEthernet0/1.10
```

```
 description ENLACE WAN CLARO - CID 865441
 encapsulation dot1Q 3605
 ip address 10.15.24.210 255.255.255.252
 ip flow ingress
 ip nat inside
 ip virtual-reassembly
 service-policy output Shape87040-mail-serpostrep-fonafe

interface GigabitEthernet0/1.20
 description Enlace WAN CLARO RPVN - CID 1067757
 encapsulation dot1Q 3612
 ip address 10.15.24.238 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip flow ingress
 ip nat inside
 ip virtual-reassembly
 service-policy output Shape8192N

interface FastEthernet0/2
 ip address 10.110.1.17 255.255.255.0
 duplex full
 speed 100

interface GigabitEthernet0/2
 ip address 10.110.3.254 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 ip route-cache flow
 load-interval 30
 duplex full
 speed 1000
 media-type rj45
 negotiation auto
 standby 1 ip 10.110.3.2
 standby 1 priority 20
```

```
standby 1 preempt
standby 1 track GigabitEthernet0/1
```

3.4.7. Configuración del protocolo BGP en el router CE principal de la sede en IBM

```
router bgp 64516
 bgp router-id 10.234.6.46
 bgp log-neighbor-changes
 neighbor WAN_IBM peer-group
 neighbor WAN_IBM remote-as 12252
 neighbor WAN_IBM password 7 1557485F4C05646079
 neighbor WAN_IBM timers 10 30
 neighbor LAN_IBM peer-group
 neighbor LAN_IBM remote-as 64516
 neighbor LAN_IBM password 7 09090D5A512A58565A
 neighbor LAN_IBM timers 10 30
 neighbor RPVN.IBM peer-group
 neighbor RPVN.IBM remote-as 12252
 neighbor RPVN.IBM password 7 111B091319434D484765
 neighbor RPVN.IBM timers 10 30
 neighbor 10.15.24.209 peer-group WAN_IBM
 neighbor 10.15.24.209 description Enlace WAN  VPN Cliente
 neighbor 10.15.24.237 peer-group RPVN.IBM
 neighbor 10.15.24.237 description Enlace WAN RPVN IBM
 neighbor 10.110.3.253 peer-group LAN_IBM
 neighbor 10.110.3.253 description Enlace LAN CE RESPALDO

 address-family ipv4
  redistribute connected
  redistribute static
  neighbor WAN_IBM send-community both
  neighbor WAN_IBM soft-reconfiguration inbound
  neighbor WAN_IBM route-map From_VPN_Telmex in
  neighbor WAN_IBM route-map SET_TELMEX_COMM out
  neighbor LAN_IBM send-community both
  neighbor LAN_IBM next-hop-self
```

```
 neighbor LAN_IBM soft-reconfiguration inbound
 neighbor RPVN.IBM send-community both
 neighbor RPVN.IBM soft-reconfiguration inbound
 neighbor RPVN.IBM route-map FROM_VPN_CLARO_NACIONAL in
 neighbor RPVN.IBM route-map SET_VPN_CLARO_NACIONAL out
 neighbor 10.15.24.209 activate
 neighbor 10.15.24.237 activate
 neighbor 10.110.3.253 activate
 no auto-summary
 no synchronization
 network 0.0.0.0 route-map Enviar_Default
exit-address-family
####Rutas estáticas para acceso a los segmentos Lan, DMZ y de gestión en IBM:
ip route 10.7.7.100 255.255.255.255 10.110.3.1
ip route 10.7.7.214 255.255.255.255 10.110.3.1
ip route 10.110.2.0 255.255.255.0 10.110.3.1
ip route 10.110.4.0 255.255.255.0 10.110.3.1
ip route 10.110.6.0 255.255.255.0 10.110.3.1
ip route 10.110.7.0 255.255.255.0 10.110.3.1
ip route 10.110.8.0 255.255.255.0 10.110.3.1
ip route 10.110.13.0 255.255.255.0 10.110.3.1
ip route 10.110.24.0 255.255.255.192 10.110.3.246
ip route 10.110.100.0 255.255.255.0 10.110.3.1
ip route 10.110.101.0 255.255.255.0 10.110.3.1
ip route 10.111.1.0 255.255.255.0 10.110.3.1
ip route 10.111.4.0 255.255.255.0 10.110.3.1
ip route 10.112.1.0 255.255.255.0 10.110.3.1
ip route 10.112.4.0 255.255.255.0 10.110.3.1
ip route 10.113.1.0 255.255.255.0 10.110.3.1
ip route 10.113.4.0 255.255.255.0 10.110.3.1
ip route 10.113.7.0 255.255.255.0 10.110.3.1
ip route 10.114.1.0 255.255.255.0 10.110.3.1
ip route 10.114.4.0 255.255.255.0 10.110.3.1
ip route 10.114.7.0 255.255.255.0 10.110.3.1
ip route 10.115.1.0 255.255.255.0 10.110.3.1
ip route 10.115.4.0 255.255.255.0 10.110.3.1
```

```
ip route 10.115.7.0 255.255.255.0 10.110.3.1
ip route 10.116.1.0 255.255.255.0 10.110.3.1
ip route 10.116.4.0 255.255.255.0 10.110.3.1
ip route 67.228.239.60 255.255.255.255 10.110.3.1
ip route 69.191.192.0 255.255.192.0 10.110.3.1
ip route 80.37.226.115 255.255.255.255 10.110.3.1
ip route 129.39.161.112 255.255.255.240 10.110.3.1
ip route 129.39.162.96 255.255.255.240 10.110.3.1
ip route 129.39.162.192 255.255.255.192 10.110.1.1
ip route 129.39.163.165 255.255.255.255 10.110.1.1
ip route 129.39.178.64 255.255.255.192 10.110.3.1
ip route 129.39.179.32 255.255.255.224 10.110.3.1
######Access-list para las políticas de Calidad de Servicio (QoS):
ip access-list extended qos2
 deny   ip host 10.110.8.5 any
 deny   ip host 10.110.8.6 any
 permit ip any any
ip access-list extended qos2-serpostrep
 permit ip host 10.114.1.8 host 192.168.4.78
ip access-list extended qos5
 permit ip 10.110.100.0 0.0.0.255 host 10.0.15.218
 permit ip host 10.110.6.33 10.0.15.0 0.0.0.255
 permit ip host 10.110.6.33 10.0.16.0 0.0.7.255
 permit ip host 10.110.6.33 172.21.3.0 0.0.0.255
 permit ip host 10.110.6.33 172.21.4.0 0.0.0.255
 permit ip host 10.110.6.33 192.9.200.0 0.0.0.255
 deny   ip any any
######Creación de filtros (prefix-list) para implementación de alta disponibilidad:
ip prefix-list Red_LAN seq 5 permit 10.110.8.0/24
ip prefix-list Red_LAN seq 10 permit 10.110.7.0/24
ip prefix-list Red_LAN seq 15 permit 10.110.6.0/24
ip prefix-list Red_LAN seq 20 permit 10.110.3.0/24
ip prefix-list Red_LAN seq 25 permit 10.110.2.0/24
ip prefix-list Red_LAN seq 30 permit 10.110.1.0/24
ip prefix-list Red_LAN seq 35 permit 10.110.13.0/24
ip prefix-list Red_LAN seq 40 permit 10.110.100.0/24
```

```
ip prefix-list Red_LAN seq 45 permit 10.110.101.0/24
ip prefix-list Red_LAN seq 50 permit 0.0.0.0/0
ip prefix-list Red_LAN seq 55 permit 10.111.1.0/24
ip prefix-list Red_LAN seq 60 permit 10.111.4.0/24
ip prefix-list Red_LAN seq 65 permit 10.112.1.0/24
ip prefix-list Red_LAN seq 70 permit 10.112.4.0/24
ip prefix-list Red_LAN seq 75 permit 10.115.1.0/24
ip prefix-list Red_LAN seq 80 permit 10.115.4.0/24
ip prefix-list Red_LAN seq 85 permit 10.234.6.46/32
ip prefix-list Red_LAN seq 90 permit 129.39.162.192/26
ip prefix-list Red_LAN seq 95 permit 129.39.178.64/26
ip prefix-list Red_LAN seq 100 permit 10.15.24.208/30
ip prefix-list Red_LAN seq 105 permit 129.39.162.96/28
ip prefix-list Red_LAN seq 110 permit 10.114.1.0/24
ip prefix-list Red_LAN seq 115 permit 10.114.4.0/24
ip prefix-list Red_LAN seq 120 permit 10.113.1.0/24
ip prefix-list Red_LAN seq 125 permit 10.113.4.0/24
ip prefix-list Red_LAN seq 130 permit 10.116.1.0/24
ip prefix-list Red_LAN seq 135 permit 10.116.4.0/24
ip prefix-list Red_LAN seq 140 permit 10.233.5.197/32
ip prefix-list Red_LAN seq 150 permit 10.114.7.0/24
ip prefix-list Red_LAN seq 160 permit 10.110.24.0/26
ip prefix-list Red_LAN seq 170 permit 129.39.161.112/28
ip prefix-list Red_LAN seq 180 permit 10.110.4.0/24
ip prefix-list Red_LAN seq 190 permit 10.7.7.214/32
route-map SET_VPN_CLARO_NACIONAL permit 10
 description Envia solo redes Lan internas de esta sede remota
 match ip address prefix-list Red_LAN
 set community 12252:1200

route-map Enviar_Default permit 10
 set community 12252:1200

route-map SET_TELMEX_COMM permit 10
 match ip address prefix-list Red_LAN
 set community 12252:1200
```

```
route-map From_VPN_Telmex deny 10
 description denegacion de redes internas y default
 match ip address prefix-list Red_LAN

route-map From_VPN_Telmex permit 20
 description Permitir las demas Redes de Sedes Remotas
 match ip address prefix-list Redes_All

route-map FROM_VPN_CLARO_NACIONAL deny 10
 description Deniega las redes anunciadas por esta sede
 match ip address prefix-list Red_LAN

route-map FROM_VPN_CLARO_NACIONAL permit 20
 description Recibe Todas las redes por la WAN de claro
 match ip address prefix-list Redes_All
```

3.4.8. Configuración del router de respaldo (pasivo) de la sede en IBM

```
 description Enlace WAN IBM PRINCIPAL
 no ip address
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 load-interval 30
 duplex full
 speed 1000
 media-type rj45
 negotiation auto

interface GigabitEthernet0/1.10
 description ENLACE WAN CLARO - CID 865435
 encapsulation dot1Q 1384
 ip address 10.10.94.74 255.255.255.252
 ip flow ingress
 service-policy output Shape87040-mail-serpostrep-fonafe
```

```
interface GigabitEthernet0/1.20
 description Enlace WAN CLARO RPVN - CID 1067758
 encapsulation dot1Q 1390
 ip address 10.10.94.102 255.255.255.252
 no ip redirects
 no ip proxy-arp
 ip nat inside
 ip virtual-reassembly
 service-policy output Shape8192N

interface FastEthernet0/2
 ip address 10.110.1.27 255.255.255.0
 duplex auto
 speed auto

interface GigabitEthernet0/2
 ip address 10.110.3.253 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 ip route-cache flow
 load-interval 30
 duplex full
 speed 1000
 media-type rj45
 negotiation auto
 standby 1 ip 10.110.3.2
 standby 1 priority 15
 standby 1 preempt
 standby 1 track GigabitEthernet0/1
```

3.4.9. Configuración del protocolo BGP en el router CE de respaldo de la sede en IBM

```
router bgp 64516
 bgp router-id 10.232.33.22
 bgp log-neighbor-changes
 neighbor WAN_IBM peer-group
```

```
neighbor WAN_IBM remote-as 12252
neighbor WAN_IBM password 7 074A621F0626564146
neighbor WAN_IBM timers 10 30
neighbor LAN_IBM peer-group
neighbor LAN_IBM remote-as 64516
neighbor LAN_IBM password 7 09090D5A512A58565A
neighbor LAN_IBM timers 10 30
neighbor RPVN.IBM peer-group
neighbor RPVN.IBM remote-as 12252
neighbor RPVN.IBM password 7 095E5E1F175451564843
neighbor RPVN.IBM timers 10 30
neighbor 10.10.94.73 peer-group WAN_IBM
neighbor 10.10.94.73 description Enlace WAN  VPN IBM
neighbor 10.10.94.101 peer-group RPVN.IBM
neighbor 10.10.94.101 description Enlace WAN RPVN IBM
neighbor 10.110.3.254 peer-group LAN_IBM
neighbor 10.110.3.254 description Enlace LAN CE RESPALDO

address-family ipv4
 redistribute connected
 redistribute static
 neighbor WAN_IBM send-community both
 neighbor WAN_IBM soft-reconfiguration inbound
 neighbor WAN_IBM route-map From_VPN_Telmex in
 neighbor WAN_IBM route-map SET_TELMEX_COMM out
 neighbor LAN_IBM send-community both
 neighbor LAN_IBM next-hop-self
 neighbor LAN_IBM soft-reconfiguration inbound
 neighbor RPVN.IBM send-community both
 neighbor RPVN.IBM soft-reconfiguration inbound
 neighbor RPVN.IBM route-map FROM_VPN_CLARO_NACIONAL in
 neighbor RPVN.IBM route-map SET_VPN_CLARO_NACIONAL out
 neighbor 10.10.94.73 activate
 neighbor 10.10.94.101 activate
 neighbor 10.110.3.254 activate
 no auto-summary
```

```
 no synchronization
 network 0.0.0.0 route-map Enviar  Default
 network 10.10.94.72 mask 255.255.255.252
 network 10.110.3.0 mask 255.255.255.0
 network 10.232.33.22 mask 255.255.255.255
exit-address-family

ip forward-protocol nd
ip route 10.7.7.100 255.255.255.255 10.110.3.1
ip route 10.7.7.214 255.255.255.255 10.110.3.1
ip route 10.110.2.0 255.255.255.0 10.110.3.1
ip route 10.110.4.0 255.255.255.0 10.110.3.1
ip route 10.110.6.0 255.255.255.0 10.110.3.1
ip route 10.110.7.0 255.255.255.0 10.110.3.1
ip route 10.110.8.0 255.255.255.0 10.110.3.1
ip route 10.110.13.0 255.255.255.0 10.110.3.1
ip route 10.110.100.0 255.255.255.0 10.110.3.1
ip route 10.110.101.0 255.255.255.0 10.110.3.1
ip route 10.111.1.0 255.255.255.0 10.110.3.1
ip route 10.111.4.0 255.255.255.0 10.110.3.1
ip route 10.112.1.0 255.255.255.0 10.110.3.1
ip route 10.112.4.0 255.255.255.0 10.110.3.1
ip route 10.113.1.0 255.255.255.0 10.110.3.1
ip route 10.113.4.0 255.255.255.0 10.110.3.1
ip route 10.113.7.0 255.255.255.0 10.110.3.1
ip route 10.114.7.0 255.255.255.0 10.110.3.5
ip route 10.115.1.0 255.255.255.0 10.110.3.1
ip route 10.115.4.0 255.255.255.0 10.110.3.1
ip route 10.115.7.0 255.255.255.0 10.110.3.1
ip route 10.116.1.0 255.255.255.0 10.110.3.1
ip route 10.116.4.0 255.255.255.0 10.110.3.1
ip route 67.228.239.60 255.255.255.255 10.110.3.1
ip route 69.191.192.0 255.255.192.0 10.110.3.1
ip route 80.37.226.115 255.255.255.255 10.110.3.1
ip route 129.39.161.112 255.255.255.240 10.110.3.1
ip route 129.39.162.96 255.255.255.240 10.110.3.1
```

```
ip route 129.39.162.192 255.255.255.192 10.110.1.1
ip route 129.39.163.165 255.255.255.255 10.110.1.1
ip route 129.39.178.64 255.255.255.192 10.110.3.1
ip route 129.39.179.32 255.255.255.224 10.110.3.1
ip access-list extended qos2
 deny   ip host 10.110.8.5 any
 deny   ip host 10.110.8.6 any
 permit ip any any
ip access-list extended qos2-serpostrep
 permit ip host 10.114.1.8 host 192.168.4.78
ip access-list extended qos5
 permit ip 10.110.100.0 0.0.0.255 host 10.0.15.218
 permit ip host 10.110.6.33 10.0.15.0 0.0.0.255
 permit ip host 10.110.6.33 10.0.16.0 0.0.7.255
 permit ip host 10.110.6.33 172.21.3.0 0.0.0.255
 permit ip host 10.110.6.33 172.21.4.0 0.0.0.255
 permit ip host 10.110.6.33 192.9.200.0 0.0.0.255
 deny   ip any any

ip prefix-list Red_LAN seq 5 permit 10.110.8.0/24
ip prefix-list Red_LAN seq 10 permit 10.110.7.0/24
ip prefix-list Red_LAN seq 15 permit 10.110.6.0/24
ip prefix-list Red_LAN seq 20 permit 10.110.3.0/24
ip prefix-list Red_LAN seq 25 permit 10.110.2.0/24
ip prefix-list Red_LAN seq 30 permit 10.110.1.0/24
ip prefix-list Red_LAN seq 35 permit 10.110.13.0/24
ip prefix-list Red_LAN seq 40 permit 10.110.100.0/24
ip prefix-list Red_LAN seq 45 permit 10.110.101.0/24
ip prefix-list Red_LAN seq 50 permit 0.0.0.0/0
ip prefix-list Red_LAN seq 55 permit 10.111.1.0/24
ip prefix-list Red_LAN seq 60 permit 10.111.4.0/24
ip prefix-list Red_LAN seq 65 permit 10.112.1.0/24
ip prefix-list Red_LAN seq 70 permit 10.112.4.0/24
ip prefix-list Red_LAN seq 75 permit 10.115.1.0/24
ip prefix-list Red_LAN seq 80 permit 10.115.4.0/24
ip prefix-list Red_LAN seq 85 permit 10.232.33.22/32
```

```
ip prefix-list Red_LAN seq 90 permit 129.39.162.192/26
ip prefix-list Red_LAN seq 95 permit 129.39.178.64/26
ip prefix-list Red_LAN seq 100 permit 10.10.94.72/30
ip prefix-list Red_LAN seq 105 permit 129.39.162.96/28
ip prefix-list Red_LAN seq 110 permit 10.114.1.0/24
ip prefix-list Red_LAN seq 115 permit 10.114.4.0/24
ip prefix-list Red_LAN seq 120 permit 10.113.1.0/24
ip prefix-list Red_LAN seq 125 permit 10.113.4.0/24
ip prefix-list Red_LAN seq 130 permit 10.116.1.0/24
ip prefix-list Red_LAN seq 135 permit 10.116.4.0/24
ip prefix-list Red_LAN seq 140 permit 10.233.5.197/32
ip prefix-list Red_LAN seq 145 permit 10.0.10.0/24
ip prefix-list Red_LAN seq 150 permit 10.114.7.0/24
ip prefix-list Red_LAN seq 160 permit 10.110.24.0/26
ip prefix-list Red_LAN seq 170 permit 129.39.161.112/28
ip prefix-list Red_LAN seq 180 permit 10.110.4.0/24
ip prefix-list Red_LAN seq 190 permit 10.7.7.214/32

route-map SET_VPN_CLARO_NACIONAL permit 10
 description Envia solo redes Lan internas de esta sede remota
 match ip address prefix-list Red_LAN
 set community 12252:1201

route-map Enviar_Default permit 10
 set community 12252:1201

route-map SET_TELMEX_COMM permit 10
 match ip address prefix-list Red_LAN
 set community 12252:1201

route-map From_VPN_Telmex deny 10
 description denegacion de redes internas y default
 match ip address prefix-list Red_LAN

route-map From_VPN_Telmex permit 20
 description Permitir las demas Redes de Sedes Remotas
```

```
 match ip address prefix-list Redes_All

route-map FROM_VPN_CLARO_NACIONAL deny 10
 description Deniega las redes anunciadas por esta sede
 match ip address prefix-list Red_LAN

route-map FROM_VPN_CLARO_NACIONAL permit 20
 description Recibe Todas las redes por la WAN de claro
 match ip address prefix-list Redes_All
```

3.4.10 Pruebas de alta disponibilidad en los enlaces principal y respaldo

Luego de realizada la implementación de la sede remota Seal, se realizan las pruebas de alta disponibilidad donde el objetivo es probar que la conectividad entre la sede remota y la sede en IBM es automáticamente restablecida ante la caída de alguno de los componentes del enlace principal: Caída de la sesión BGP entre el router CE principal y su correspondiente router PE, caída del enlace de última milla del router CE principal, caída de la interfaz LAN del router CE principal y caída del propio router CE principal.

a) Prueba 1: Caída de la sesión BGP entre el router CE principal y su correspondiente router PE:

```
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=20ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=16ms TTL=251
Reply from 10.110.6.33: bytes=32 time=19ms TTL=251
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=16ms TTL=251
Reply from 10.110.6.33: bytes=32 time=23ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=19ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
```

Figura 3.2 Pérdida de conectividad desde la sede remota hacia la sede principal en IBM

```
IBM's internal systems must only be used only for conducting IBM's business, or for purposes au
thorized by IBM management.

username: ibmcbeas
password:

fnf-seal-cf-1#
fnf-seal-cf-1#
fnf-seal-cf-1#
fnf-seal-cf-1#
Dec 21 13:04:07.603: %BGP-5-ADJCHANGE: neighbor 10.225.68.181 Down BGP Notification sent
Dec 21 13:04:07.603: %BGP-3-NOTIFICATION: sent to neighbor 10.225.68.181 4/0 (hold time expired
) 0 bytes
Dec 21 13:04:07.607: %BGP_SESSION-5-ADJCHANGE: neighbor 10.225.68.181 IPv4 Unicast topology bas
e removed from session  BGP Notification sent
Dec 21 13:04:16.819: %BGP-5-ADJCHANGE: neighbor 10.225.68.185 Down BGP Notification sent
Dec 21 13:04:16.819: %BGP-3-NOTIFICATION: sent to neighbor 10.225.68.185 4/0 (hold time expired
) 0 bytes
Dec 21 13:04:16.823: %BGP_SESSION-5-ADJCHANGE: neighbor 10.225.68.185 IPv4 Unicast topology bas
e removed from session  BGP Notification sent
```

Figura 3.3 Caída de sesión BGP entre router CE principal y router PE

Para esta prueba, el proveedor de servicios realiza el apagado de la interfaz del switch de acceso que se encuentra en el POP de dicho proveedor, ubicado en Arequipa, del la cual viene el enlace de última milla hacia el router CE principal de la sede remota.

Ante la caída de la interfaz del switch de acceso, se observa en la figura 3.3 que las dos sesiones BGP (neighbor 10.225.68.181 y neighbor 10.225.68.185) del router CE principal con su correspondiente router PE han caído y en la figura 3.2 se aprecia la pérdida de paquetes hacia la sede en IBM.

```
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=16ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=16ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
Reply from 10.110.6.33: bytes=32 time=16ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=18ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=21ms TTL=251
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
```

Figura 3.4 Verificación de conectividad y prueba de tracert. (Fuente: Propia)

```
Tracing route to 10.110.6.33 over a maximum of 30 hops

  1    83 ms     4 ms     4 ms  10.0.10.120
  2    11 ms    11 ms    11 ms  10.0.10.121
  3     5 ms     4 ms     4 ms  10.225.68.193
  4    17 ms    17 ms    17 ms  10.15.24.237
  5    24 ms    24 ms    24 ms  10.110.3.1
  6    18 ms    17 ms    17 ms  10.110.6.33

Trace complete.
```

Figura 3.5 Prueba de tracert a través de enlace de respaldo (Fuente: Propia)

Luego de ello, se observa en la figura 3.4 que la conectividad ha sido restablecida automáticamente y en la figura 3.5 se observa que desde la PC de prueba ubicada en el segmento lan de la sede remota se realiza una prueba de tracert hacia la IP ubicada en el segmento lan de la sede en IBM, verificando que el tráfico tiene como primer salto al router CE principal (default Gateway, 10.0.10.120) pasando luego por el router CE de respaldo (10.0.10.121) a través de la sesión BGP entre ambos; y finalmente a través del enlace de respaldo llega a la sede en IBM.

Luego de realizada la verificación el enlace de respaldo, el proveedor procede a levantar nuevamente la interfaz del switch de acceso que había apagado para esta prueba, con lo cual las sesiones BGP entre el router CE principal y su correspondiente router PE se restablecen, permitiendo que el tráfico pueda viajar por este enlace principal. Se observa en la figura 3.6 el tracert a través de este enlace principal.

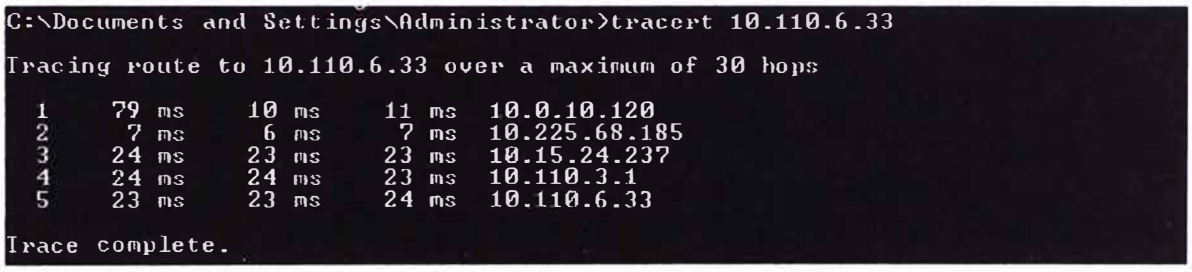


Figura 3.6 Restablecimiento de la sesión BGP entre el router CE principal y PE, Prueba de tracert (Fuente: Propia)

Se puede apreciar en la figura 3.6 que luego del restablecimiento de las sesiones BGP del router CE principal, el tracert tiene como primer salto a este equipo (default gateway 10.0.10.120) y a su correspondiente router PE (10.225.68.185) como siguiente salto.

b) Caída del enlace de última milla del router CE principal:

En esta prueba se realiza la caída del enlace de última milla del router CE principal.

Para ello, se procede con el apagado del equipo media converter, el cual se encuentra dentro de la sede remota conectado en la interfaz WAN del router CE principal. Su función es convertir el medio físico de cobre en fibra óptica.

Al realizar el apagado del media converter, se observa en la figura 3.8 que la interfaz WAN del router CE principal GigabitEthernet 0/0 cae y por consiguiente, también caen las sesiones BGP con su router PE.

Se aprecia igualmente en esta figura, que el router CE principal pasa al estado Standby a través del protocolo HSRP; el cual genera un tiempo de pérdida de conectividad con la sede en IBM, figura 3.7, mientras dura el proceso de convergencia del protocolo HSRP.

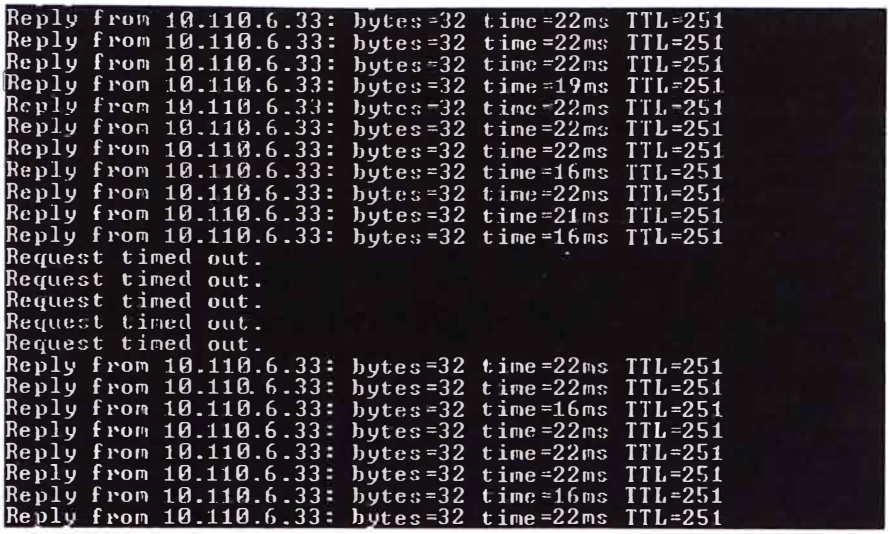


Figura 3.7 Pérdida de conectividad entre la sede remota y la sede en IBM, producto de la caída de enlace de última milla, (Fuente: Propia)

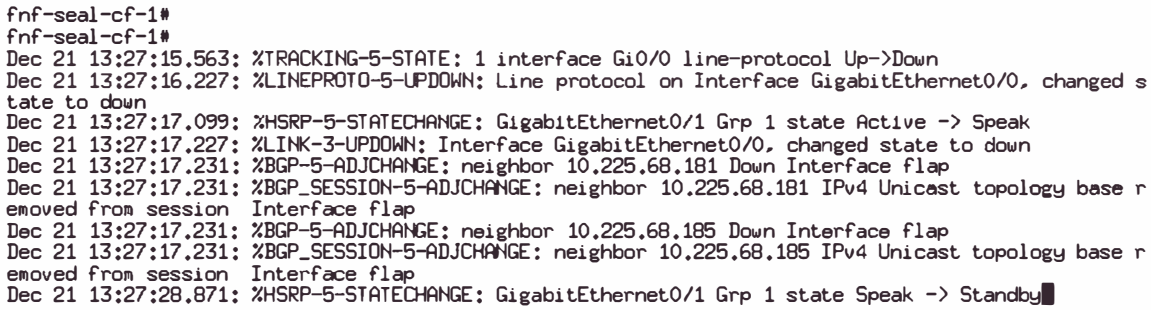


Figura 3.8 Caída de enlace de última milla y estado Standby del router CE principal del protocolo HSRP. (Fuente: Propia)

En la figura 3.7 se observa también, que la conectividad con la sede en IBM se restablece. El tracert de la figura 3.9 indica que el default Gateway es ahora el router CE de respaldo (10.0.10.121) quien asume la función de router Activo a través del protocolo HSRP. Luego de ello, el tráfico es enviado a través del enlace de respaldo hacia la sede en IBM.

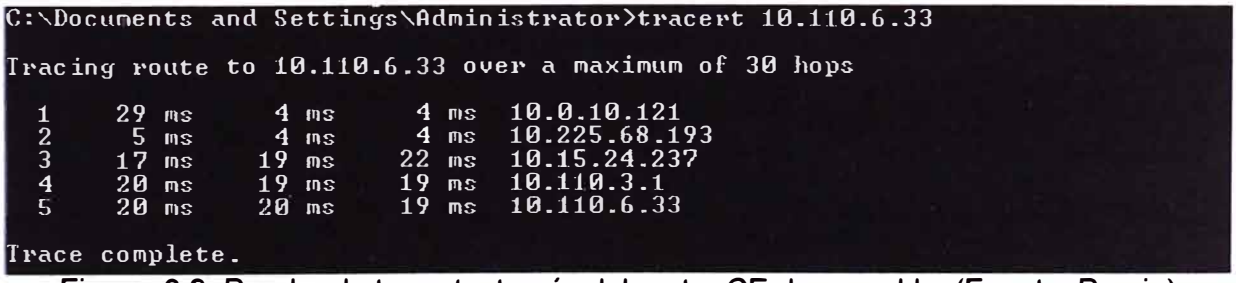
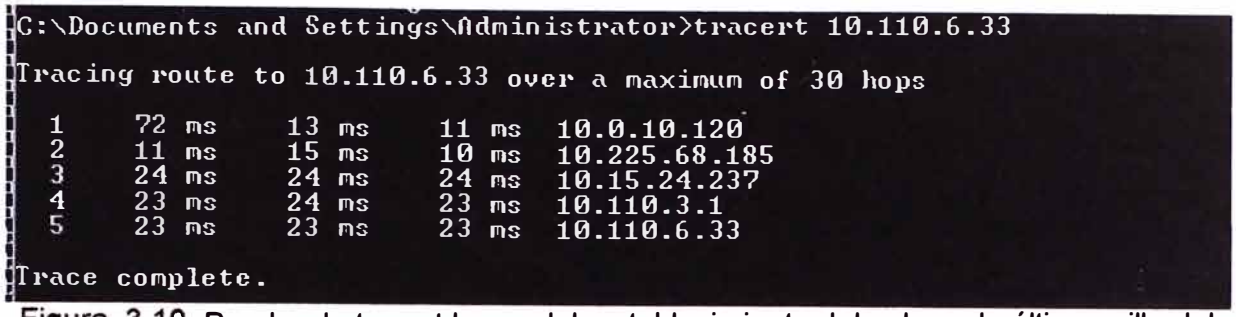


Figura 3.9 Prueba de tracert a través del router CE de respaldo. (Fuente: Propia)

Luego de realizada la prueba, se procede con el encendido del equipo media converter con lo cual las sesiones BGP del router CE principal (10.0.10.120) se activan nuevamente y este equipo retoma el roll de default Gateway de la sede remota, figura 3.11.

Esto se aprecia en la figura 3.10 con la prueba de tracert realizada; el primer salto es el

router CE principal (10.0.10.120) y el siguiente salto es su correspondiente router PE (10.225.68.185) a través del enlace principal.



```
C:\Documents and Settings\Administrator>tracert 10.110.6.33

Tracing route to 10.110.6.33 over a maximum of 30 hops

  1    72 ms    13 ms    11 ms  10.0.10.120
  2    11 ms    15 ms    10 ms  10.225.68.185
  3    24 ms    24 ms    24 ms  10.15.24.237
  4    23 ms    24 ms    23 ms  10.110.3.1
  5    23 ms    23 ms    23 ms  10.110.6.33

Trace complete.
```

Figura 3.10 Prueba de tracert luego del restablecimiento del enlace de última milla del router CE principal. (Fuente: Propia)

```
fnf-seal-cf-1#
fnf-seal-cf-1#
Dec 21 13:27:15.563: %TRACKING-5-STATE: 1 interface Gi0/0 line-protocol Up->Down
Dec 21 13:27:16.227: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
tate to down
Dec 21 13:27:17.099: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Active -> Speak
Dec 21 13:27:17.227: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
Dec 21 13:27:17.231: %BGP-5-ADJCHANGE: neighbor 10.225.68.181 Down Interface flap
Dec 21 13:27:17.231: %BGP_SESSION-5-ADJCHANGE: neighbor 10.225.68.181 IPv4 Unicast topol
emoved from session  Interface flap
Dec 21 13:27:17.231: %BGP-5-ADJCHANGE: neighbor 10.225.68.185 Down Interface flap
Dec 21 13:27:17.231: %BGP_SESSION-5-ADJCHANGE: neighbor 10.225.68.185 IPv4 Unicast topol
emoved from session  Interface flap
Dec 21 13:27:28.871: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Speak -> Standb
Dec 21 13:32:09.227: %TRACKING-5-STATE: 1 interface Gi0/0 line-protocol Down->Up
Dec 21 13:32:10.227: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
Dec 21 13:32:10.431: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Standby -> Acti
Dec 21 13:32:11.227: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
tate to up
Dec 21 13:32:16.375: %BGP-5-ADJCHANGE: neighbor 10.225.68.185 Up
Dec 21 13:32:19.443: %BGP-5-ADJCHANGE: neighbor 10.225.68.181 Up
Dec 21 13:32:29.359: %TRACKING-5-STATE: 1 interface Gi0/0 line-protocol Up->Down
Dec 21 13:32:30.207: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Active -> Speak
Dec 21 13:32:30.227: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
tate to down
Dec 21 13:32:31.227: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to down
Dec 21 13:32:31.231: %BGP-5-ADJCHANGE: neighbor 10.225.68.181 Down Interface flap
Dec 21 13:32:31.231: %BGP_SESSION-5-ADJCHANGE: neighbor 10.225.68.181 IPv4 Unicast topol
emoved from session  Interface flap
Dec 21 13:32:31.235: %BGP-5-ADJCHANGE: neighbor 10.225.68.185 Down Interface flap
Dec 21 13:32:31.235: %BGP_SESSION-5-ADJCHANGE: neighbor 10.225.68.185 IPv4 Unicast topol
emoved from session  Interface flap
Dec 21 13:32:31.359: %TRACKING-5-STATE: 1 interface Gi0/0 line-protocol Down->Up
Dec 21 13:32:33.087: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Speak -> Active
Dec 21 13:32:33.227: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
Dec 21 13:32:34.227: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0,
tate to up
Dec 21 13:32:37.871: %BGP-5-ADJCHANGE: neighbor 10.225.68.181 Up
Dec 21 13:32:42.991: %BGP-5-ADJCHANGE: neighbor 10.225.68.185 Up
```

Figura 3.11 Restablecimiento del enlace de última milla del router CE principal y retorno a estado Activo. (Fuente: Propia)

c) Caída de la interfaz lan de router CE principal:

En esta prueba se realiza la caída de la interfaz lan del router CE principal. Para ello se procede con la desconexión de la red de la interfaz lan del router CE principal. Se puede observar en la figura 3.13 que el protocolo HSRP en el router CE principal conmuta del estado Activo a Init, por lo que se deduce que el router CE de respaldo pasa de estado Standby a Activo, asumiendo la función de default Gateway de la sede remota.

```
Reply from 10.110.6.33: bytes=32 time=16ms TTL=251
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
Reply from 10.110.6.33: bytes=32 time=21ms TTL=251
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=16ms TTL=251
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
Reply from 10.110.6.33: bytes=32 time=21ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=21ms TTL=251
Reply from 10.110.6.33: bytes=32 time=16ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=18ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=21ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=19ms TTL=251
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=17ms TTL=251
Reply from 10.110.6.33: bytes=32 time=16ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=21ms TTL=251
Reply from 10.110.6.33: bytes=32 time=19ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
```

Figura 3.12 Pérdida de conectividad hacia la sede en IBM. (Fuente: Propia)

```
fnf-seal-cf-1#
fnf-seal-cf-1#
Dec 21 13:36:42.227: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, change
tate to down
Dec 21 13:36:43.227: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
Dec 21 13:36:43.227: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Active -> Init
Dec 21 13:37:08.187: %BGP-5-ADJCHANGE: neighbor 10.0.10.121 Down BGP Notification sent
Dec 21 13:37:08.187: %BGP-3-NOTIFICATION: sent to neighbor 10.0.10.121 4/0 (hold time expired)
ytes
Dec 21 13:37:08.187: %BGP_SESSION-5-ADJCHANGE: neighbor 10.0.10.121 IPv4 Unicast topology base
oved from session  BGP Notification sent
```

Figura 3.13 Protocolo HSRP en router CE principal pasa a estado INIT (Fuente: Propia)

Se puede observar también, en la figura 3.12, que luego de la caída la conectividad con la sede en IBM es reestablecida automáticamente.

También, puede apreciarse en la figura 3.14 que el tracert hacia la sede en IBM es enviado al router CE de respaldo (10.0.10.121) y luego a su correspondiente router PE a través del enlace de respaldo.

```
C:\Documents and Settings\Administrator>tracert 10.110.6.33

Tracing route to 10.110.6.33 over a maximum of 30 hops

  1    32 ms     4 ms     4 ms  10.0.10.121
  2    11 ms    10 ms    10 ms  10.225.68.193
  3    17 ms    16 ms    17 ms  10.15.24.237
  4    24 ms    23 ms    23 ms  10.110.3.1
  5    17 ms    17 ms    17 ms  10.110.6.33

Trace complete.
```

Figura 3.14 Tracert a través de router CE de respaldo. (Fuente: Propia)

```
fnf-seal-cf-1#
fnf-seal-cf-1#
Dec 21 13:36:42.227: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
tate to down
Dec 21 13:36:43.227: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
Dec 21 13:36:43.227: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Active -> Init
Dec 21 13:37:08.187: %BGP-5-ADJCHANGE: neighbor 10.0.10.121 Down BGP Notification sent
Dec 21 13:37:08.187: %BGP-3-NOTIFICATION: sent to neighbor 10.0.10.121 4/0 (hold time exp
ytes
Dec 21 13:37:08.187: %BGP_SESSION-5-ADJCHANGE: neighbor 10.0.10.121 IPv4 Unicast topology
oved from session  BGP Notification sent
```

Figura 3.15 Protocolo HSRP en router CE principal pasa a estado INIT.(Fuente: Propia)

Finalmente, luego de realizada la prueba, se realiza la conexión de la interfaz LAN del router CE principal, con lo cual éste router pasa a estado Activo, asumiendo nuevamente la función de default Gateway de la sede remota, ver figura 3.17. Se observa en la figura 3.16 la prueba del tracert donde el tráfico es enviado al router CE principal (10.0.10.120) y luego a través del enlace principal hacia la sede en IBM.

```
C:\Documents and Settings\Administrator>tracert 10.110.6.33

Tracing route to 10.110.6.33 over a maximum of 30 hops

  1    70 ms    11 ms    10 ms  10.0.10.120
  2    11 ms    11 ms    10 ms  10.225.68.185
  3    23 ms    23 ms    23 ms  10.15.24.237
  4    24 ms    23 ms    23 ms  10.110.3.1
  5    23 ms    23 ms    24 ms  10.110.6.33

Trace complete.
```

Figura 3.16 Prueba de tracert, router CE principal retorna al estado Activo. (Fuente: Propia)

```
fnf-seal-cf-1#
Dec 21 13:36:42.227: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
tate to down
Dec 21 13:36:43.227: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to down
Dec 21 13:36:43.227: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Active -> Init
Dec 21 13:37:08.187: %BGP-5-ADJCHANGE: neighbor 10.0.10.121 Down BGP Notification sent
Dec 21 13:37:08.187: %BGP-3-NOTIFICATION: sent to neighbor 10.0.10.121 4/0 (hold time exp
ytes
Dec 21 13:37:08.187: %BGP_SESSION-5-ADJCHANGE: neighbor 10.0.10.121 IPv4 Unicast topology
oved from session  BGP Notification sent
Dec 21 13:40:35.227: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
Dec 21 13:40:36.227: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1,
tate to up
Dec 21 13:40:37.107: %BGP-5-ADJCHANGE: neighbor 10.0.10.121 Up
Dec 21 13:40:38.455: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Listen -> Active
```

Figura 3.17 Protocolo HSRP, router CE principal retorna al estado Activo. (Fuente: Propia)

d) Apagado de router CE principal:

En esta prueba, se realiza el apagado del router CE principal, con el objeto de simular la caída del equipo. Se muestra las siguientes gráficas, luego del apagado:

```
Reply from 10.110.6.33: bytes=32 time=16ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=21ms TTL=251
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
Reply from 10.110.6.33: bytes=32 time=21ms TTL=251
Reply from 10.110.6.33: bytes=32 time=16ms TTL=251
Reply from 10.110.6.33: bytes=32 time=22ms TTL=251
```

Figura 3.18 Pérdida de conectividad hacia la sede en IBM (Fuente: Propia)

```
IBM's internal systems must only be used only for conducting IBM's business, or for purposes a
rized by IBM management.

username: password$1
password:

Enter old password:

% Authentication failed

username: ibmcbeas
password:

fnf-seal-cf-2#
fnf-seal-cf-2#
fnf-seal-cf-2#
Dec 21 13:49:40.419: %HSRP-5-STATECHANGE: GigabitEthernet0/1 Grp 1 state Standby -> Active
Dec 21 13:49:55.191: %BGP-5-ADJCHANGE: neighbor 10.0.10.120 Down BGP Notification sent
Dec 21 13:49:55.191: %BGP-3-NOTIFICATION: sent to neighbor 10.0.10.120 4/0 (hold time expired)
ytes
Dec 21 13:49:55.191: %BGP_SESSION-5-ADJCHANGE: neighbor 10.0.10.120 IPv4 Unicast topology base
oved from session  BGP Notification sent
```

Figura 3.19 Router CE de respaldo pasa a estado Activo en HSRP. (Fuente: Propia)

Se puede observar en la figura 3.18 que se presenta una pérdida de conectividad con la sede en IBM, la cual es automáticamente restablecida y en la figura 3.19 se observa que el protocolo HSRP converge y el router CE de respaldo pasa a estado Activo.

En la figura 3.20 se observa la prueba de tracert desde la PC de prueba en la sede remota hacia la sede en IBM, donde se puede apreciar que el tráfico es enviado al router CE de respaldo (10.0.10.121) que es ahora el default Gateway de la sede remota; luego el tráfico es enviado al router PE del enlace de respaldo para llegar a la sede principal en IBM.

Se puede observar que los tiempos de respuesta por cada salto son similares a través del enlace principal y de respaldo.

```
C:\Documents and Settings\Administrator>tracert 10.110.6.33

Tracing route to 10.110.6.33 over a maximum of 30 hops

  1    73 ms    11 ms    12 ms  10.0.10.121
  2     4 ms     4 ms     4 ms  10.225.68.193
  3    24 ms    23 ms    40 ms  10.15.24.237
  4    24 ms    24 ms    24 ms  10.110.3.1
  5    23 ms    23 ms    23 ms  10.110.6.33

Trace complete.
```

Figura 3.20 Prueba de tracert a través de router CE de respaldo. (Fuente: Propia)

```
C:\Documents and Settings\Administrator>tracert 10.110.6.33

Tracing route to 10.110.6.33 over a maximum of 30 hops

  1    72 ms    11 ms    11 ms  10.0.10.120
  2    11 ms    10 ms    10 ms  10.225.68.185
  3    20 ms    19 ms    19 ms  10.15.24.237
  4    24 ms    25 ms    25 ms  10.110.3.1
  5    24 ms    23 ms    23 ms  10.110.6.33

Trace complete.
```

Figura 3.21 Prueba de tracert hacia la sede en IBM, router CE principal. (Fuente: Propia)

```
fnf-seal-cf-2#telnet 10.0.10.120
Trying 10.0.10.120 ... Open

IBM's internal systems must only be used only for conducting IBM's business, or for purpo
rized by IBM management.

username: ibmcbeas
password:

fnf-seal-cf-1#sh ver
Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(3)T, RELEASE SOFTW
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Mon 15-Nov-10 22:51 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)

fnf-seal-cf-1 uptime is 2 minutes
System returned to ROM by power-on
System image file is "flash0:c2900-universalk9-mz.SPA.151-3.T.bin"
Last reload type: Normal Reload


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.


fnf-seal-cf-1#
```

Figura 3.22 Encendido de router CE principal luego de realizada la prueba. (Fuente: Propia)

Finalmente, en la figura 3.22 se observa el encendido del router CE principal, lo cual permite que este router retorne al estado Activo del protocolo HSRP; pasando a ser nuevamente el default Gateway de la sede remota. La prueba de tracert de la figura 3.21 muestra el primer salto a través del router CE principal (10.0.10.120) y el segundo salto a través del router PE del enlace principal hacia la sede en IBM.

3.5. Análisis de resultados

Se ha realizado la implementación de un servicio de datos e internet; soportado sobre un equipo router utilizado como principal y otro de similares características utilizado como respaldo.

La interconexión entre los equipos de la sede del cliente y el centro de cómputo donde se encuentran alojados los servicios (servidores, aplicaciones, BDs, servicios de internet y correo) se realiza a través de la red del proveedor de servicios, quien asegura la conectividad de red a nivel capa 3 (IP), capa 2 (enlace de datos) y física; así como también, la priorización y asignación de BW a los tipos de tráfico de acuerdo a la calidad requerida por el cliente.

El servicio de Red Privada Virtual sobre la red MPLS está orientado a ofrecer la integración de los servicios a través de un proveedor, con lo cual se tiene:

-Convergencia: consolidar la comunicación de voz, datos e internet en un solo enlace.

-Seguridad: Los enlaces VPN presentan autenticación y algoritmos complejos, asegurando la privacidad y seguridad.

-Escalabilidad: la red implementada soporta diferentes cambios sobre servicios y redes, siendo el cambio o modificaciones de fácil implementación en cuanto coste y horas hombre.

-Calidad de Servicio: La Red Privada Virtual sobre la red MPLS garantiza la priorización del tráfico de acuerdo a las aplicaciones que requieran servicio en tiempo real ó servicio para datos críticos.

La red de acceso (Metro Ethernet) del proveedor, soporta puertos con capacidades de Gigabit Ethernet, lo cual asegura la escalabilidad necesaria para soportar el tráfico de aplicaciones futuras y crecimiento de la red de los clientes.

Luego de realizada la implementación del enlace hacia una sede remota; se realizan las pruebas de contingencia cuya finalidad es la de probar que automáticamente el tráfico de datos será encaminado por el enlace de respaldo en condiciones en las que el enlace principal se encuentre indisponible; estas pruebas realizadas resultaron exitosas.

CONCLUSIONES Y RECOMENDACIONES

1. Es necesario indicar que los enlaces de respaldo juegan un papel importante en garantizar una máxima disponibilidad de servicios de red del cliente, ya que, ante la avería del enlace principal ó equipo de comunicación (switch, router) perteneciente a este enlace, el enlace de respaldo asumirá la carga de tráfico y transporte de los datos del cliente al centro de cómputo final, de manera casi transparente para el cliente.

2. Se deben tener claros los criterios de enrutamiento a emplear en la configuración de los equipos ruteadores para la conmutación del enlace principal al de respaldo, ya que de no estar correctamente definidos podrían derivar en un mal funcionamiento de este enlace; generando su activación sin que haya sido afectado el enlace principal ó no activándose cuando sea requerido.

3.- La red MPLS – VPN está orientada a ofrecer la integración de los servicios a través de la red de un proveedor, con lo cual se tiene:

-Convergencia: consolidad la comunicación de voz, datos e internet en un solo enlace.

-Seguridad: los enlaces VPN presentan autenticación y algoritmos complejos, asegurando la privacidad.

-Escalabilidad: la red MPLS – VPN soporta diferentes cambios sobre servicios y redes siendo éstos de fácil implementación en cuanto coste y horas hombre.

-Calidad de Servicio: la red MPLS – VPN garantiza la priorización del tráfico de acuerdo a las aplicaciones que requieran servicio en tiempo real ó servicio para datos críticos.

4. Se recomienda realizar un análisis previo del nivel y cantidad de BW que requieren las aplicaciones del cliente (servicios de voz, datos, internet, correo, BD, etc.) a fin de dimensionar correctamente el nivel necesario de calidad de servicio a los enlaces de las sedes remotas y no incurrir en un gasto innecesario al proyecto.

5. Es importante la realización de pruebas periódicas de respaldo, como las indicadas en el informe, con la finalidad de probar su correcto funcionamiento. Estas pruebas pueden realizarse con una periodicidad anual o semi-anual.

6.- Se recomienda utilizar el uso de sistemas de monitoreo que permitan reportar el consumo, caída/falla del enlace principal.

ANEXO A
GLOSARIO DE TÉRMINOS

ANEXO A
GLOSARIO DE TÉRMINOS

ARP:	Address Resolution Protocol
AS:	Autonomous System
ATM:	Asynchronous Transfer Mode
BGP:	Border Gateway Protocol
CIDR:	Classless Inter-Domain Routing
EIGRP:	Enhanced Interior Gateway Routing Protocol
ELSR:	Edge Label Switch Router
IGP:	Internal Gateway Protocol
IOS:	Internetwork Operating System
IP:	Internet Protocol
ISDN:	Integrated Services Digital Network
ISP:	Internet Service Provider.
LSR:	Label Switch Router
MPBGP:	Multi Protocol BGP
MPLS:	Multiprotocol Label Switching
OSPF:	Open Shortest Path First
PVC:	Permanent Virtual Circuit
QoS:	Quality of Service
RIP:	Routing Information Protocol
RPVL:	Red Privada Virtual Local
RPVN:	Red Privada Virtual Nacional
TTL:	Time To Live
TI:	Technology of Information
VC:	Virtual Circuit
VLSM:	Variable Length Subnet Masking
VRF:	Virtual Routing and Forwarding

ANEXO B

TABLA DE RELACIÓN DE EQUIPOS CISCO Y CAPACIDADES

Tabla Nº B.1 Relación de equipos cisco y capacidades

	Equipo	Interfaz de Red (Mbps)	Flash	DRAM	POTENCIA	DIMENSIONES (H x W x D cm)
Sede IBM	Switch Cisco WS-CBS3110X-S-I	100/1000 /10000	512KB	264 MB	45 w	26.0 x 11.2 3.0
	Switch Cisco WS-C6506-E	1000 /10000	64 MB	1024 MB	950 w	48.8 x 44.5 x 46.0
	Router Cisco 7206VXR	100/1000	64 MB	2048 MB	370 w	13.34 x 42.67 x 43.18
	Firewall Cisco ASA 5540	1000	256 MB	2048 MB	190 w	4.45 x 20 x 36.2
	Router Cisco 2921/K9	100/1000	256 MB	512 MB	370 w	8.9 x 43.8 x 47
Sede Remota	Router Cisco 2921/K9	100/1000	256 MB	512 MB	370 w	8.9 x 43.8 x 47
	Switch Cisco WS-C2960-24LC-S	100/1000	64 KB	64 MB	123 w	4.4 x 45 x 33

ANEXO C
TABLAS DE COMANDOS QOS PARA ROUTER CISCO

Tabla C.1 Creación de Clases de tráfico a nivel LAN

class-map match-any P5	Crea una clase de tráfico llamada P5.
match ip dscp cs5	Clasifica el tráfico definido como CS5 (DSCP 40) que el cliente utiliza para el tráfico de voz ó video, cuyos paquetes han sido marcados por el cliente a fin de ser clasificados por el router.
match access-group name qos5	Clasifica el tráfico definido dentro de un ACL llamado "qos5" el cual contiene el tráfico de voz ó video.
class-map match-any P2	Crea una clase de tráfico llamada P2.
match ip dscp cs2	Clasifica el tráfico definido como CS2 (DSCP 16) que el cliente utiliza para el tráfico de datos críticos, cuyos paquetes han sido marcados previamente por el cliente a fin de ser clasificados por el router.
match access-group name qos2	Clasifica el tráfico definido dentro de un ACL llamado "qos5" el cual contiene el tráfico de datos críticos.

Tabla C.2 Creación de Políticas de Calidad de Servicio (QoS) a nivel LAN

policy-map SetDscpLan	Creación de una política llamada "SetDscpLan".
class P5	Llama a la clase de servicio P5 creada previamente.
set ip dscp cs5	Acción de marcar todos los paquetes de esta clase con DSCP CS5.
class P2	Llama a la clase de servicio P2 creada previamente.
set ip dscp cs2	Acción de marcar todos los paquetes de esta clase con DSCP CS2.
class class-default	Clase de servicio Default (creada por defecto).
set ip dscp cs1	Se marcan todos los paquetes de esta clase (que no pertenecen a ninguna de las 2 clases anteriores) con DSCP CS1.

Tabla C.3 Creación de Políticas de Calidad de Servicio (QoS) para la gestión del tráfico a nivel WAN

policy-map wanN	Creación de una política llamada "wanN".
class qos5	Llama a la clase de servicio qos5 creada previamente.
priority 1024	Asigna prioridad de acuerdo al parámetros de ancho de ancho de banda por canal de tráfico del tipo VoIP, ToIP, Videoconferencia o cualquier otro tipo de tráfico sensible al retardo.
police 1024000 conform-action transmit exceed-action drop	
Limita el ancho de banda asignado como tráfico con prioridad cs5 (clase qos5) a un valor de 1024 kbps, descartando el exceso.	
class qos2	Llama a la clase de servicio qos2 creada previamente.
bandwidth 4096	Asigna un ancho de banda de 4096 kbps para el tráfico que pertenece a la clase qos2.
police 4096000 768000 1536000 conform-action transmit exceed-action set-dscp-transmit cs1	
Limita el ancho de banda asignado como tráfico con prioridad 2 (cs2), el exceso de tráfico será remarcado como prioridad 1 (cs1).	
class qos1	Llama a la clase de servicio qos1 creada previamente.
bandwidth 3072	Asigna un ancho de banda de 3072 kbps para el tráfico que pertenece a la clase qos1.
class class-default	Asigna el ancho de banda para el tráfico por defecto
fair-queue	Cola con pesos equitativos
policy-map Shape8192N	
Creación de una política llamada "Shape8192N", la cual define el límite del ancho de banda a ser aplicado en una interfaz.	
class class-default	Define todo el tráfico de salida por la interface WAN como una sola clase
shape average [8193000]	
Asigna el ancho de banda a un valor máximo igual a la suma de los diversos tipos de tráfico.	
service-policy wanN	Llama a la política "wanN" definida previamente, la cual contiene los diversos tipos de tráfico.

Tabla C.4 Creación de Clases de tráfico para la gestión del tráfico a nivel WAN

class-map match-any qos5	Crea una clase de tráfico llamada qos5.
match ip dscp cs5	Clasifica el tráfico definido como CS5.
match ip dscp cs6	Clasifica el tráfico definido como CS6
class-map match-any qos2	Crea una clase de tráfico llamada qos2.
match ip dscp cs2	Clasifica el tráfico definido como CS2.
class-map match-any qos1	Crea una clase de tráfico llamada qos1.
match ip dscp cs1	Clasifica el tráfico definido como CS1.
El tráfico que no se encuentre dentro de alguna clase definida, será considerado dentro de la clase "default".	

BIBLIOGRAFÍA

[1] G.Corral, J.Abella. ADSL y MPLS. Editorial Ingeniería La Salle. Madrid, España, 1997.

[2] BARBERÁ, José. MPLS: Una arquitectura de backbone para la Internet del siglo XXI.Revista: Actas del V Congreso de Usuarios de Internet. Mundo Internet 2000. Madrid, febrero 2000. Madrid, España, 1997.

[3] Monique Morrow, Azhar. MPLS and Next-Generation Networks: Foundations for NGN and Enterprise Virtualization. Indianapolis, USA. Cisco Systems 2007.

[4] Srinivas Vegesna. Cisco Press: IP Quality of Service. Indianapolis, USA. 2001

[5] Building Scalable Cisco Internetworks. Volumen1. Versión 2.1. Cisco Systems 2004.

[6] Building Scalable Cisco Internetworks. Volumen2. Versión 3.0. Cisco Systems 2006.

[7] Implementing Secure Converged Wide Area Networks. Volume 1. Cisco Systems 2006.

[8] http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps5138/product_data_sheet09186a00800ff916_ps708_Products_Data_Sheet.html

[9] http://www.cisco.com/en/US/prod/collateral/switches/ps6746/ps8741/ps8761/data_sheet_c78-468188.html

[10] http://www.cisco.com/en/US/prod/collateral/routers/ps341/data_sheet_c78_339749.html

[11] http://www.cisco.com/en/US/prod/collateral/routers/ps10537/data_sheet_c78_553896.html

[12] http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html

[13] http://www.cisco.com/en/US/docs/ios/12_1/qos/configuration/guide/qcdintro.html

[14] http://docwiki.cisco.com/wiki/MPLS/Tag_Switching

[15] http://docwiki.cisco.com/wiki/Border_Gateway_Protocol

[16] http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml